OneSpan

2022 OneSpan Global Financial Regulations Report

Contents

Introduction

Welcome to our 2021 Global Financial Regulations Report.

As we approach the two-year anniversary of the onset of the global coronavirus pandemic, the regulatory environment continues to evolve with laser focus on cybersecurity, digital identity, digital currencies and agreement automation solutions featuring electronic signatures.

While policymakers and regulators implemented temporary emergency measures in 2020 such as permitting remote online notarization, 2021 saw many temporary regulations become permanent.

Financial institutions worldwide are challenged to comply with the ever-changing regulatory landscape, while leveraging the latest technologies to balance compliance, consumer friendliness, security and expenses.

This year's report highlights results from a recent survey commissioned by OneSpan and conducted by Arizent, providing insights from financial institution compliance leaders in the United States, Mexico and Europe.

Like last year's report, we literally scanned the globe to identify recent regulations, policies, and legislation that impact banks and other financial institutions. This report is not an inventory of all regulations. It is concentrated on regulations enacted in 2020 and 2021 or those that will take effect in 2021 and 2022.

The scope of this report includes regulations and policies pertaining to privacy, cybersecurity, anti-money laundering, KYC practices, digital identity, authentication, cryptocurrency, central bank digital currencies and electronic signatures.

We hope this report is a valuable resource for you and your organization. As always, we welcome your comments and feedback. Your input will enable us to improve on this work for next year's edition. Please drop us a note at **regulations@onespan.com**.

Respectfully,

E-SIGNED by Michael Magrath
on 2021-11-01 15:07:15 GMT

Michael Magrath
Vice President
Global Regulations & Standards

E-SIGNED by Gabrielle Inhofe
on 2021-11-01 15:19:14 GMT

Gabrielle Inhofe
Strategy & Global Regulatory
Researcher

Executive Summary

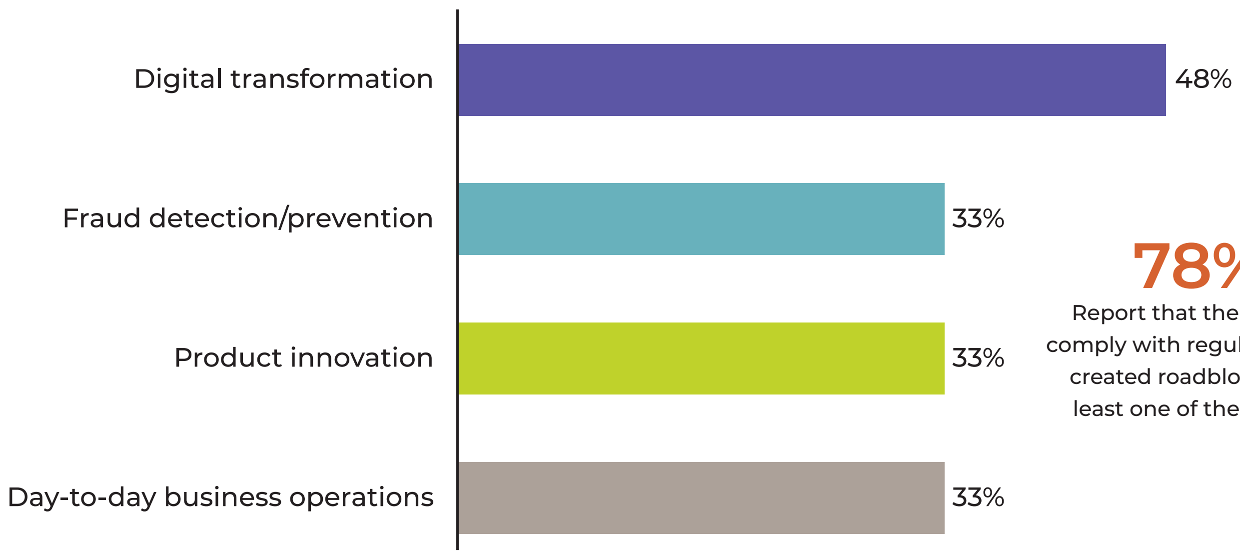
Like 2020, this past year has been defined by the COVID-19 pandemic, which has led to millions of deaths, exposed economic and financial vulnerabilities across the world, undone poverty reduction and other development progress, and worsened disparities between the Global North and the Global South. Although vaccines, containment measures and adaptations have offered some states a chance at normalcy, the pandemic continues to evolve, often with unforeseen consequences. Developing countries have faced vicious waves of infection with the arrival of the Delta variant, and global supply chains face continued disruptions. The International Monetary Fund (IMF) estimates a 5.9% expansion of the global GDP in 2021 as recovery momentum slows, and warns of inflation.[1] In 2022, structural challenges will persist and recovery will be uneven.

Alongside incalculable suffering, the health crisis has accelerated digital transformation across the world. Governments, companies and people have irrevocably changed the way they live, interact and do business in response to limits on physical contact. Consumers have flocked to e-commerce and digital payments, banks and other financial institutions have instituted remote onboarding and other digital solutions, fintechs have raked in investment funds and regulators have rushed to accommodate, develop and adopt innovative solutions. Global fintech investment reached a staggering USD$98 billion in the first half of 2021, compared with USD$121.5 billion in the whole of 2020.[2] As governments spearhead recovery initiatives, digitalization will be key in helping states to regain progress lost and build modern, strong and inclusive economies.

Indeed, digitalization initiatives are increasingly interconnected with financial inclusion goals. Approximately two billion people across the globe are unbanked, which perpetuates poverty traps as individuals are unable to apply for loans, access credit, invest and more. Digital solutions like remote onboarding can help people in rural Guatemala, Kenya or Thailand to open a bank account, even if they live hours away from a physical bank branch. In some states, however, digitalization has already widened digital divides, especially along gender, geographic and socioeconomic lines. When digital

Globally, half of banking executives responding to our survey report that the need to comply with industry regulations has created roadblocks or slowed progress on digital transformation

Has the need to comply with industry regulations created roadblocks or slowed your institution's progress in any of the following areas?



78%
Report that the need to comply with regulations has created roadblocks in at least one of these areas

Base: Total Respondents: n=172

Research conducted by Arizent and American Banker

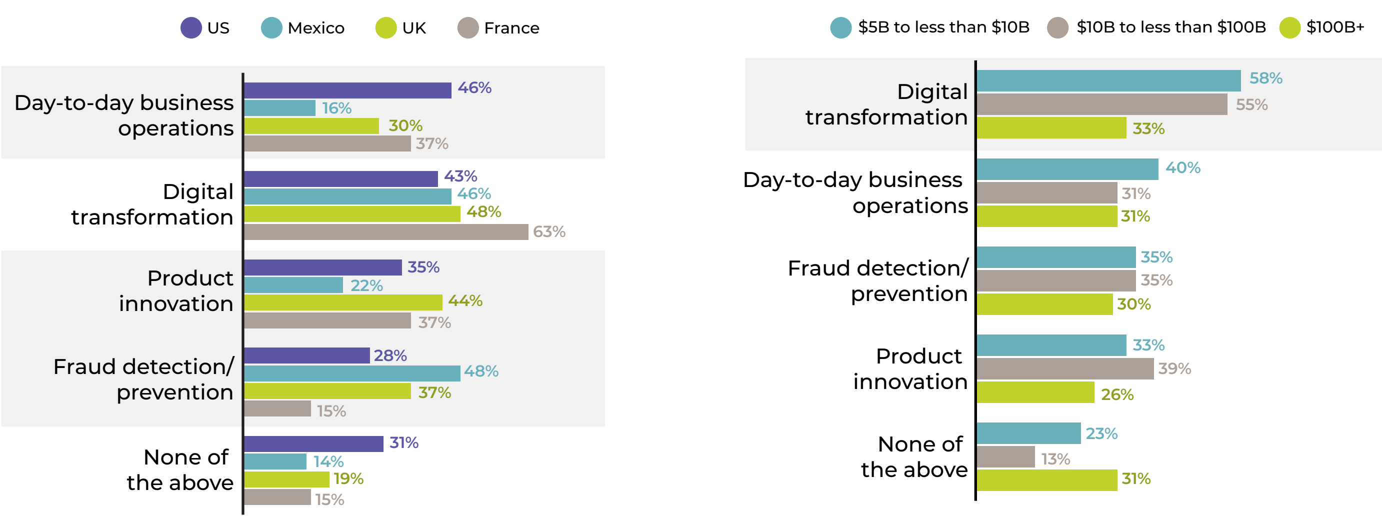
transformation is applied unevenly, it can exacerbate inequalities like a lack of access to education and job opportunities. This digital stratification will have far-reaching implications, like slowing down national recoveries.[3]

In analyzing how banks are responding to this rapid digitalization and a changing regulatory landscape, Arizent and American Banker—on behalf of OneSpan—conducted a fall 2021 survey of 172 bank leaders and executives. The respondents represented banks—with USD$5 billion or more in assets—across France, Mexico, the UK and the US. According to the survey's findings, banks are adopting innovative technologies in order to comply with industry regulations, but in some cases, regulatory requirements have slowed digital transformation. Going into 2022, a balance between digitalization and compliance will be increasingly important as disruptive technologies continue to gain ground.

Central bank digital currency (CBDC), a central bank-issued digital currency that complements cash and coins, will be one of next year's most exciting trends. About 81 jurisdictions are currently exploring CBDC, both wholesale—designed for restricted access by financial institutions, and similar to central bank reserve and settlement accounts—and retail models, issued by the central bank directly to all users. CBDCs will revolutionize financial systems by making payments cheaper, faster and more accessible,

Smaller banks are more likely to report having their digital transformation stalled by the need to comply with regulations

Has the need to comply with industry regulations created roadblocks or slowed your institution's progress in any of the following areas?

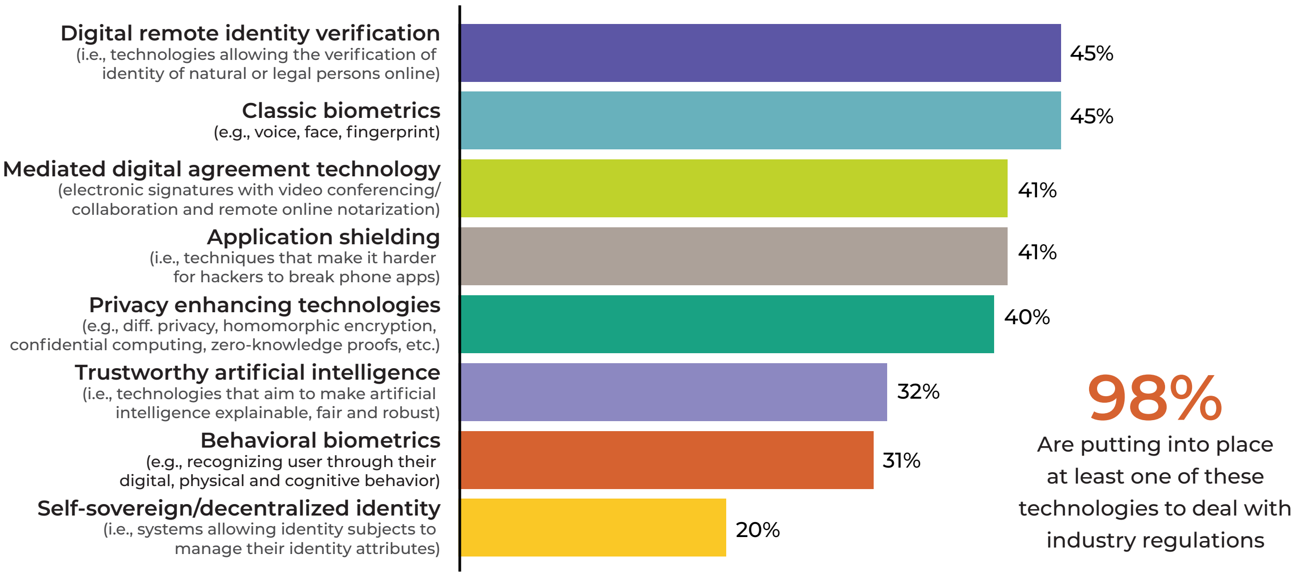


Base: US: n=68; Mexico: n=50; UK: n=27; France: n=27; $100B+: n=61; $10B to less than $100B: n=71; $5B to less than $10B: n=39
Box highlights significant differences between highest and lowest subgroups at the 95% confidence level

Research conducted by Arizent and American Banker

To comply with industry regulations, banks are most commonly putting digital remote identity verification and classic biometrics in place

What emerging technologies has your institution put in place to help you comply with industry regulations?



Base: Total Respondents: n=172

Research conducted by Arizent and American Banker

which will drive financial inclusion and ease cross-border transaction friction points. Although many central banks cite dwindling reliance on cash as motivation for a CBDC, the rising popularity of privately-issued digital currencies like Bitcoin and Ether has also driven central banks to explore their own digital currencies. Cryptocurrencies pose a potential threat to the monetary authority of central banks, and can facilitate money laundering and other illegal activities due to their decentralized nature. Some jurisdictions have banned cryptocurrency altogether. Still, it is unclear whether CBDC will actually draw investors away from cryptoassets, which are particularly popular in jurisdictions with high inflation, a lack of public confidence in the banking system and general instability.

Artificial intelligence will be another innovative technology to watch. As the AI industry continues to grow, governments across the world have introduced policies and frameworks considering the privacy and ethical implications of its use, including racial bias in biometric facial recognition. Australia, Brazil and Israel—to name just a few—are exploring ways to harness AI in the growth of the digital economy. The European Commission's proposed **Artificial Intelligence Regulation** seeks to encourage the development of AI, while classifying and regulating AI solutions according to risk. American policymakers and regulators have engaged with the National Institute for

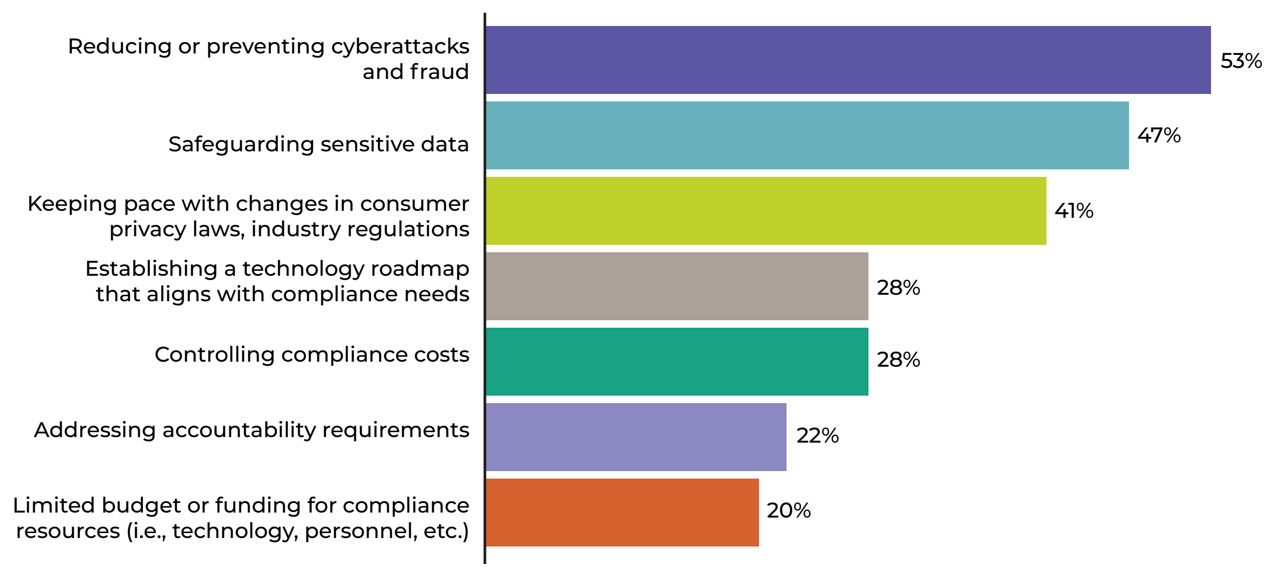
Standards and Technology (NIST) to develop an AI Risk Management framework, and the White House's Office of Science and Technology Policy released a Request for Information on public and private sector use of biometric technologies, including AI-driven ones. AI has the potential to add up to USD$15.7 trillion to the global economy by 2030, due to increased productivity and consumer demand.[4]

Digital identity is another significant trend in the development of the global digital economy. Although it has provoked cybersecurity and data privacy concerns in some instances, digital identity can encourage financial inclusion, reduce fraud and facilitate participation in the economy and public services. Much of the world's unbanked population does not have access to accepted—or any—identity documents, and a digital identity would provide them with the means to open an account and access financial products and services.

As innovation continues at breakneck pace, some governments have sought to cultivate the national fintech ecosystem, while others have taken a more hesitant approach. Bahrain and Taiwan have been particularly progressive in fostering fintech-friendly regulatory environments, and their ecosystems will be ones to watch in 2022. Fintech regulatory sandboxes, funds and tax breaks will help to lower barriers to new entrants, which will allow for a more

Globally, the top challenges are: reducing cyberattacks and fraud, safeguarding sensitive data, and keeping pace with changing laws and regulations

What are the top challenges your institution faces complying with government regulations in the banking industry?



Base: Total Respondents: n=172

Research conducted by Arizent and American Banker

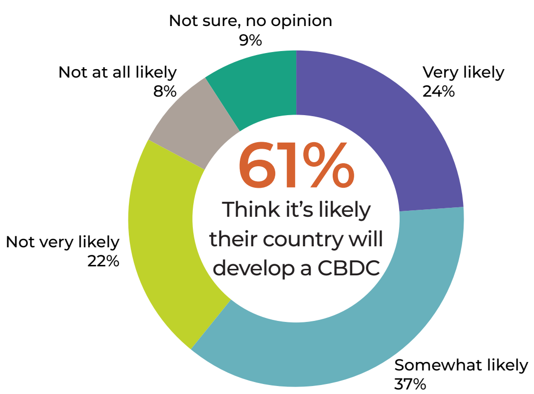
competitive ecosystem and attract foreign direct investment. Open banking will be especially instrumental in driving down the costs of financial services and products, while offering consumers more choice. In some jurisdictions, barriers to the launch of fintechs are high, and a lack of regulatory clarity prevents fintechs from competing with traditional banks.

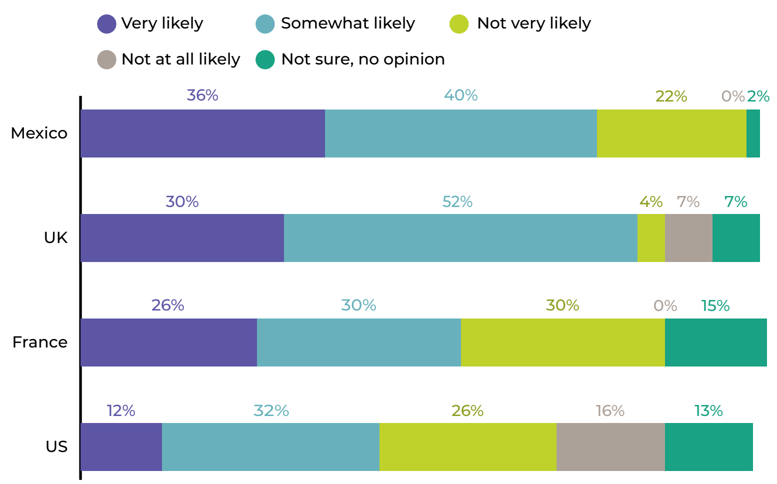
This rapid digitalization—which has effected incredible positive change—has also brought with it heightened risks, especially with regard to cybersecurity, data protection, money laundering and other illicit activities. Since the onset of the pandemic, cyberattacks have increasingly wrought havoc on governments, businesses and individuals worldwide. The World Economic Forum's ***Global Risks Report 2021*** names cyberattacks as one of the key threats of the coming decade. In the United States, the Colonial Pipeline ransomware attack brought the company's operations to a halt for nearly a week in May, causing a spike in oil prices and a disruption in oil distribution across the East Coast.

Cybersecurity concerns often go hand in hand with cryptocurrency, which—due to their anonymity and a general lack of regulations on exchanges—are frequently demanded as payment in the case of ransomware attacks. Central banks are issuing warnings, instituting licensing regimes, banning banks and other financial institutions from dealing in or facilitating crypto transactions,

Globally, 6-in-10 expect their country will develop a CBDC in the next two years, with greatest expectations in Mexico and least in the US

In your opinion, how likely is your country to develop a CBDC (central bank digital currency) program in the next two years?



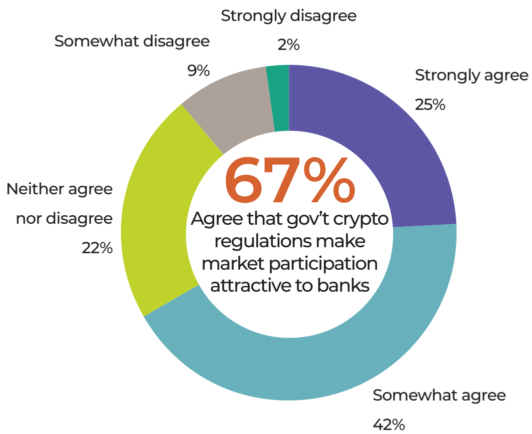


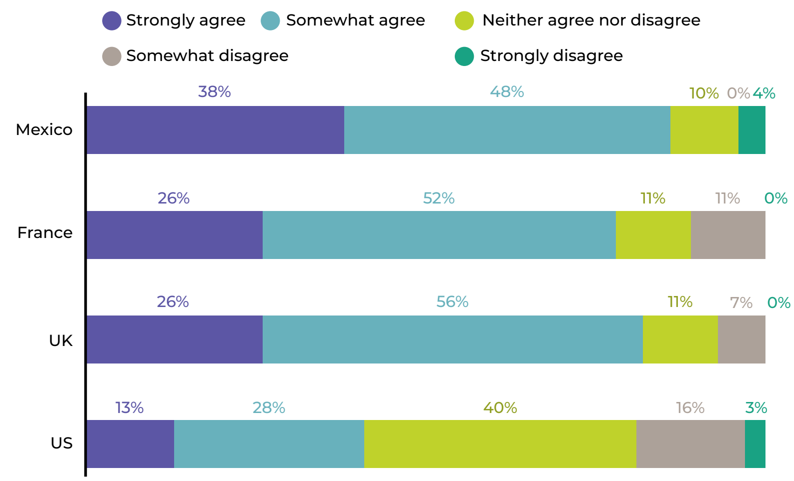
Base: Total Respondents: n=172; US: n=68; Mexico: n=50; UK: n=27; France: n=27

Research conducted by Arizent and American Banker

Globally, more than 6-in-10 agree that government crypto regulations make it more attractive for banks to participate in the market

Please rate your level of agreement with the following statement: "Governmental cryptocurrency regulations make it very attractive for banks to participate in the market."



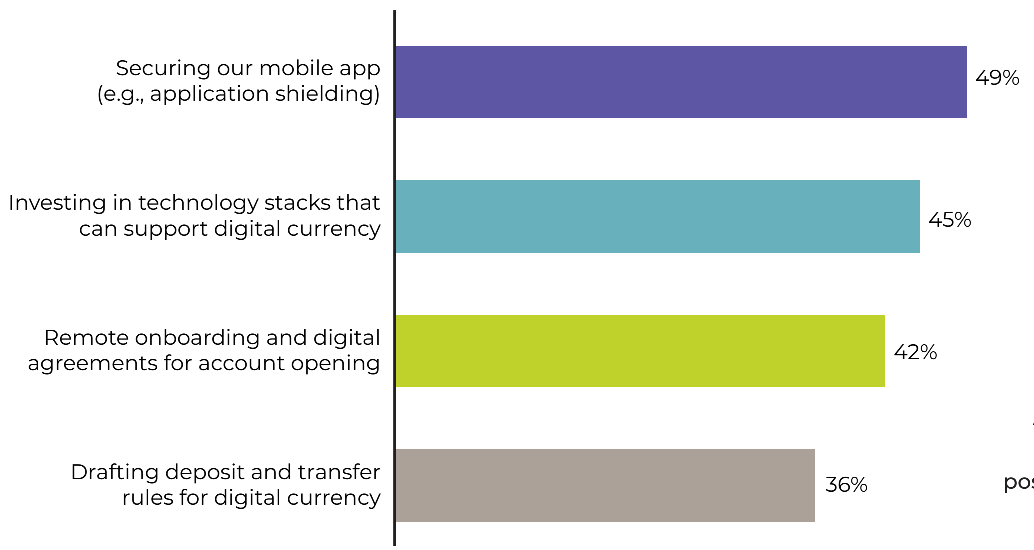


Base: Total Respondents: n=172; US: n=68; Mexico: n=50; UK: n=27; France: n=27

Research conducted by Arizent and American Banker

Globally, half of bankers report they are securing their mobile app to prepare for a possible central bank digital currency

What steps, if any, is your institution taking to prepare for a possible CBDC?



84%
Are taking steps to prepare for a possible Central Bank Digital Currency

Base: Total Respondents: n=172

Research conducted by Arizent and American Banker

and applying know-your-customer and other anti-money laundering and counter-terrorist financing rules to crypto exchanges. Still, crypto investors are undeterred, as interest levels hit record highs in 2021.

Meanwhile, the increasing reliance on digital technology has had serious data protection and privacy implications. Governments have adopted, strengthened or are currently legislating national and state data protection frameworks, many of them modeled on the European Union's General Data Protection Regulation (GDPR).

This report covers countries—and the European Union—across North America, Latin America, Europe, the Middle East, Asia-Pacific and Africa. Although each region, and each state, faces unique challenges, they are all bound by the COVID-19 pandemic, digitalization and the desire to foster a strong and modern economy.

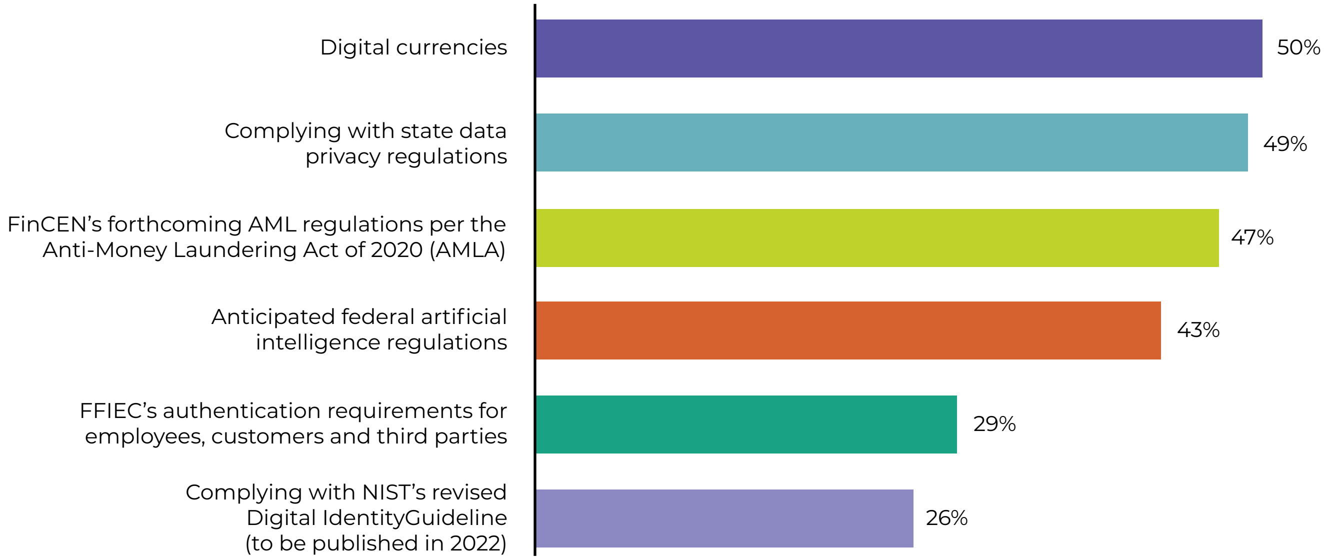
North America

Although the United States is considered the most cybersecure country in the world, in recent years, high-profile attacks on SolarWinds, Colonial Pipeline and the federal government have exposed both the state's vulnerabilities and the increasing sophistication of cybercrime. President Joe Biden and the first-ever Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger have responded strongly, making cybersecurity a top national priority. In the wake of the ransomware attack on Colonial Pipeline, President Biden issued the **Executive Order on Improving the Nation's Cybersecurity**, and he and Neuberger are launching a counter-ransomware task force. In August, the Federal Financial Institutions Examination Council (FFIEC) issued a **guidance** to financial institutions on authentication and access risk management principles and practices, pertaining to digital banking access. Cybersecurity is increasingly perceived as a matter of national security, especially as actors are often state-sponsored, and it is included in the US's first-ever **Anti-Money Laundering and Countering the Financing of Terrorism National Priorities**.

Although the United States has been progressive in fostering its digital economy, it has yet to institute a national data protection framework, a national digital identity infrastructure or an open banking system. States, including California, Colorado and Virginia, have enacted data protection laws, and a handful of other states are in the midst of legislation. The pandemic has also driven 37 states (and counting) to enact laws making remote online notarization (RON) permanent.

United States' top concerns for 2022 are digital currencies, privacy regulations, and AML

Which of these regulations are the top concerns for your institution in 2022?



Base: US: n=68

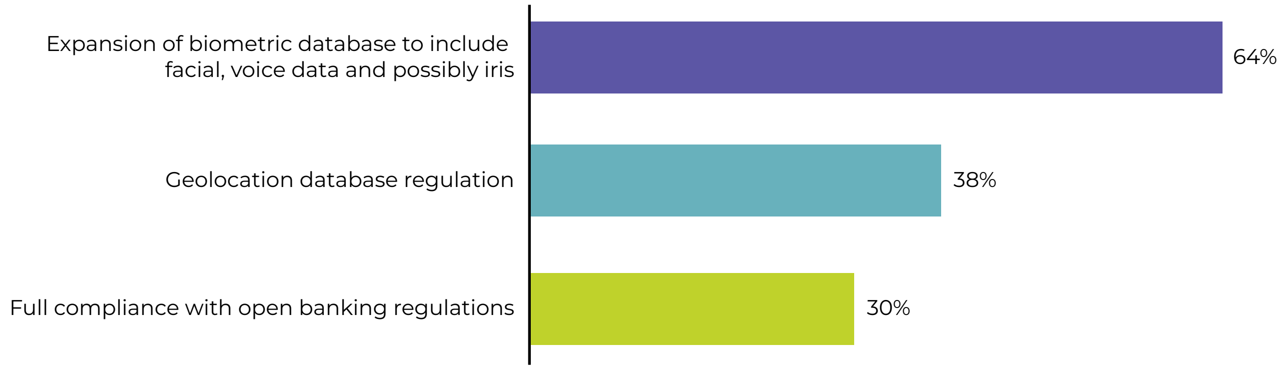
Research conducted by Arizent and American Banker

Canada has taken a divergent approach to innovation than has the United States. Its open banking system is expected to go live in January 2023, and the **Retail Payments Activities Act**, which received royal assent in June 2021, will help fintechs compete with traditional banks. The government is poised to launch a national digital identity for access to online government services. Canadian provinces have also charged ahead in implementing cutting-edge digitalization initiatives. Ontario plans to introduce Canada's first provincial data authority and a trustworthy AI framework, and is preparing to launch its optional digital identity infrastructure. The eID-Me digital identity mobile application, first launched in Ontario in 2020, was introduced in Alberta, Manitoba and Nunavut.

Neither the United States nor Canada are planning to issue a CBDC anytime soon, but a July Bank of Canada **paper** stated that one was "probably necessary" to ensure a competitive digital economy. US Federal Reserve Chair Jerome Powell, also in July, noted that a CBDC could help to counter the rising influence of cyptocurrency.

Mexico's top concern for 2022 is the expansion of a biometric database

Which of these regulations are the top concerns for your institution in 2022?



Base: Mexico: n=50
Research conducted by Arizent and American Banker

Latin America

Latin America—the most hard-hit region in the world by the pandemic—is undergoing rapid digitalization and growth in fintech, but economic resilience has faltered. Alongside a weakened economy, political instability and deepening inequality will be steep challenges as the region seeks to recover and pursue development goals. This year, its governments have focused on digital transformation, financial inclusion and the development of fintech ecosystems.

Brazil, Chile, Colombia and Mexico will be key players to watch in the fintech sphere. Colombia is set to be the third Latin American state to introduce open banking, after Brazil and Mexico. Brazil began its phased implementation of open banking in February, a process that is slated to finish in September 2022. At the time of this writing, Chile's Financial Innovation Bill is working its way through the legislative process. If passed, it will create a framework for open banking and introduce regulations designed to foster competition and innovation in the financial services sector. Mexico continues to enact provisions of its 2018 Fintech Law, which seeks to foster the development of innovative companies. Brazil and Guatemala are investigating CBDC, and Colombia and Mexico are rolling out national digital ID systems. Fintech will be key in encouraging financial inclusion, a major obstacle to further socioeconomic development in Latin America. Financial inclusion in the region has stalled since 2011, but cheaper financial services and products and a more open regulatory environment could spur on competition and widen access to banking services. Still, weak institutions and digital infrastructure remain barriers to the growth of fintech.[5]

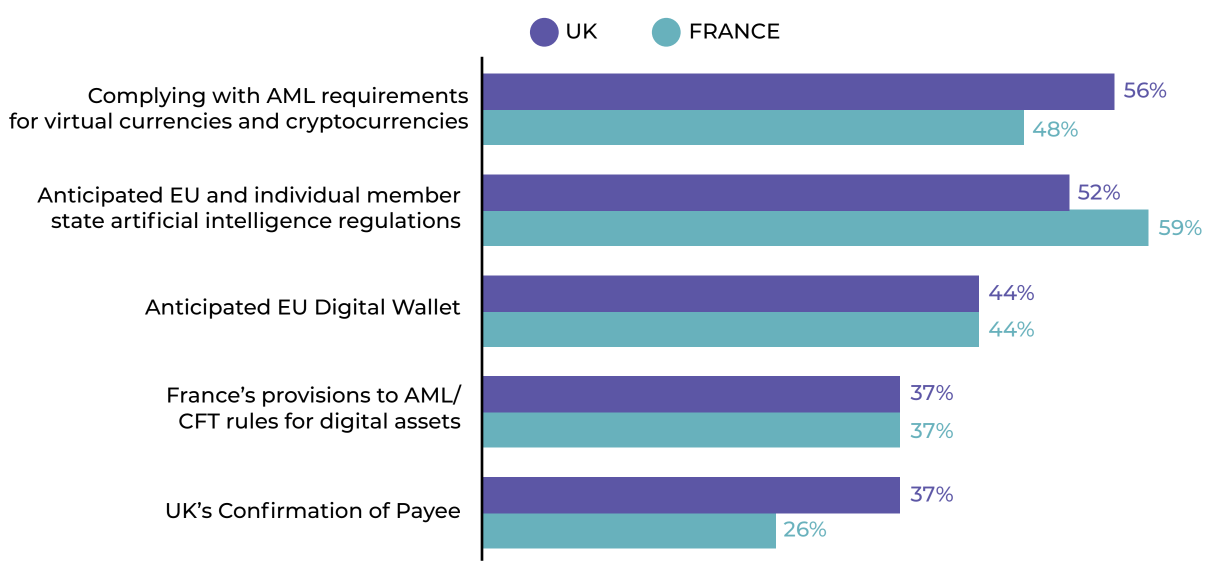
Europe

Europe is home to some of the world's most cashless societies, stable economies and progressive regulatory environments, but stark intraregional differences persist. The COVID-19 economy had disparate effects across the region, which has allowed up-and-coming fintech hubs in Northern Europe to more readily compete with established hotspots like London and Berlin. While Denmark, Norway and Sweden have been relatively unscathed by the pandemic, other countries—like Germany and the United Kingdom—have faced significant setbacks. Meanwhile, although Eastern Europe has not yet reached the smartphone penetration and cashless rates of Western Europe, Poland has become a major fintech player in Central and Eastern Europe. This evolving landscape will make Europe an interesting region to watch as it recovers from the pandemic, and this shake-up could help spur on further digital transformation in countries like Belgium and France, where it has begun to plateau.

The European Commission has been particularly keen to spearhead—and regulate—digitalization. In June, the Commission issued its proposal for a **European Digital Identity**, which would enable member states to offer individuals and businesses digital wallets that can be linked with national digital identities and that will be interoperable across the bloc. The proposal aims to reduce fraud, promote trust in e-commerce and facilitate the access

In Europe, banks in both the UK and France are most concerned about complying with AML requirements and expected AI regulations

Which of these regulations are the top concerns for your institution in 2022?



Base: UK: n=27; France: n=27

Research conducted by Arizent and American Banker

to services across member states. The European Union's digitalization efforts are often geared towards driving further regional integration, especially amidst the rise of populist and nationalist parties. In July, the Commission unveiled a comprehensive **AML/CFT legislative package**, which would establish an EU-wide Authority for Anti-Money Laundering and promote a harmonized approach to AML/CFT across the EU. The package also includes a proposal to apply AML/CFT rules to cryptoasset service providers, which would dovetail with its proposed **Regulation on Markets in Crypto-Assets (MiCA)**. MiCA, a component of the EU's **Digital Finance Strategy**, is a framework to regulate cryptoassets and cryptoasset issuers across the Single Market.

The European Union's regulatory approach is also remarkable in that it is human-centric and rights-based, which is reflected in proposals like the **Artificial Intelligence Regulation** and the **Regulation on Markets in Crypto-Assets (MiCA)**. Both proposals straddle a fine balance between encouraging the development of disruptive technologies, while protecting consumers and mitigating risks. Although the regulations must go through a lengthy legislative process before they can be enacted, they will be sure to ignite similar standards across the globe. Just three years after the GDPR went into effect, countries have rushed to emulate it and align more closely with its standards.

As European Union member states seek to recover from the pandemic, they are also pursuing ambitious national digitalization agendas. The European Union's EUR 672.5 billion (approximately USD$779.97 billion) Resilience and Recovery Fund, to be divvied up between the member states, will go towards national plans that must adhere to broad EU requirements. Member states' plans must allocate at least a fifth of their stimulus package towards digitalization initiatives. Under President Emmanuel Macron, France has been particularly notable for making digital headway, though it still lags behind the rapidly digitalizing Finland, Sweden, Denmark and the Netherlands. This year, France is focused on multiple CBDC projects, the regulation of virtual assets, the launch of a national digital ID and the strengthening of its AML/CTF framework.

As Europe's digital economy strengthens, CBDCs will be a major area to watch. The central banks of the European Union, Belgium, France, Norway, Sweden, Switzerland and the United Kingdom are all investigating CBDCs.

Middle East

Fintech is rapidly expanding in Israel and the Gulf Cooperation Council (GCC) states, including Bahrain, the Kingdom of Saudi Arabia, Qatar and the United Arab Emirates. Israel, nicknamed the "Startup Nation," is home to the world's most startups per capita,[6] the second-highest research and development expenditure per GDP[7] and over a dozen fintech unicorns.[8] The central bank has completed a digital shekel pilot, the Ministry of Finance has called for the establishment of a fintech regulatory sandbox and a national artificial intelligence program is in the works.

The wealthy and ambitious GCC states are similarly committed to fostering competitive and cutting-edge digital economies, especially as they attempt to promote growth in the non-oil sector. In February, the central bank of the United Arab Emirates partnered with the central banks of Hong Kong and Thailand, as well as the Digital Currency Institute of the People's Bank of China, for a multiple CBDC project aimed at exploring the use of CBCDs in real-time cross-border transactions. The project comes on the heels of a November 2020 joint experiment between the Kingdom of Saudi Arabia and the United Arab Emirates, also focused on cross-border payments. The GCC states have some of the highest numbers of migrant workers proportionate to the population at large, and these workers would benefit from cheaper, faster and simpler remittance processes.

Egypt is poised to make strides in digitalization, but political tension, continued reliance on oil and structural challenges like inequality remain obstacles to the development of an inclusive and modern digital economy. Still, regulators have already made progress in providing greater regulatory clarity for fintech, and digital payments are gaining in popularity. Digitalization in payments will be especially important in expanding access to financial services, as Egypt's unbanked population stands at an astonishing 67%.[9]

Meanwhile, conflict-affected Libya and Iraq continue to grapple with political and economic instability; high poverty, inflation and food insecurity; and weak digital infrastructure. Digitalization would be invaluable in bolstering financial inclusion and diversifying their oil-dependent economies, but their governments must first partner with the private sector and international development organizations in strengthening national digital infrastructure.

Asia-Pacific

Diverse and vibrant Asia-Pacific is emerging as the world's most exciting region for fintech. Regulators, financial institutions and fintechs are intent on cultivating digital talent and developing innovative solutions like artificial intelligence. Regional demand for fintech apps is surging.[10] Although Asia-Pacific fintech investment shrank in 2020 amidst the COVID-19 pandemic, it rose to USD$7.5 billion in the first half of 2021.[11] Steep competition between jurisdictions—especially in the shadow of a digital powerhouse like China—will ensure that growth in fintech continues to accelerate.

Wealthy and established economies like Australia, Hong Kong, South Korea and Taiwan are pursuing ambitious digital plans. Taiwan, Asia's top economic performer of 2020 and one of the world's most competitive economies, will be a key market to watch. Its regulators have sought to lower entry barriers for fintechs, strengthen cybersecurity and data protection frameworks, and promote the development of disruptive technologies. Hong Kong is similarly aiming to cement its status as a global financial center. In June 2021, the Hong Kong Monetary Authority (HKMA) announced its **Fintech 2025** strategy, which aims to modernize data infrastructure, promote the uptake of fintech by the financial sector, set the stage for the advent of CBDCs and provide more financial and regulatory support for the development of fintech.

Meanwhile, emerging markets like India and Southeast Asia are experiencing incredible digitalization, though structural challenges and the continued effects of the pandemic could stall progress in economic transformation. India's fast-growing fintech market is currently valued at USD$31 billion, and is forecast to expand by a staggering USD$84 billion by 2025.[12] Its young and tech-savvy population is leading a surge in digital payments, and India's United Payments Interface (UPI) recorded 3.55 billion transactions in August—an all-time high.[13]

Australia, Hong Kong, India, Japan, Malaysia, New Zealand, Taiwan and Thailand are all exploring CBDCs, which will both promote financial inclusion and interregional and international trade.

Africa

The COVID-19 pandemic drove a 2.1% contraction in Africa's 2020 GDP, its worst recession in fifty years,[14] and reversed years of poverty reduction. Poverty and inequality are set to worsen, and 39 million people across the continent will live in extreme poverty this year.[15] Although regional economic expansion has picked up in 2021, growth is still weak due to a lack of access to vaccines and structural challenges like weak institutions.[16]

Although there have been some state-led initiatives to drive fintech, the private sector has been more proactive in promoting disruptive technologies. Mobile payments have surged in Africa over the past few years, and services like Kenyan company Safaricom's M-Pesa have been instrumental in driving financial inclusion. Fintech ecosystems in Côte d'Ivoire, Ghana, Kenya, Nigeria and South Africa are particularly promising, but must be met with greater regulatory clarity and improvements to national digital infrastructure. Africa still has some of the world's lowest internet penetration rates, especially in Eastern Africa and Central Africa, at 24% and 26%, respectively.[17]

Still, there is reason for optimism on the regulatory front. In February, the Central Bank of Nigeria issued its **Regulatory Framework for Open Banking**, a month after approving a regulatory fintech sandbox. On 25 October, it became one of the first countries in the world to issue a CBDC. The bank announced the CBDC project in February, after it issued a directive banning banks and other financial institutions from dealing in and facilitating cryptocurrency transactions. Despite the ban, crypto investment continues to gain traction in the state amidst high inflation and frictional cross-border transactions. According to the director-general of the Nigerian Securities and Exchange Commission (SEC), the ban has caused market disruption, and the SEC and central bank are devising a crypto regulatory framework.

Similarly, the Bank of Ghana launched a **regulatory and innovation sandbox** in February, and in August the bank partnered with a German tech firm to spearhead a **retail CBDC trial**. Kenya has expanded its fintech regulatory sandbox to include firms with machine learning and artificial intelligence applications, and its central bank governor has addressed the possibility of exploring a CBDC. Côte d'Ivoire has also signaled an interest in exploring a CBDC.

The South African digital agenda for this year is especially robust. Signed into law in 2013, its enforcement of the **Protection of Personal Information Act (POPIA)** finally went into full effect on 01 July. The South African Reserve Bank has partnered with the Bank for International Settlements (BIS) Innovation Hub and the central banks of Australia, Malaysia and Singapore to trial the use of CBDCs in cross-border transactions. A cross-border CBDC would be crucial in making remittances faster and cheaper, especially as South Africa is the continent's largest remittance send-market, at a volume of USD$921 million in 2020. Approximately 50% of its remittances are sent via informal channels.[18]

In May, South Africa's **Cybercrimes and Cybersecurity Act** was signed into law. The Act requires electronic communications service providers and financial institutions to report cybersecurity breaches to the SA Police Service, within 72 hours of becoming aware. The Act also criminalizes cyber fraud, extortion, forgery, the sending of harmful data messages and the unauthorized access of personal data, a data storage medium or computer system. Perpetrators face fines and prison sentences of up to 15 years.[19] Lastly, South Africa is considering the development of a **cryptoassets regulatory framework** as crypto becomes increasingly popular in the state.

Conclusion

Heading into 2022, digital transformation, financial inclusion and recovery will continue to shape digital agendas. Growth in digital payments is only set to accelerate, and heightened competition between fintechs and traditional banks will lower costs, simplify transactions, provide consumers more choice and expand access to financial services. CBDC projects will become more fully developed, and they will require countries to further strengthen cybersecurity and data protection frameworks if they have not already. Interest in cryptocurrency will keep rising, especially in states with high inflation, low public confidence in national banking and high remittance volumes. Although many governments, from China to Turkey, have sought to ban cryptoassets, investment has soared unchecked, and states—like Nigeria—may seek to adapt and accommodate, rather than prohibit.

Digitalization initiatives in some jurisdictions, especially the European Union and Asia, will inspire similar efforts elsewhere as governments seek to compete and align with regional and international standards. Although established digital economies like the EU and Northern Asia will dominate headlines and set trends, emerging

markets with incredible fintech growth, such as India, should not be underestimated. Meanwhile, small but wealthy and innovative countries like Bahrain and Denmark are poised to attract new entrants and capture market share.

In closing, momentous change is underway. We have compiled this resource to help you stay informed on important regulatory changes pertaining to digital identity, fraud prevention, data privacy and data protection, and related topics impacting the global financial services sector. We welcome your comments and feedback on how we can improve this valuable report next year.

Endnotes

1 Rappeport, Alan. "The I.M.F. warns of inflation and a slowing recovery as it lowers its forecast." The New York Times, 12 October 2021. https://www.nytimes.com/2021/10/12/business/imf-global-economic-recovery-forecast.html#:~:text=The%20I.M.F.,6%20percent%20projected%20in%20July.&text=Earlier%20this%20year%2C%20the%20I.M.F.

2 Pollari, Ian. "Record-breaking VC investment in fintech in first half of 2021." KPMG, https://home.kpmg/xx/en/home/media/press-releases/2021/08/record-breaking-vc-investment-in-fintech-in-first-half-of-2021.html.

3 "The Global Risks Report 2021." The World Economic Forum. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

4 "Sizing the prize: What's the real value of AI for your business and how can you capitalise?" PwC. https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html.

5 Herrera, Luis et al. "Fintech and Financial Inclusion in Latin America and the Caribbean." IMF eLibrary, 20 August 2021. https://www.elibrary.imf.org/view/journals/001/2021/221/article-A001-en.xml?rskey=KfWRzA&result=97.

6 Santosdlaz, Richie. "In Focus With Fintech and Israel's Fintech-Aviv." The Fintech Times, 24 April 2021. https://thefintechtimes.com/in-focus-with-fintech-and-israels-fintech-aviv/.

7 "Leading countries by research and development (R&D) expenditure as share of gross domestic product (GDP) worldwide in 2021." Statista, February 2021. https://www.statista.com/statistics/732269/worldwide-research-and-development-share-of-gdp-top-countries/.

8 Levanon, Adi. "Israel's maturing fintech ecosystem may soon create global disruptors." TechCrunch, 26 August 2021. https://techcrunch.com/2021/08/26/israels-maturing-fintech-ecosystem-may-soon-create-global-disruptors/.

9 "Share of the population without access to the services of banks or similar organizations worldwide in 2021, by country." Statista, February 2021. https://www.statista.com/statistics/1246963/unbanked-population-in-selected-countries/.

10 Lim, Jamilah. "Asia Pacific shows explosive growth in demand for fintech apps." Tech Wire Asia, 30 June 2021. https://techwireasia.com/2021/06/asia-pacific-shows-explosive-growth-in-demand-for-fintech-apps/.

11 "Pulse of Fintech H1 2021 – ASPAC." KPMG. https://home.kpmg/xx/en/home/insights/2021/08/pulse-of-fintech-h1-21-aspac.html.

12 Mankotia, Atharv. "BFSI – Fintech & Financial Services." Invest India, 05 October 2021. https://www.investindia.gov.in/sector/bfsi-fintech-financial-services.

13 Panda, Subrata. "At 3.5 billion transactions in August, UPI clocks 120% surge in volume." Business Standard, 02 September 2021. https://www.business-standard.com/article/finance/upi-clocks-3-55-billion-transactions-in-august-worth-rs-6-39-trillion-121090100409_1.html.

14 "African Economic Outlook 2021." African Development Bank Group. https://www.afdb.org/en/knowledge/publications/african-economic-outlook.

15 Blokhuis, Veerle. "How COVID-19 has impacted work and poverty in Africa." One, 06 July 2021. https://www.one.org/international/blog/coronavirus-impact-work-poverty-africa/.

16 "Regional Economic Outlook." International Monetary Fund, 15 April 2021. https://www.imf.org/en/Publications/REO.

17 "Internet penetration rate in Africa as of January 2021, by region." Statista, January 2021. https://www.statista.com/statistics/1176668/internet-penetration-rate-in-africa-by-region/.

18 "South Africa." Remitscope. https://remitscope.org/africa/south_africa.

19 Pickworth, Evan. "PODCAST | What are the implications of the recently enacted Cybercrimes and Cybersecurity Act?" Business Day, 02 July 2021. https://www.businesslive.co.za/bd/companies/telecoms-and-technology/2021-07-02-podcast-what-are-the-implications-of-the-recently-enacted-cybercrimes-and-cybersecurity-act/.

North America

The COVID-19 pandemic has accelerated digital transformation in the wealthy and innovative United States and Canada, and both states are eager to develop and adopt disruptive technologies, drive a digitalization-based recovery and bolster cybersecurity. This past year has been an especially progressive year for cybersecurity regulation in the US, as cyberattacks against SolarWinds and Colonial Pipeline exposed vulnerabilities in national cyber resilience. In the wake of the ransomware attack on Colonial Pipeline, President Joe Biden issued his Executive Order on Improving the Nation's Cybersecurity, and he and Deputy National

Security Advisor for Cyber and Emerging Technology Anne Neuberger are launching an anti-ransomware task force. Senators Diane Feinstein (D-CA) and Marco Rubio (R-FL) have proposed legislation to further crack down on ransomware attacks through sanctions and mandatory cybersecurity standards, and cybersecurity is included in the Financial Crimes Enforcement Network's First National AML/CFT Priorities. As cryptocurrency increasingly facilitates fraud and ransomware demand schemes, both American and Canadian legislators and regulators are looking to apply AML/CFT rules to cryptocurrency exchanges and further protect consumers.

Still, the neighbors differ in their attempts to strengthen their respective digital economies. The United States has yet to implement a national digital identity infrastructure or an open banking system, while Canada is slated to launch both. Meanwhile, the Canadian provinces are particularly ambitious in their digitalization initiatives. Alberta, British Columbia, Manitoba, Nunavut, Ontario and Quebec have already adopted provincial digital identities, and many provinces are rushing to institute data protection frameworks and digitalize government services. Similarly, a handful of US states have adopted—or are currently legislating—state data protection frameworks.

Going forward, cybersecurity, artificial intelligence, data privacy, digital identity and digital payments will be major areas to watch in both states.

Country Overview

Wealthy and ambitious Canada, home to the world's ninth-largest economy,[1] is poised for incredible innovation in the financial sector. Venture capital funding for fintech companies is booming, the AI ecosystem is well developed,[2] and the COVID-19 pandemic spurred on increased demand for digital services and products.[3] The government is eager to digitalize its services, strengthen the digital economy and bolster the country's global competitiveness.

Meanwhile, the pandemic drove an increase in the severity of cybersecurity incidents and lent uncertainty to Canada's economic outlook. The average cost of a data breach rose to CAD$6.75 million (approximately USD$5.40 million) per incident in 2020, up from CAD$6.35 million (approximately USD$5.06 million) in 2019.[4] The Canadian government has been slow to respond to the evolving threat landscape, which could hinder its delicate post-pandemic economy recovery. The Canadian economy contracted by 5.4% in 2020, its worst economic performance on record,[5] and the GDP is expected to plunge by a record 12% in the second quarter of 2021.[6] The highly infectious Delta variant could cause further hits to economic growth, but overall financial stability remains strong.

The 2021 national digital agenda focuses on the digitalization of government services, innovation in payments and a potential central bank digital currency (CBDC). An updated data privacy act, introduced in November 2020, has stalled. Provincial governments have been especially progressive in their digitalization efforts. Ontario plans to introduce Canada's first provincial data authority and a trustworthy AI framework, and provinces have flocked to introduce digital IDs and digitalize government services. At the national level, the Pan-Canadian Trust Framework has gone through alpha testing and when launched will positively impact Canada's economy. A key challenge will be ensuring that further digital transformation does not exclude vulnerable populations, especially Indigenous and rural communities. Although digitalization has helped to ensure economic resilience amidst the pandemic, it has widened the country's digital divide.[7] Alongside increasing digitalization, Canadian regulators must also seek to bolster national cybersecurity measures and provide extra support for small and medium-sized entities.[8]

Financial Regulatory Authorities

The **Bank of Canada** is the central bank.

The **Office of the Privacy Commissioner of Canada (OPC)** is the primary data protection authority that supervises and guides individuals and businesses regarding protection of personal information.

The **Office of the Superintendent of Financial Institutions (OSFI)** is an independent agency reporting to the Minister of Finance that acts as the primary authority regulating financial institutions conducting business in Canada.

The **Financial Consumer Agency of Canada (FCAC)** is a federal regulatory agency that assists financial institutions with consumer protection compliance in relation to federal legislation and implementing regulations.

The **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** is Canada's financial intelligence agency that detects and prevents money laundering and terrorist financing.

The **Canadian Securities Administrators (CSA)** is an organization composed of Canada's provincial securities regulators that facilitates effective regulation in the country's capital markets.

Policy, Laws and Regulations

Final Report on Open Banking, 03 August 2021

The Advisory Committee on Open Banking issued its *Final Report*, which details recommendations for the implementation of a national open banking system. Per the report, three pillars must be established for open banking to begin operating:

1. "Common rules for open banking participants to replace the need for bilateral contracts and ensure consumers are protected;
2. An accreditation framework and process to allow third party service providers to participate in an open banking system; and
3. Technical specifications that allow for safe and efficient data transfer and serve the established policy objectives."[9]

The Committee also lists six consumer outcomes that should underpin open banking:

- **“Consumer data is protected**
- **Consumers are in control of their data**
- **Consumers receive access to a wider range of useful, competitive and consumer friendly financial services**
- **Consumers have reliable, consistent access to services**
- **Consumers have recourse when issues arise**
- **Consumers benefit from consistent consumer protection and market conduct standards”[10]**

The Committee supports a speedy approach to the rollout of open banking, with an operational date of January 2023.

Central Bank Paper on the Positive Case for a CBDC, 20 July 2021

The Bank of Canada’s staff discussion paper *The Positive Case for a CBDC* states that a central bank digital currency is “probably necessary” to ensure a competitive digital economy. A CBDC could promote innovation and competition, and would be particularly valuable in “disciplining” the payments market. The authors note two main benefits per this argument: a CBDC could enable new markets and applications, as well as limit “abuses of market power” and avoid “coordination failures in payments and new markets such as for smart contracts.” The two potential scenarios that would motivate the issuance of a CBDC include significantly low national cash use and the widespread adoption of alternate digital currencies, the latter of which is unlikely.

In 2020, the central bank developed four business priorities per its digital transformation strategy, including “advancing work toward a central bank digital currency as a contingency.” The bank’s **Annual Report 2020**, released in April 2021, states that the introduction of a CBDC is not imminent but that it continues to monitor changes in the payments landscape.

Updated ISO 20022 Lynx Message Specifications, 19 July 2021

Payments Canada updated its ISO 20022 message specifications for Lynx, a new real-time gross settlement system as part of Payments Canada’s modernization initiative. “The updated specifications will allow Lynx participants to prepare their existing applications to leverage the value of the ISO 20022 messaging standard. This includes access to enhanced remittance data, support for global interoperability, and improved transparency. Vendors who support Canada’s payments ecosystem can use the published messages to update their applications and develop new services for Lynx participants and the wider ecosystem. The ISO 20022 messages for Lynx also support Canadian financial institutions preparing to meet SWIFT's ISO 20022 migration date for cross-border payments, expected to roll out at the end of 2022." Lynx will go live in 2021.

On 02 March 2021, Payments Canada **announced** that it had chosen Interac Corp. as the exchange solution provider for the Real-Time Rail (RTR), Canada's upcoming real-time payments system. RTR will allow Canadians to initiate and receive payments within seconds, around the clock. It is expected to go live in 2022.

Retail Payments Activities Act Receives Royal Assent, 29 June 2021

Released as part of budget Bill C-30, the Retail Payments Activities Act (RPAA) establishes a new regulatory framework for retail payment activities, applicable to payment service providers (PSPs) whose place of business is in Canada and PSPs outside of Canada whose retail payment activities are directed at individuals or entities in the country. Retail payment activities are defined as payment functions, which involve:

- **"The provision or maintenance of an account that, in relation to an electronic funds transfer, is held on behalf of one or more end users**
- **The holding of funds on behalf of an end user until they are withdrawn by the end user or transferred to another individual or entity**
- **The initiation of an electronic funds transfer at the request of an end user**
- **The authorization of an electronic funds transfer or the transmission, reception or facilitation of an instruction in relation to an electronic funds transfer**
- **The provision of clearing or settlement services"**

The Act seeks to protect consumers, drive innovation and regulate disruptive technologies, and could be instrumental in helping fintech companies to compete with traditional banks. It requires that PSPs register with, submit an annual assessment fee to, and report to the Bank of Canada, which is responsible for oversight and monitoring trends in retail payment activities. PSPs must also develop and implement a risk management and incident response framework, which will be assessed by the central bank, and issue disclosures to end users. Fines up to CAD $10 million (approximately USD$8 million) may be imposed for non-compliance.

FINTRAC Updates Identity Verification Methods, 01 June 2021

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) updated its methods on the identity verification of persons and entities, which went into effect 01 June 2021, per the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The previous guidance included three methods: the government-issued photo identification method, the credit file method and the dual process method. The updated guidance introduces two new methods: the affiliate or member method and the reliance method. The affiliate or member method requires that one of the following has previously identified the person or entity:

- **"An affiliate that is a [reporting entity: "RE"] referred to in any of paragraphs 5(a) to (g) of the PCMLTFA**
- **A foreign affiliate that carries out activities outside of Canada that are similar to the activities of an RE referred to in any of paragraphs 5(a) to (g) of the PCMLTFA**
- **A financial entity that is subject to the PCMLTFA and is a member of your financial services cooperative or credit union central"[11]**

Paragraphs 5(a) to (g) cover reporting entities such as certain authorized foreign banks; certain cooperative credit societies, savings and credit unions; and companies covered by the **Trust and Loan Companies Act**.

The reliance method requires that a person's or entity's identity may be verified through reliance on measures previously taken by:

- **"Another RE (person or entity that is referred to in section 5 of the PCMLTFA)**
- **An entity that is affiliated with you or with another RE and carries out activities outside of Canada that are similar to those of a person or entity referred to in any of paragraphs 5(a) to (g) of the PCMLTFA (an affiliated foreign entity)"[12]**

Digital Operations Strategic Plan: 2021-2024, 24 May 2021

The Canadian government unveiled its *Digital Operations Strategic Plan: 2021-2024*, which outlines priorities toward digitalizing government services, including a "common and secure approach" to digital identity. The report states, "We are on track to launch the OneGC platform, which will allow individuals and businesses to use a single identity and password to access federal government services through a single window on Canada.ca."

In September 2020, the Digital ID & Authentication Council of Canada (DIACC) launched the alpha testing phase of the **Pan-Canadian Trust Framework**, "a set of digital ID and authentication industry standards" seeking to deliver economic benefits across the public and private sectors. The alpha testing phase will also contribute to the introduction of the DIACC PCTF Voila Verified Trustmark Assurance Program ("Voila Verified") in late 2021 or early 2022.[13] The program will issue a PCTF Voila Verified Trustmark to entities in compliance with PCTF standards.[14]

FINTRAC Signs MoU with Society of Notaries Public of British Columbia, 20 May 2021

FINTRAC and the Society of Notaries Public of British Columbia signed a Memorandum of Understanding (MoU) enabling information sharing per compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. The MoU seeks to reduce the "duplication of effort and compliance burden for notaries public in British Columbia." Information to be shared for compliance purposes includes "lists of person and entities subject to their respective Acts and Regulations as well as compliance examination plans resulting in more coordinated and risk-informed examinations."

Financial System Review 2021, 19 May 2021

The Bank of Canada's *Financial System Review 2021* identifies six vulnerabilities in the financial system, including cyberthreats. Digitalization has boosted the attack surface available to cybercriminals, but the bank points to numerous initiatives toward countering cyberthreats, including its 2019-2021 **Cyber Security Strategy** and the **Canadian Financial Sector Resiliency Group** (CFRG). In May 2021, the CFRG led its first cyber incident simulation exercise, which gave its members a chance to practice information sharing and decision coordination in the face of a cyberthreat. The publication follows a 17 May 2021 Bank of Canada **report** on results of the biannual Financial System Survey. Respondents reported that cyber incidents were one of the three main risks to the Canadian financial system.

The report also notes that “the rapid evolution of cryptoasset markets” is an emerging vulnerability. Although the rising popularity in cryptoassets such as Bitcoin and Ethereum does not currently pose a significant threat to Canadian financial stability, this could change if a big tech company were to issue a cryptocurrency. Furthermore, the rapidly evolving and unique nature of cryptoassets presents challenges to the regulatory response. Investor protection issues and the role of cryptoassets in illicit transactions are main regulatory challenges. In December 2020, FINTRAC issued a **guidance** to reporting entities on money laundering and terrorist financing indicators in virtual currency transactions.

FINTRAC Delays Enforcement of Crypto and EFT AML Regulations, 18 May 2021

FINTRAC announced that it would begin assessing reporting entities’ compliance with amended AML regulations on 01 April 2022. The two amended regulations, published in the Canada Gazette on **10 July 2019** and **10 June 2020**, went into force 01 June 2021. Reporting entities must submit a Large Virtual Currency Transaction Report (LVCTR) in the event that they receive a virtual currency transaction of CAD $10,000 (approximately USD$8,000) or more in a single transaction. Reporting entities must also submit an Electronic Funds Transfer (EFT) report in the case that they receive or initiate an international EFT of CAD $10,000 or more in a single transaction. In both instances, the 24-hour rule may apply. FINTRAC expects reporting entities to have implemented their reporting systems no later than 01 December 2021. Unreported LVCTRs and EFTs for the period of 01 June 2021 to 30 November 2021 must be submitted as soon as possible, and no later than 31 March 2022.

Bank of Canada Annual Report 2020, 22 April 2021

The Bank of Canada’s *Annual Report 2020* briefly addresses the bank’s digital transformation strategy. In “cultivating a digital-first culture,” the bank supports the development and adoption of emerging technologies such as intelligent automation, advanced cybersecurity and digital learning. To manage an uncertain future with regard to the evolution of the COVID-19 pandemic, the bank will “increase investments in the risks and opportunities arising from automation and other innovations linked to artificial intelligence.” The bank notes that further digitalization of the economy will be integral to Canada’s post-pandemic recovery.

Legislation

Digital Charter Implementation Act, 17 November 2020

The Minister of Innovation, Science and Industry introduced the Digital Charter Implementation Act, which would enact the Consumer Privacy Protection Act (CPPA) and the Personal Information and Data Protection Tribunal Act (PIPTD). The acts would grant Canadians more control over their personal data; impose new requirements on entities that collect, use and disclose personal data; and impose fines for non-compliance. Under the CPPA, entities must obtain express consent from individuals at or before the time of personal information collection. The following information must be provided for the consent to be valid:

- **The purposes of the collection, use or disclosure of personal information**
- **The way in which personal information is to be collected, used or disclosed**
- **Any reasonably foreseeable consequences that could arise from the collection, use or disclosure of the personal information**
- **The specific type of personal information that is to be collected, used or disclosed**
- **The names of any third parties or types of third parties to which the organization may disclose the personal information**

Individuals have the right to withdraw consent; be informed as to whether an entity has their personal information, how it was used and whether it was disclosed; access their personal information; and request disposal of personal information. Under the PIPTD, the Personal Information and Data Protection Tribunal can impose fines of up to CAD$10,000,000 (approximately USD$8,000,000) or 3% of the entity's gross global revenue, whichever is greater.

On 11 May 2021, the Federal Privacy Commissioner Daniel Therrien sent a **letter** critiquing the bill to the House of Commons Standing Committee on Access to Information, Privacy and Ethics. Therrien notes that the bill would be a "step back overall" and that it is "less protective than laws of other jurisdictions." He commissioned Teresa Scassa, Canada Research Chair in Information Law and Policy at the University of Ottawa, to **assess** the bill's treatment of cross-border transfers of personal information.

Notable Provincial Updates

Amended Quebec Data Protection Act, 11 June 2021

Introduced in the Quebec National Assembly in summer 2020, A*n Act to modernize legislative provisions as regards the protection of personal information* (Bill 64) was amended in parliamentary proceedings, which ended 11 June 2021.[15] The Committee on Institutions, which adopted the bill in February 2021, made several key modifications, including:

- **Personal information may be used without consent when its use is necessary for the supply or delivery of a product or provision of a service, or when its use is necessary for the prevention and detection of fraud or the evaluation and improvement of protection and security measures**
- **The transfer of personal information outside of Quebec must receive "adequate" protection, aligned with "generally accepted data protection principles"**
- **Entities that collect personal information must inform individuals of the "name of the third persons" with whom information may be shared per the collection**
- **Entities must publish detailed information about its personal information governance policies and practices**

Parliament will reconvene in fall 2021. Other provinces have likewise been eager to revamp their data protection frameworks. Alberta **solicited feedback** on the Personal Information Protection Act (PIPA) and the Freedom of Information and Protection of Privacy Act (FOIP). The consultation, which closed 20 August 2021, sought to gather information on enhancing Albertans' data protection rights, bolstering transparency and oversight, and creating legal requirements on the processing of de-identified data.

Quebec Digitalization Law, 10 June 2021

An Act to amend the Act respecting the governance and management of the information resources of public bodies ("The Quebec Act") went into effect. The Act requires all public bodies to develop and implement a digital transformation plan, which will involve the digitalization of Quebec residents' personal information. A digital data manager will be appointed to advise the Executive Council of Quebec on the exchange of government data between various government bodies.[16]

Ontario's **Digital and Data Directive, 2021** similarly seeks to digitalize government services, as well as enable access to public government data.

Building a Digital Ontario: Digital and Strategy, 30 April 2021

Building on the Ontario Onwards Action Plan, Ontario's Digital and Data Strategy aims to make the province a global leader in digital transformation, bolster economic growth and improve people's lives. The strategy outlines plans for a data authority and a trustworthy AI framework. The data authority, which will enter into consultation phase in summer 2021, "will be responsible for building modern data infrastructure to support economic and social growth at scale, while ensuring that data is private, secure, anonymous and cannot identify people individually." The **AI framework**, which was in consultation from 07 May 2021 to 04 June 2021, will hinge on several draft commitments:

- **No AI in secret**
- **AI use Ontarians can trust**
- **AI that serves all Ontarians**

The Ontario government plans to develop and share action plans for each commitment in fall 2021. Its rights-based approach echoes the European Union's proposed Artificial Intelligence Regulation.

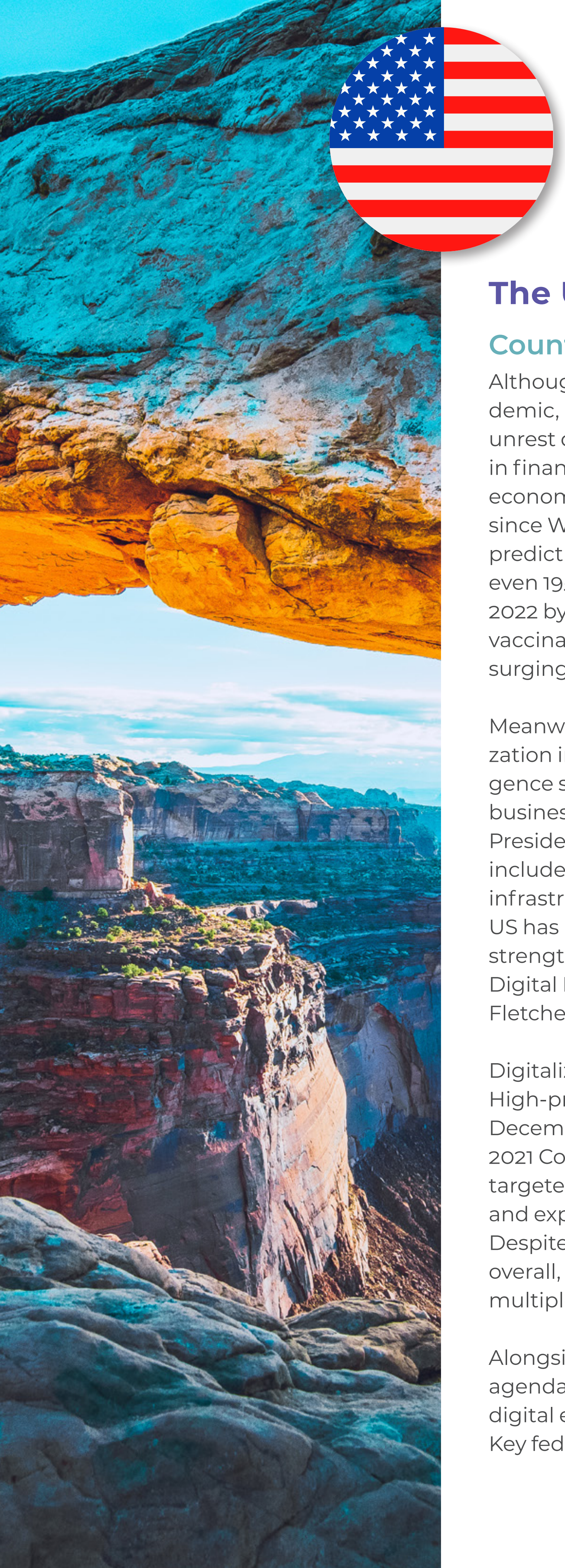
Ontario's Accelerating Access to Justice Act, 19 April 2021

The Accelerating Access to Justice Act received royal assent. The Act enables the permanent witnessing of wills and powers of attorney, and it will also grant courts the power to validate wills that could have otherwise been invalidated due to technical error. The latter provision will go into effect no earlier than 01 January 2022. The Act will retroactively apply to all wills and powers of attorney that fall under the 07 April 2020 emergency order.[17]

Digital ID App Launches in Alberta, Manitoba and Nunavut, 27 January 2021

The eID-Me digital identity mobile application, first launched in Ontario in 2020 by the Ottawa-based company Bluink, was introduced in Alberta, Manitoba and Nunavut. Although the app does not serve as an official Canadian identification, it allows users to verify their identities to access online services and offers a digital backup to driver's licenses and photo ID cards. To register for the app, users must have a passport—either Canadian or American—and a secondary identification such as a driver's license or photo ID card. The app also launched in British Columbia and Quebec in 2020.

Ontario Onwards: Digital Identity Project, 19 October 2020
The Ontario-Onwards: Digital Identity Project, announced by the Office of the Premier, seeks to establish a digital identity infrastructure. Two public consultations have since been held, and the province will begin its introduction of the optional **digital ID** in late 2021. The digital ID can be used by individuals for a variety of services, including to open a bank account, update vaccine records and obtain a birth or death certificate. Businesses can use the digital ID to verify customers' identities, open business accounts and apply for tax credits.



The United States of America

Country Overview

Although the United States has faced the COVID-19 pandemic, economic uncertainty, political upheaval and social unrest during 2020-2021, the country remains a global leader in financial stability and digital transformation. The American economy contracted by 3.5% in 2020, its worst performance since World War II,[18] but a spectacular recovery has experts predicting the strongest economic growth since 1984, or even 1951.[19] The economy is forecasted to expand in 2021 and 2022 by 6.7% and 3.7%,[20] respectively, due in part to a swift vaccination rollout, USD$2.8 trillion in stimulus money, surging demand and a growing jobs market.

Meanwhile, the COVID-19 pandemic has accelerated digitalization in the US, including the adoption of artificial intelligence solutions[21] and digital banking.[22] The digitalization of business operations has driven a rise in productivity,[23] and President Joe Biden's proposed **American Jobs Plan** includes a USD$65 billion budget toward revitalizing digital infrastructure over the next eight years.[24] Although the US has progress to make in bridging the digital divide and strengthening digital skills, it still ranked #2 on the 2020 Digital Evolution Scorecard, developed by Tufts University's Fletcher School and Mastercard.

Digitalization has not come without hurdles, however. High-profile cyberattacks like the 2016 election hacking, December 2020 SolarWinds cybersecurity attack and May 2021 Colonial Pipeline ransomware attack have increasingly targeted American government agencies and businesses and exposed vulnerabilities in national cyber resilience. Despite this worrisome landscape, the US remains strong overall, and the Biden administration is spearheading multiple efforts to further bolster cybersecurity.

Alongside cybersecurity, the United States' 2021 digital agenda seeks to heighten digital inclusion, invigorate the digital economy and counter the rising influence of China. Key federal legislative initiatives address digital identity, data privacy and the regulation of virtual currencies. The Federal Reserve is planning to release a report in September 2021 addressing the opportunities and risks in digital payments, including cryptoassets, stablecoins and a possible central bank digital currency (CBDC).[25] Although the Federal Reserve has been clear that it has no immediate plans to issue a CBDC, Federal Reserve Chair Jerome Powell noted in July 2021 that a CBDC could help to undermine the popularity of privately-issued digital currencies like cryptocurrencies and stablecoins.[26]

State legislatures have similarly been eager to address data protection, as well as enable the digitalization of services like notarization. Colorado and Virginia have joined California in enacting comprehensive data privacy laws, and Massachusetts, New York, North Carolina and Pennsylvania have active bills.[27]

Financial Regulatory Authorities

The **Federal Reserve System** is the central banking system in the US.

The **Consumer Financial Protection Bureau (CFPB)** is an agency of the United States government responsible for consumer protection in the financial sector. Regarding rulemaking and legislation, the CFPB "implements and enforces federal consumer financial laws to ensure that all consumers have access to markets for consumer financial products and services that are fair, transparent, and competitive."

The **Federal Deposit Insurance Corporation (FDIC)** "insures deposits; examines and supervises financial institutions for safety, soundness, and consumer protection; makes large and complex financial institutions resolvable; and manages receiverships."

The **Federal Trade Commission (FTC)** protects consumers and businesses by preventing anticompetitive, deceptive, and unfair business practices. The FTC enforces laws and provides advocacy and education.

The **Financial Crimes Enforcement Network (FinCEN)** is a bureau of the US Department of the Treasury. Its mission is to "safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence."

The **Financial Industry Regulatory Authority (FINRA)** is a government-authorized, not-for-profit organization that acts as a self-regulatory organization overseeing US broker-dealers.

The **National Credit Union Association (NCUA)** is an independent organization that issues charters and serves as regulator for all federal credit unions. In addition, it insures deposits at federally insured credit unions.

The **Office of the Comptroller of Currency (OCC)** is an independent branch of the US Department of the Treasury. The OCC issues charters and serves as regulator for all national banks and federal savings associations. In addition, it supervises federal branches and agencies of foreign banks.

The **Securities and Exchange Commission (SEC)** is an independent federal agency that seeks to prevent market manipulation.

Policy, Laws and Regulations

RFI on Public and Private Sector Uses of Biometric Technologies, 08 October 2021

The Office of Science and Technology Policy (OSTP) issued a Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies. According to the notice, "The purpose of this RFI is to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation."[28] The comment period will end 15 January 2022.

Authentication and Access to Financial Institution Services and Systems, 11 August 2021

The Federal Financial Institutions Examination Council (FFIEC) issued its guidance on *Authentication and Access to Financial Institution Services and Systems*, which details authentication and access risk management principles and practices for digital banking services and information systems. The guidance addresses the following principles and practices:

TOP 3 REGULATORY CONCERNS FOR 2022

47%

FinCEN's forthcoming AML regulations per the Anti-Money Laundering Act of 2020 (AMLA)

49%

Complying with state data privacy regulations

50%

Digital currencies

- **"Conducting a risk assessment for access and authentication to digital banking and information systems**
- **Identifying all users and customers for which authentication and access controls are needed, and identifying those users and customers who may warrant enhanced authentication controls, such as MFA**
- **Periodically evaluating the effectiveness of user and customer authentication controls**
- **Implementing layered security to protect against unauthorized access**
- **Monitoring, logging, and reporting of activities to identify and track unauthorized access**
- **Identifying risks from, and implementing mitigating controls for, email systems, Internet access, customer call centers, and internal IT help desks**
- **Identifying risks from, and implementing mitigating controls for, a customer-permissioned entity's access to a financial institution's information systems**
- **Maintaining awareness and education programs on authentication risks for users and customers**
- **Verifying the identity of users and customers"[29]**

More information on the updated guidance may be found **here**.

Fraud Types and Authentication for Remote Payment Use Cases, 03 August 2021

The Federal Reserve issued *Brief #2: Fraud Types and Authentication for Remote Payment Use Cases* as part of its Fraud Landscape Series. The brief outlines various fraud types, including new account fraud (NAF), NAF based on stolen legitimate identities, NAF based on synthetic identity fraud (SID) and account takeover (ATO). ATO is an increasingly prevalent type of fraud in online payments. According to the brief, "ATO fraud attempts to steal from consumers and e-commerce merchants grew 282% between Q2 2019 to Q2 2020."[30] Fraudsters employ numerous tactics to enable fraud during remote authentication, including data breaches, phishing, malware, attacks-in-the-middle (sometimes referred to as Man-in-the-Middle or MitM) and attacks-in-the-browser (also referred to as Man-in-the-Browser or MitB), and SIM swap attacks. To prevent fraud, authentication methods can be conducted at numerous points in the authentication and verification process. The brief then overviews vulnerabilities and fraud prevention methods pertaining to new account opening and onboarding, person-to-person (P2P) payment authentication for enrollment and transaction, enrollment in contactless mobile and digital wallets, enrollment in payment service provider (PSP) or proprietary merchant wallet and transaction authentication across remote wallets.

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, 28 July 2021

President Joe Biden issued the "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems," which outlines the newly-established Industrial Control Systems Cybersecurity Initiative. The Initiative is a voluntary collaboration between the federal government and the critical infrastructure community aimed at "encouraging and facilitating deployment of technologies and systems that provide threat visibility, indications, detection, and warnings, and that facilitate response capabilities for cybersecurity in essential control system and operational technology networks. The goal of the Initiative is to greatly expand deployment of these technologies across priority critical infrastructure." Although the initiative is voluntary, the Biden administration could seek to make compliance mandatory by entreating Congress to incorporate the standards into federal law.

Social Security Administration's Electronic Consent Based Social Security Number Verification (eCBSV) Service, 19 July 2021

The Social Security Administration (SSA) began its Expanded Rollout of the electronic Consent Based Social Security Number Verification (eCBSV) Service after the Clearance Package was approved by the Office of Management and Budget on 24 June 2021.The eCBSV service enables permitted entities to verify whether an individual's name, birth date and Social Security Number match Social Security records. The service yields a "yes" or "no" match verification. Financial institutions can utilize the eCBSV service during account opening to prevent synthetic identity fraud.

First National Anti-Money Laundering Priorities, 30 June 2021

The Financial Crimes Enforcement Network (FinCEN) issued the first Anti-Money Laundering and Countering the Financing of Terrorism National Priorities per a requirement under the Anti-Money Laundering Act of 2020 (AMLA). The priorities—developed in consultation with federal and state banking regulators, law enforcement and national security agencies, the Department of Treasury and the Attorney General—include:

- **Corruption**
- **Cybercrime, including relevant cybersecurity and virtual currency considerations**
- **Foreign and domestic terrorist financing**
- **Fraud**
- **Transnational criminal organization activity**
- **Drug trafficking organization activity**
- **Human trafficking and human smuggling**
- **Proliferation financing**

Regarding cybercrime, FinCEN notes that, "Treasury is particularly concerned about cyber-enabled financial crime, ransomware attacks, and the misuse of virtual assets that exploits and undermines their innovative potential, including through laundering of illicit proceeds." The internet is also increasingly facilitating fraud like romance scams and identity theft. FinCEN will update the priorities every four years to take into account the evolving threat landscape, and the agency will issue regulations detailing how financial institutions should integrate the priorities into their AML programs. Per AMLA, the regulations must be promulgated by 27 December 2021.

The SSA's eCBSV service was born out of 2019's Economic Growth, Regulatory Relief, and Consumer Protection Act, Section 215, with the purpose of reducing the prevalence of synthetic identity fraud. eCBSV is a valuable service and has benefitted several US banks under the initial pilot, but under the law, it is limited to the financial services industry. The reality is identity fraud, and specifically synthetic identity fraud, is not limited to financial services. Other regulated industries including healthcare and telecommunications could benefit from eCBSV. Further expansion would require an act of Congress and would benefit all Americans and the economy.

Second Circuit Court Ruling on Fintech Charters, 03 June 2021

The Second Circuit Court overturned a 2019 decision to rule that the Office of the Comptroller of the Currency (OCC) could grant special purpose, federal bank charters—“fintech charters”—to non-depository institutions. This will allow for a streamlined and standardized approach to the licensing and regulation of fintech companies across the US. Fintech companies offering certain financial services and products were previously required to obtain a license by each state in which they conducted business.[31]

Executive Order on Improving the Nation’s Cybersecurity, 12 May 2021

President Joe Biden’s Executive Order on Improving the Nation’s Cybersecurity calls for the implementation of several strategies toward bolstering national cybersecurity in the wake of the Colonial Pipeline ransomware attack. The federal government shall partner with the private sector, remove barriers to sharing threat information, modernize its cybersecurity framework, enhance software supply chain security, establish a cyber safety review board, standardize its incident response processes, improve detection of vulnerabilities and incidents on its networks, improve its investigation and remediation capabilities and adopt National Security Systems requirements. Each goal is underpinned by target actions, often to be completed on a rigorous timeline. President Biden states, “It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.” The US ranked #1 on the 2020 Global Cybersecurity Index, developed by the United Nations’ International Telecommunication Union.

Financial Industry Regulatory Authority on Protections from Account Takeover Attempts, 12 May 2021

The Financial Industry Regulatory Authority (FINRA) issued Regulatory Notice 21-18 on practices firms use to protect customers from online account takeover (ATO) attempts. FINRA notes that the prevalence and sophistication of ATOs have risen. The guidance was developed in roundtable discussions with representatives from twenty firms. Practices include:

- **Verifying customers’ identities when they establish online accounts**
- **Authenticating customers’ identities during login attempts**

  - Multifactor authentication
  - Adaptive authentication
  - Supplemental authentication factors such as SMS text message codes, third-party authenticator apps and biometrics
- **Back-end monitoring and controls**
- **Procedures for potential or reported customer ATOs**
- **Automated threat detection**
- **Restoring customer account access**
- **Investor education**

Federal Reserve Board's Proposed Guidelines for Evaluating Account and Services Requests, 05 May 2021

The Federal Reserve Board's Proposed Guidelines for Evaluating Account and Services Requests are intended for use by Federal Reserve Banks "in evaluating requests for master accounts and/or access to Federal Reserve Bank financial services (accounts and services)." Technological change has driven a shifting payments landscape and the advent of new financial products and services, and banks are increasingly receiving "requests for access to accounts and services from novel institutions" such as fintech companies. The Federal Reserve Board thus seeks to promote a transparent and standardized response to the requests, outlined in the proposed guidelines. The five guidelines are founded on risk management and mitigation. In evaluating requests, banks must ensure that:

- **Institutions are eligible to "maintain an account at a Federal Reserve Bank (Reserve Bank) and receive Federal Reserve services"**
- **The provision of an account and services will not pose undue risks related to operations, credit, settlement and cybersecurity**
- **The provision of an account and services will not pose undue risks related to operations, credit, liquidity and cybersecurity to the overall payment system**
- **The provision of an account and services will not pose undue risk to the stability of the financial system**
- **The provision of an account and services will not pose "undue risk to the overall economy by facilitating activities such as money laundering, terrorism financing, fraud, cybercrimes, or other illicit activity"**

The Board called for public feedback on its proposed guidelines.

TOP COMPLIANCE TECHNOLOGIES FOR US BANKS

49%

Digital remote identity verification

(i.e., technologies allowing the verification of identity of natural or legal persons online)

46%

Classic biometrics

(e.g., voice, face, fingerprint)

41%

Application shielding

Synthetic Identity Fraud Definition, 06 April 2021

The Federal Reserve announced that an industry-recommended definition of synthetic identity fraud had been developed by a focus group of twelve fraud experts. "Synthetic identity fraud (SIF) is the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain." Primary elements of PII include name, date of birth and Social Security number, as well as other government-issued identifiers, and secondary elements of PII include address, phone number, email address and digital footprint. Synthetic identities can be used for credit repairs, fraud for living, payment default schemes and other illegal activities.

FinCEN Regulatory Process for Beneficial Ownership Reporting Requirement, 01 April 2021

FinCEN issued an Advance Notice of Public Rulemaking (ANPRM) inviting public feedback on procedures and standards pertaining to a requirement that reporting companies submit information on their beneficial owners, per the implementation of the Corporate Transparency Act (CTA). Reporting companies must submit to FinCEN information on each identified beneficial owner and applicant, including "(i) Full legal name; (ii) date of birth; (iii) current residential or business street address; and (iv) a unique identifying number from an acceptable identification document or the individual's FinCEN identifier." Per the CTA, FinCEN must keep the reported information in a secure, non-public database for five years upon termination of the reporting company, and the unauthorized disclosure of the information is prohibited. FinCEN must also provide a "FinCEN identifier" to entities or individuals who have submitted their beneficial ownership information, upon request. According to the notice, "A FinCEN identifier is to be a unique identifier for each individual or entity that may be used for subsequent reporting to FinCEN in lieu of providing certain other information."

Request for Information on Artificial Intelligence, 31 March 2021

The Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration and Office of the Comptroller of the Currency issued a request for information (RFI) on financial institutions' use of artificial intelligence, including machine learning. The RFI seeks "to understand respondents' views on the use of AI by financial institutions in their provision of services to customers and for other business or operational purposes; appropriate governance, risk management, and controls over AI; and any challenges in developing, adopting, and managing AI." The deadline for comments was 01 July 2021.

American regulators have demonstrated increasing interest in the adoption of AI, alongside the mitigation of its risks. On 19 March 2021, the National Security Commission on Artificial Intelligence published a **Final Report** outlining a strategy to "win the broader technology competition" in the "AI era." On 19 April 2021, the Federal Trade Commission (FTC) published a **blog** on "Aiming for truth, fairness, and equity in your company's use of AI," which delivers guidance on avoiding negative outcomes like racial bias.

The financial services industry continues to utilize Artificial Intelligence to improve customer experience and reduce costs. The expanded use of AI and documented bias in algorithms has made AI a high priority for US financial regulators and policymakers. The regulators' RFI was one of many initiatives this year.

In April the FTC published a blog post, "Aiming for truth, fairness, and equity in your company's use of AI". The regulator warns developers and users of AI that exaggerating or misleading consumers will put companies in the crosshairs of the FTC citing potential enforcement action under the FTC Act, the Fair Credit Reporting Act, and Equal Credit Opportunity Act.

Bias in artificial intelligence systems and machine learning and the algorithms these systems employ can negatively affect, or harm, people's lives. In the delivery of financial services in particular, AI- or ML-caused harms include allocation and quality of service harms. Allocation harms consist of offering or withholding opportunities, resources, or information from certain sub-populations – for example differing loan approval rates for males vs. females. Quality-of-service harms occur when a system's accuracy or performance differs for certain subpopulations – for example, facial recognition/comparison systems with higher error rates for Black women.

At the same time, applying AI/ML to financial services use cases can also mitigate inequities, advance inclusion, improve the user experience, and protect people against fraud. For example, ID verification technology powered by AI/ML can extend financial service offerings to subpopulations whose credit scores might disqualify them via traditional means. In addition, applying machinelearning to session-monitoring and fraud analysis for digital financial services helps reduce unnecessary authentication friction to improve user experiences and more accurately detect and interdict fraud.

In June, NIST released Draft Special Publication 1270, “A Proposal for Identifying and Managing Bias in Artificial Intelligence”. The report, “proposes a strategy for managing AI bias, and describes types of bias that may be found in AI technologies and systems. The proposal is intended as a step towards consensus standards and a risk-based framework for trustworthy and responsible AI”.

In July, NIST published a Request for Information (RFI) to solicit input as it drafts an Artificial Intelligence Risk Management Framework, a “guidance document for voluntary use intended to help technology developers, users and evaluators improve the trustworthiness of AI systems.”

2022 is certain to be a very interesting year as it pertains to the regulatory environment for AI and we will be closely tracking activities in Washington, DC.

Office of the Comptroller of the Currency Approves Banks’ Use of Blockchain and Stablecoins in Payments, 04 January 2021

The Office of the Comptroller of the Currency (OCC) issued an interpretive letter approving banks’ use of independent node verification networks (INVN) and stablecoins in payment activities. The letter notes that, “Industry participants recognize that using stablecoins to facilitate payments may combine the efficiency and speed of digital currencies with the stability of existing currencies…stablecoins can provide a means of transmitting value denominated in an existing currency using INVN technology. Stablecoins thus provide a means by which participants in the payment system may avail themselves of the potential advantages associated with INVNs. Billions of dollars’ worth of stablecoin trade globally, and demand for stablecoin continues to grow. INVNs and related stablecoins represent new technological means of carrying out bank-permissible payment activities. We therefore conclude that a bank may validate, store, and record payments transactions by serving as a node on an INVN. Likewise, a bank may use INVNs and related stablecoins to carry out other permissible payment activities. A bank must conduct these activities consistent with applicable law and safe and sound banking practices.”

FinCEN’s Proposed Rule on Virtual Currency and Digital Asset Transactions, 18 December 2020

FinCEN issued a notice of proposed rulemaking to solicit public feedback on “Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets.” The proposed rule seeks to address anti-money laundering regulatory gaps, and would "require banks and money service businesses ('MSBs') to submit reports, keep records, and verify the identity of customers in relation to transactions involving convertible virtual currency ('CVC') or digital assets with legal tender status ('legal tender digital assets' or 'LTDA') held in unhosted wallets...or held in wallets hosted in a jurisdiction identified by FinCEN." An unhosted wallet is one that is controlled by an individual in lieu of an intermediary. Banks and MSBs must file a report with FinCEN in the case of a transaction exceeding USD$10,000 (or a series of transactions amounting to the same within a 24-hour period), and banks and MSBs must maintain records in the case of a transaction exceeding USD$3,000.

On 06 July 2021, FinCEN appointed its **first-ever** Chief Digital Currency Advisor, Michele Korver.

Legislation

Sanction and Stop Ransomware Act of 2021, 05 August 2021

Introduced by Senators Diane Feinstein (D-CA) and Marco Rubio (R-FL), the Sanction and Stop Ransomware Act of 2021 aims to strengthen national cybersecurity through the development of mandatory cybersecurity standards, the regulation of cryptocurrency exchanges, sanctions and reporting requirements. If passed, the Act would require the Department of Homeland Security (DHS) Secretary—in consultation with the Director of the Cybersecurity and Infrastructure Security Agency (CISA)—to issue mandatory cybersecurity standards, applicable to critical infrastructure entities. Within 180 days, the Secretary of Treasury would issue regulations for cryptocurrency exchanges "in order to reduce anonymity of accounts and users suspected of ransomware activity and make records available to the US government in connection with ransomware incidents."[32] Ransomware threats to critical infrastructure would be classified as a national intelligence priority, and states found to have provided support to ransomware demand schemes would be classified as a "state sponsor of ransomware." Such states would face sanctions and penalties, to be issued by the President. Lastly, the Act directs CISA to establish a ransomware operation reporting system within 180 days.

SAFE DATA Act, 28 July 2021

Introduced by Senators Roger Wicker (R-MI) and Marsha Blackburn (R-TN), the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act aims to give Americans more control over their data and bolster businesses' transparency and accountability. Consumers would be granted the rights to access, correct, delete and port their data. Businesses would have to obtain consent for the processing or transferring of sensitive data, and would be limited in undertaking secondary uses of data without consent. Businesses would also have to "disclose a privacy policy to consumers detailing their data collection, processing, and transfer activities, and notify consumers of any material changes to those activities;"[33] conduct privacy impact assessments; and secure data through the maintenance of internal controls and reporting structures. The Federal Trade Commission (FTC) would be required to maintain a data broker registry and share information with the relevant agency "if it obtains information that a business has processed or transferred consumer data in a way that violates Federal anti-discrimination laws."[34] The FTC would also be authorized "to develop new rules to expand categories of sensitive data"[35] and its authority in overseeing data use practices of nonprofits and common carriers would be expanded.

Digital Asset Market Structure and Investor Protection Act, 28 July 2021

Introduced by Representative Don Beyer (D-VA), the Digital Asset Market Structure and Investor Protection Act seeks to "protect consumers and promote innovation by incorporating digital assets into existing financial regulatory structures." The **bill** would:

- **Establish statutory definitions for digital assets and digital asset securities**
- **Grant the Federal Reserve the authority to issue a CBDC**
- **Include digital assets and digital asset securities under the statutory definition of "monetary instruments"**
- **Direct regulators to issue consumer advisories to ensure that consumers are aware their digital assets and digital asset securities are not "insured or protected in the same way as bank deposits or securities"**
- **"Require digital asset transactions that are not recorded on the publicly distributed ledger to be reported to a registered Digital Asset Trade Repository within 24 hours to minimize the potential for fraud and promote transparency"**

Cyber Incident Notification Act, 21 July 2021

The bipartisan Cyber Incident Notification Act—introduced by Senators Susan Collins (R-ME), Marco Rubio (R-FL) and Mark Warner (D-VA)—would require federal government agencies, federal contractors and critical infrastructure operators to report "cybersecurity intrusions" and "potential cybersecurity intrusions" to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) within twenty-four hours of discovery. A cybersecurity intrusion is defined as an incident that involves or is assessed to involve a nation-state, an advanced persistent threat actor or a transnational organized crime group, as well as one that may result in "demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of people in the United States; is or is likely to be of significant national consequence; or is identified by covered entities but affects, or has the potential to affect, agency systems." Reports must include a description of the incident; a description of tactics employed by the actor in conducting the attack; vulnerabilities leveraged; information that could help in identifying the cyber actor; and contact information of the reporting entity.

Improving Digital Identity Act of 2021, 30 June 2021

Representatives Bill Foster (D-IL), John Katko (R-NY), Jim Langevin (D-RI) and Barry Loudermilk (R-GA) reintroduced the Improving Digital Identity Act of 2021, which seeks to establish a government framework for a nationwide digital identity. The bill notes the rise of identity theft and identity fraud in the US, which is in part facilitated by the lack of an affordable and reliable identity verification method for online activities. If enacted into law, the bill would establish an Improving Digital Identity Task Force under the Executive Office of the President. The task force would be charged with creating a "governmentwide effort to develop secure methods for Federal, State and local agencies to validate identity attributes to protect the privacy and security of individuals and support reliable, interoperable digital identity verification in the public and private sectors." Toward this end, the task force would evaluate restrictions in an agency's ability to verify identity information; evaluate necessary regulatory changes in relation to such restrictions; recommend a standards-based architecture allowing for agencies to provide digital identity verification services; identify funding and additional resources required by agencies in the provision of digital identity verification; and evaluate potential risks associated with criminal exploitation of digital identity verification. Additionally, the Director of the National Institute of Standards and Technology (NIST) would be tasked with developing a digital identity standards framework, and the Secretary of Homeland Security would award grants to states to upgrade systems providing identity credentials.

In a 27 May **speech**, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger briefly addressed security in devising digital identity standards, saying, "...are there commercial ways for digital identity so that we can ensure both devices and people have [security,] particularly when they want to have authenticated identity online."

> The inadequacy of our identity infrastructure remains a major challenge in financial services: FinCEN last year reported banks are losing more than $1 billion each month due to identity-related cybercrime. Meanwhile, millions of Americans cannot get a bank account because they don't have the foundational identity documents needed to prove who they are. Amidst all of this, identity theft losses soared by 42% last year.
>
> On the cybersecurity front, it remains an anomaly when a major incident occurs and identity does not provide the attack vector. The SolarWinds attack several months ago was just the latest example of this, with Russian attackers targeting the administrative layer of identity and access management systems to do devastating damage. As a leader at the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security stated back in March, "Identity is everything now."

JEREMY GRANT, BETTER IDENTITY COALITION
WRITTEN TESTIMONY FOR THE US HOUSE FINANCIAL SERVICES COMMITTEE, TASK FORCE ON ARTIFICIAL INTELLIGENCE, HEARING "I AM WHO I SAY I AM: VERIFYING IDENTITY WHILE PRESERVING PRIVACY IN THE DIGITAL AGE" JULY 16, 2021

Data Protection Act of 2021, 17 June 2021

Senator Kirsten Gillibrand (D-NY) reintroduced the Data Protection Act of 2021, which would establish a federal Data Protection Agency (DPA). The DPA would establish and enforce data protection rules, ensure "fair competition within the digital marketplace", advise Congress on the privacy and technology landscapes, coordinate with federal and state regulators in supporting a consistent regulatory approach to privacy issues and ensure that "high-risk data privacy practices" do not discriminate against a protected class. The bill has a heavy focus on justice and would establish an Office of Civil Rights as part of the DPA. Senator Gillibrand has been particularly adamant in bolstering privacy protections against big tech companies, and the bill allows for the DPA to review company mergers that involve the transfer of data of 50,000 or more individuals.

The reintroduction of the Data Protection Act of 2021 follows the 29 April 2021 reintroduction of the **Consumer Data Privacy and Security Act** by Senator Jerry Moran (R-KS). The Act would strengthen consumer data protections and impose new requirements on entities that handle consumer data. Entities handling consumer data would be required to develop and implement security programs safeguarding personal data, consumer consent would be required for the collection of data and consumers would have the rights to access, correct and erase their personal data.

Securing and Enabling Commerce Using Remote and Electronic Notarization Act, 13 May 2021

The bipartisan Securing and Enabling Commerce Using Remote and Electronic (SECURE) Notarization Act, reintroduced by Senator Kevin Cramer (R-ND), would authorize all notaries in the US to perform remote online notarizations (RONs) through the use of audio-visual communication and recording. The bill outlines definitions, requirements and standards for conducting RONs, such as the retention of the audio-visual recording of the performance of a RON for a period of at least five years, or ten in some cases. The notary must utilize at least two types of processes or services "through which a third party provides a means to verify the identity of the remotely located individual through a review of public or private data sources", and the electronic signature must be affixed to the electronic record in such a way that tampering is "evident." Notaries may perform notarizations that affect interstate commerce. Due to business operations shifting online as a result of the COVID-19 pandemic, states have increasingly passed laws enabling RONs, both temporarily and permanently.

Token Taxonomy Act of 2021, 08 May 2021

Representative Warren Davidson (R-OH) introduced the Token Taxonomy Act, which aims to "exclude digital tokens from the definition of a security" in an effort to strengthen regulatory clarity. Cryptoassets would need to meet several requirements to qualify as a digital token, which is defined per the Act as a "digital unit (A) that is created (i) in response to the verification or collection of proposed transactions; (ii) pursuant to rules for the digital unit's creation and supply that cannot be altered by any single person or persons under common control; or (iii) as an initial allocation of digital units that will otherwise be created in accordance with clause (i) or (ii)." The digital unit must also have a transaction history recorded in a distributed digital ledger or digital data structure, the consensus of which cannot be modified or tampered with by a single person or group; it must be transferable without the means of an intermediary; and it cannot be a "representation of a financial interest in a company or partnership." The bill also introduces small taxation adjustments, including the creation of a tax exemption for the exchange of a virtual currency into another; "a de minimus exemption from taxation for gains realized from the sale or exchange of virtual currency for other than cash;" and an adjustment to the "taxation of virtual currencies held in individual retirement accounts."

Eliminate Barriers to Innovation Act of 2021, 20 April 2021

The House of Representatives passed the Eliminate Barriers to Innovation Act of 2021, first introduced by Representative Patrick T. McHenry (R-NC) on 08 March 2021. The Act would establish a digital assets working group between the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) in an effort to create an integrated approach to the regulation of digital assets. The working group would be composed of employees from both agencies as well as at least one representative from six categories, including:

- **"Financial technology companies providing digital assets**
- **Financial firms under the jurisdiction of the SEC or CFTC**
- **Institutions or organizations engaged in academic research or advocacy on digital assets**
- **Small businesses engaged in financial technology**
- **Investor protection organizations**
- **Institutions and organizations that support investment in historically-underserved businesses"**

and **Canada**

Within a year of its establishment, the working group would have to supply a report addressing the legal and regulatory frameworks pertaining to digital assets, with an analysis of how a lack in clarity has affected primary and secondary markets in digital assets, how the frameworks affect US competitiveness and how developments in other countries related to digital assets affect US competitiveness. The report must then deliver recommendations on the creation, maintenance and improvement of primary and secondary markets in digital assets with regard to strengthening fairness, transparency and integrity; standards on cybersecurity, custody and private key management; best practices on reducing fraud and market manipulation; and best practices on bolstering investor protections and assisting in AML/CFT compliance measures. As of the publication of this report, the bill is in the Senate Banking, Housing, and Urban Affairs Committee.

Bank Service Company Examination Coordination Act, 26 March 2021

Introduced by Representative Roger Williams (R-TX), the Act was introduced and referred to the Committee on Financial Services and the Committee on the Budget. The Act seeks to amend the Bank Service Company Act and would enable the coordination of state and federal banking agencies—with particular regard to information sharing—in overseeing and regulating activities of third-party service providers, referred to as bank service companies. Enhanced cooperation would help to more efficiently detect vulnerabilities in the financial system and promote a more consistent approach to oversight and regulation.

Stablecoin Tethering and Bank Licensing Enforcement Act, 02 December 2020

The Stablecoin Tethering and Bank Licensing Enforcement (STABLE) Act, introduced by Representative Rashida Tlaib (D-MI), seeks to protect consumers against financial threats related to cryptocurrency. The Act would require stablecoin issuers to notify and acquire a written approval from the Federal Reserve, Federal Deposit Insurance Corporation and the relevant state or federal banking agency. These agencies would be required to conduct an ongoing risk analysis with regard to monetary policy. Stablecoin issuers would have to ensure that they could “immediately redeem all outstanding stablecoins at their nominal redemption value, upon demand, in United States dollars.”

Although the bill was introduced shortly before the close of the previous congressional session, it is expected to be reintroduced in 2021.[36]

Notable State Laws and Bills

New Hampshire Adopts Remote Online Notarization, 10 August 2021

The New Hampshire legislature enacted SB 134, which adopts RON effective 06 February 2022. New Hampshire joins 36 other states that have also enacted permanent RON measures, including Alaska, Arizona, Arkansas, Colorado, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Mexico, New Jersey, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin and Wyoming. States began to adopt RON measures as the COVID-19 pandemic led to social distancing rules and forced businesses to shift their operations online. Each state's measures include the same basic elements, including the use of audio-visual communication methods, recording of the audio-visual communication and authentication by the notary of the signatory.[37] The following states enacted RON measures in 2021:

On 22 July 2021, New Jersey Governor Phil Murphy signed **A 4250**, which adopts RON effective 21 October 2021.

On 23 June 2021, Maine enacted **HP 1033**, which temporarily extends an executive order enabling RONs until 01 January 2023. HP 1033 also tasks the Secretary of State with conducting a study on RONs, developing recommendations on permanent RON measures and submitting a report to the state legislature by 01 February 2022.

On 15 June 2021, Oregon Governor Kate Brown signed **SB 765**, which makes temporary RON measures permanent. The law went into immediate effect.

On 29 April 2021, Arkansas Governor Asa Hutchinson signed **SB 340** (Act 1047) into law. The law went into immediate effect, retroactive to 30 March 2020.

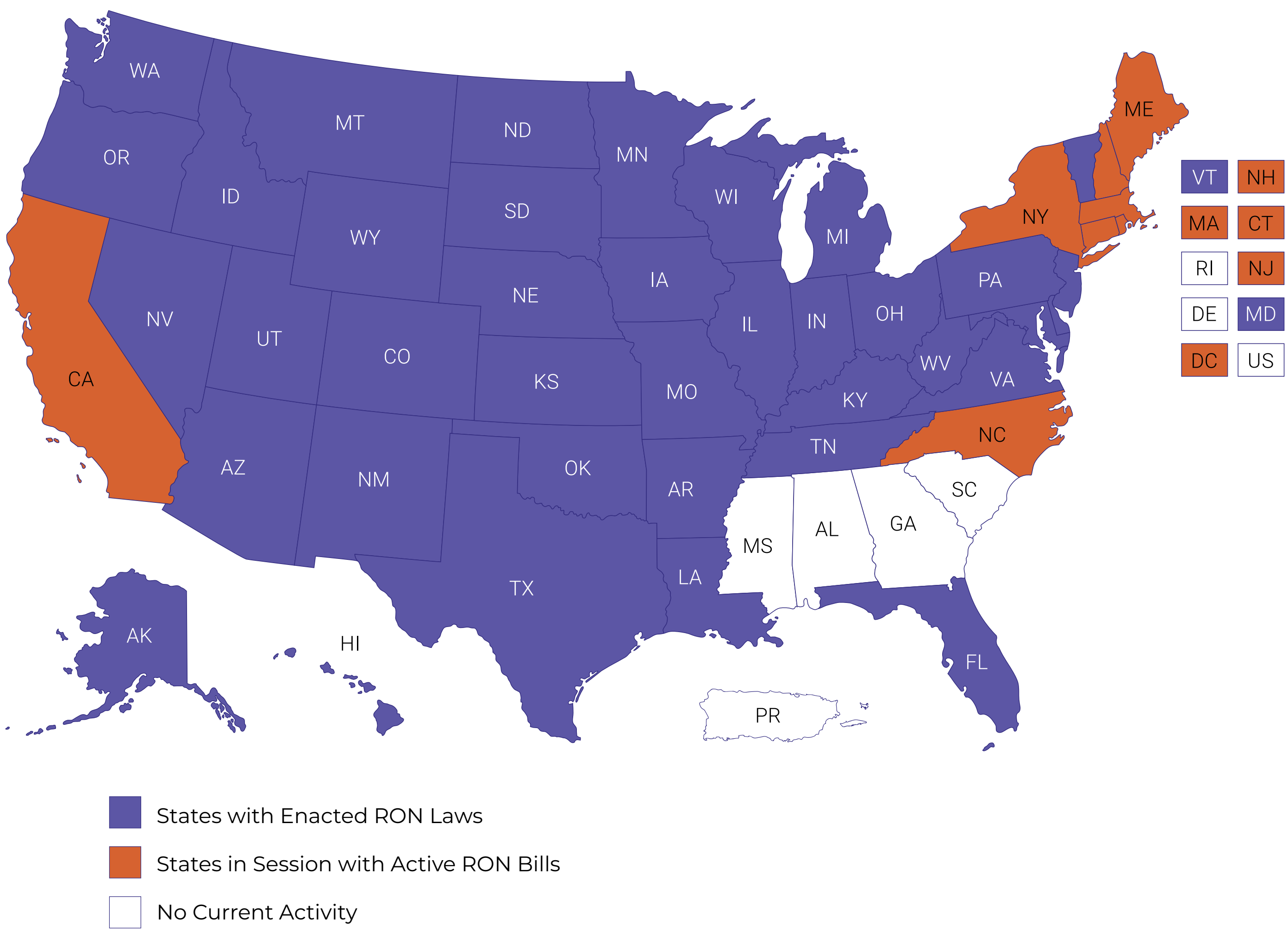
On 21 April 2021, Kansas Governor Laura Kelly **SB 106** into law. The law will go into effect 01 January 2022.

On 05 April 2021, New Mexico Governor Lujan Grisham signed **SB 12** into law. The law will go into effect 01 January 2022.

On 30 March 2021, West Virginia Governor Jim Justice signed **SB 469** into law. The law went into effect 17 June 2021.

On 26 February 2021, Wyoming Governor Mark Gordon signed **SF 0029** into law. The law went into effect 01 July 2021.

On 23 January 2021, Illinois Governor J.B. Pritzker signed **SB 2664** into law. The law will go into effect 01 January 2022.



Source: As of 24 August 2021. Mortgage Bankers Association.
Please visit the Mortgage Bankers Association's remote online notarization (RON) resource page (www.mba.org/RON) for the most current legislative tracking map and other information on the status of RON legislation in the states.

State Insurance Cybersecurity Laws

In October 2017, the National Association of Insurance Commissioners (NAIC) adopted the NAIC Insurance Data Security Model Law. According to the NAIC, the Model Law "seeks to establish data security standards for regulators and insurers to mitigate the potential damage of a data breach. The law applies to insurers, insurance agents and other entities licensed by the state department of insurance."

Moreover, the US Treasury Department has advised states to adopt the Model Law within the next 5 years or the department will ask Congress to preempt the states. While each state can modify the Model Law to accommodate its unique requirements, key components of the Model Law include requiring insurance licensees to implement a written information security program and for insurance licensees to consider whether certain safeguards are appropriate, including access controls such as multi-factor authentication, penetration testing, encryption, audit trails and other security methods.

At the time of this writing, 18 states have adopted the NAIC Model Law: Alabama, Connecticut, Delaware, Hawaii, Indiana, Iowa, Louisiana, Maine, Michigan, Minnesota, Mississippi, New Hampshire, North Dakota, Ohio, South Carolina, Tennessee, Wisconsin and Virginia.

Laws passed in 2021 include:

The Wisconsin Insurance Cybersecurity Law, signed by Governor Tony Evers on 16 July 2021. It will go into effect 01 November 2022.

Hawaii's **Insurance Data Security Law**, signed by Governor David Ige on 28 June 2021. It went into effect 01 July 2021. Licensees must be in compliance with the majority of information security program requirements by 01 July 2022, and be in compliance with third-party service provider oversight requirements by 01 July 2023.[38]

Minnesota's commerce and energy omnibus bill, signed by Governor Tim Walz on 26 June 2021, includes provisions based on the NAIC Model Law. It went into effect 01 August 2021. Licensees must be in compliance with the majority of information security program requirements by 01 August 2022, and be in compliance with third-party service provider oversight requirements by 01 August 2023.[39]

The **Tennessee Insurance Data Security Law**, signed by Governor Bill Lee on 06 May 2021. It went into effect 01 July 2021.

The **Iowa Insurance Data Security Act**, signed by Governor Kim Reynolds on 30 April 2021. It will go into effect 01 January 2022.

The **North Dakota Insurance Data Security Act**, signed by Governor Doug Burgum on 24 March 2021. It will go into effect 01 August 2022. The requirement to report and document cybersecurity incidents and responses will go into effect 01 August 2023.

The **Maine Insurance Data Security Act**, signed by Governor Janet Mills on 17 March 2021. It will go into effect 01 January 2022. Requirements on the use of third-party service providers will go into effect 01 January 2023.

Biometric Privacy in New York City Administrative Code, 09 July 2021

Although New York's Biometric Privacy Act was not passed, New York City incorporated rules on biometric identity identification into the New York City Administrative Code. Per the code, "Any commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable." The code deems it illegal to profit from the transaction of biometric identifier information. In the case that a person faces a violation of the rules, they may send written notice to the establishment, which will have thirty days to remedy the violation and provide an "express written statement" to the aggrieved person. If the establishment continues to violate the rules, the aggrieved person may initiate an action against the establishment. The new rules went into effect 09 July 2021.

NYDFS Ransomware Guidance, 30 June 2021

In light of the increasing prevalence of ransomware attacks, the New York State Department of Financial Services (NYDFS) issued a Ransomware Guidance to New York State regulated entities. Regulated entities should institute email filtering anti-phishing training, a "documented program to identify, assess, track, and remediate vulnerabilities on all enterprise assets within their infrastructure," multi-factor authentication (MFA) and a method to monitor systems for intruders. Regulated entities should also disable RDP access, ensure that strong passwords are used and develop an incident response plan. In the case that a ransomware attack is successful, regulated entities must report it to the NYDFS within 72 hours.

Colorado Privacy Act, 07 June 2021

The Colorado Privacy Act (CPA), signed into law by Governor Jared Polis, makes Colorado the third state to enact a comprehensive privacy regime, after California and Virginia. Once in effect, Colorado residents will be granted greater control over their personal data, including the rights to access, correct and delete personal data, as well as the right to opt out of the processing of personal data in the cases of targeted advertising, sale of personal data and profiling. The law will go into effect 01 July 2023.

Virginia's **Consumer Data Protection Act** was signed into law 02 March 2021. The law will apply to all entities that conduct business in the state and either control or process the personal data of at least 100,000 people, or garner over 50% of gross revenue from the sale of personal data while controlling or processing the personal data of at least 25,000 people. Consumers will be granted the rights to access, correct, delete and obtain a copy of their personal data. The law will go into effect 01 January 2023.

The **California Privacy Rights Act of 2020** (CPRA), passed 03 November 2020 by a majority of California voters in the general election, echoes the EU's General Data Protection Regulation (GDPR) and significantly expands consumer rights. Consumers will have the rights to correct inaccurate personal data, opt out of the sale and sharing of personal data and request limits on the use and disclosure of sensitive personal information (SPI). The newly made SPI category includes such data as genetic data, biometric information, social security, financial information, race, ethnicity, religion, personal communications and more.[40] The law also creates a new enforcement agency. The California Privacy Protection Agency (CPPA) will be tasked with rule-making and guidance, with a budget of USD$10 million. On 19 March 2021, California **announced** the appointment of five board members to the CPPA. The law will go into effect 01 January 2023.

(i.e., techniques that make it harder for hackers to break phone apps)

38%

of US banks report challenges aligning technology roadmaps with compliance needs

Meanwhile, legislatures in Massachusetts, New York, North Carolina, Ohio and Pennsylvania are contemplating their own privacy frameworks. The Ohio Personal Privacy Act (OPPA), introduced 13 July 2021, would grant consumers the rights to access, delete, obtain a copy and opt out of the sale of their personal data. The Act would apply to businesses that generate at least USD$25 million in gross annual revenue in Ohio; control or process the personal data of at least 100,000 Ohio consumers; and that control or process the personal data of at least 25,000 Ohio consumers while garnering at least 50% of its gross annual revenue from the sale of personal data.[41]

The **New York Privacy Act** (NYPA), reintroduced by Senator Kevin Thomas on 13 May 2021, would strengthen consumer protections and impose requirements on certain data controllers. Obliged entities would include legal persons that conduct business in New York or sell services and products marketed towards New York residents, and meet one of a number of criteria. The criteria include entities that generate an annual gross revenue of USD$25 million or greater; control or process the personal data of 100,000 or more New York residents; control or process the personal data of 500,000 or more individuals in the US, of whom at least 10,000 are New York residents; and garner over half of gross revenue from the sale of personal data, while controlling and processing the personal data of at least 25,000 New York residents. Consumers would be granted the rights to be given notice of how their personal data is processed; to give or not give consent to the processing of their personal data; and to delete, correct and access their personal data. Data controllers would have to provide a notice to consumers detailing how their personal data is to be processed, utilizing language at or below an 8th-grade reading level.

On 07 April 2021, Pennsylvania's **Consumer Data Privacy Act** (CDPA) was introduced in the State House of Representatives. The Act would grant consumers the rights to access and delete their personal information; know whether their personal data is being collected, sold or disclosed; and decline or opt out of the sale of their personal information. Data collectors would be required to disclose information to the consumer regarding the category of personal data collected, the purpose of collection or sale and categories of third parties with which the data is shared.

On 06 April 2021, the **Consumer Privacy Act of North Carolina** (CPA) was introduced in the State Senate. The CPA would grant consumers the rights to access, correct and delete their personal data, as well as confirm whether it is being processed and opt out of the processing of personal data for the purposes of targeted advertising, sales and profiling. Data controllers would be required to comply with consumer requests in the exercise of their rights, disclose to the consumer the purpose of personal data collection, issue a privacy notice to consumers regarding their rights and the purpose of the personal data processing, conduct an annual data protection assessment and collect only the personal data that is "adequate, relevant and reasonably necessary"[42] for the prescribed purpose. Data controllers may not process sensitive personal data without consent. Data controllers who violate the CPA could face fines up to USD$5,000.

On 29 March 2021, **The Massachusetts Information Privacy Act** (MIPA) passed to the State Senate. MIPA would protect people from the unauthorized collection, use and sale of their personal data, especially biometric information; establish the Massachusetts Information Privacy Commission; protect employees from "unwarranted electronic monitoring" while working; and prohibit digital discrimination. The **MIPA Fact Sheet** states that the Act aims to "Blend the best approaches from other states and jurisdictions, including parts of similar laws passed in California, Illinois, and the European Union."

Sixteen other states have introduced data protection legislation but have failed to pass them. On 19 July 2021, the Uniform Law Commission (ULC) issued the **Uniform Personal Data Protection Act** in an effort to standardize data protection legislation across the states.

Nebraska Financial Innovation Act, 25 May 2021

The Nebraska Financial Innovation Act, introduced 20 January 2021, was passed and signed into law. The law establishes a charter for companies holding cryptocurrencies and creates a new class of financial institution and bank, called a "digital asset depository institution." Banks that already have a charter can offer cryptocurrency services. The law notes that institutions are expected to comply with national and state laws on know-your-customer (KYC), anti-money laundering and other requirements.

Oklahoma Electronic Title (e-Title) Law, 07 May 2021

Governor Kevin Stitt signed Senate Bill 998 into law, making Oklahoma the 25th state to enact legislation enabling the use of electronic titles and liens for vehicles.[43] The law will go into effect 01 November 2021. The Oklahoma Tax Commission (OTC) has been tasked with developing a program for the electronic storage and filing of motor vehicle titles, as well as the electronic assignment and release of liens. The program will be operational by 01 July 2022.

On 16 March 2021, Michigan's **Electronic Lien and Title (ELT)** program went into effect, "allowing for the electronic exchange of lien and title information with lienholders in lieu of a paper certificate of title." In the case that a customer finances a vehicle with a participating financial institution, the title will be kept electronically. If the ownership of a vehicle changes, a paper title shall be required. On 12 May 2021, a **bill** was introduced to the New Jersey legislature that would allow for the electronic processing of salvage titles.

Washington Uniform Electronic Wills Act, 26 April 2021

On 17 July 2019, the US passed the national Electronic Wills Act, which enables the electronic execution of wills. Washington's Uniform Electronic Wills Act was signed into law 26 April 2021, making Washington the fourth state to have transposed the Act onto state law. North Dakota's **Uniform Electronic Wills Act** was signed into law 09 March 2021 by Governor Doug Burgum, the **Colorado Uniform Electronic Wills Act** was signed into law 21 January 2021 by Governor Jared Polis and Utah's **Uniform Electronic Wills Act** became law 31 August 2021. Virginia's **Uniform Electronic Wills Act**, introduced 07 January 2021, passed the State House of Representatives and was referred to the State Senate in early February 2021. The spate of laws comes amidst the COVID-19 pandemic, which made the in-person signing and witnessing of wills difficult due to social distancing restrictions.

Arizona Recognizes Mexico's Consular Registration Card as Valid ID, 05 March 2021

Governor Doug Ducey signed Senate Bill 1420, which recognizes Mexican consular registration cards as a valid form of ID in Arizona. The law notes that Arizona shall accept IDs issued by foreign governments that have employed biometric identity verification techniques, including fingerprints and retina scans. In his **signing letter**, Governor Ducey said, "This legislation will ensure that law enforcement is able to quickly and accurately identify more of the individuals with whom they interact. This is critical to ensure safety for both law enforcement and the public... This bill does not authorize any new rights or responsibilities for non-citizens. It simply recognizes that governments in Arizona will accept cards issued by countries who use strict biometric identity verification techniques as lawful identification."

ENDNOTES

1 Johnston, Matthew. "The Economy of Canada: An Explainer." Investopedia, 27 July 2021. https://www.investopedia.com/articles/investing/042315/fundamentals-how-canada-makes-its-money.asp.

2 Davenport, Tom. "Learning From The Canadian Model Of AI." Forbes, 19 November 2019. https://www.forbes.com/sites/tomdavenport/2019/11/19/learning-from-the-canadian-model-of-ai/?sh=7f66f29b2300.

3 Lecuyer, Marc. "Pandemic-fuelled demand for digital services is here to stay." The Hill Times, 02 August 2021. https://www.hilltimes.com/2021/08/02/pandemic-fuelled-demand-for-digital-services-is-here-to-stay/309531.

4 Stephenson, Amanda. "Average cost of a data breach in Canada hit new record in 2021, IBM Security report says." The Globe and Mail, 28 July 2021. https://www.theglobeandmail.com/business/article-average-cost-of-a-data-breach-in-canada-hit-new-record-in-2021-ibm.

5 "2020 was the worst year on record for Canada's economy. It shrank by 5.4%." The Canadian Broadcasting Corporation, 02 March 2021. https://www.cbc.ca/news/business/statscan-economy-2020-1.5933072.

6 Gordon, Julie and Kelsey Johnson. "Canada second-quarter GDP likely to fall record 12% on COVID-19 shutdowns." Reuters, 31 July 2021. https://www.reuters.com/article/us-canada-economy-gdp-idUSKCN24W1Z3.

7 Graham, Jack. "Covid-19 is Highlighting Canada's Digital Divide. What Can We Do About It?" Future of Good, 16 April 2021. https://futureofgood.co/covid-19-is-highlighting-canadas-digital-divide-what-can-we-do-about-it/.

8 Horwood, Matt. "Businesses need federal investment in cybersecurity, says Beatty." The Hill Times, 24 July 2021. https://www.hilltimes.com/2021/07/24/businesses-need-federal-investment-in-cybersecurity-says-beatty/308194.

9 "Final Report." Advisory Committee on Open Banking, April 2021. https://www.canada.ca/content/dam/fin/consultations/2021/acob-ccsbo-eng.pdf.

10 "Final Report." Advisory Committee on Open Banking, April 2021. https://www.canada.ca/content/dam/fin/consultations/2021/acob-ccsbo-eng.pdf.

11 "Methods to verify the identity of persons and entities." Financial Transactions and Reports Analysis Centre of Canada, June 2021. https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng#s2a.

12 "Methods to verify the identity of persons and entities." Financial Transactions and Reports Analysis Centre of Canada, June 2021. https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng#s2a.

13 "Canada commences testing of digital ID framework." Finextra, 16 September 2020. https://www.finextra.com/pressarticle/84093/canada-commences-testing-of-digital-id-framework.

14 "Newly Launched Digital ID Framework to Begin Testing in Canada." Business Wire, 15 September 2020. https://www.businesswire.com/news/home/20200915005744/en/Newly-Launched-Digital-ID-Framework-to-Begin-Testing-in-Canada.

15 Gratton, Éloïse et al. "End of parliamentary proceedings in Quebec: An Update on Bill 64." Lexology, 21 June 2021. https://www.lexology.com/library/detail.aspx?g=2cab3fdb-e6f7-423f-8257-384d5ccea244.

16 Morgan, Charles S. et al. "Bill 95: Quebec's Digitization Law Unpacked." Lexology, 16 July 2021. https://www.lexology.com/library/detail.aspx?g=524bcdba-ff17-422f-bb26-865766500429.

17 Mezzetta, Rudy and Melissa Shin. "It's official: marriage no longer revokes a will in Ontario." Investment Executive, 03 May 2021. https://www.investmentexecutive.com/news/industry-news/its-official-marriage-no-longer-revokes-a-will-in-ontario/.

18 Rushe, Dominic. "US economy shrank by 3.5% in 2020, the worst year since second world war." The Guardian, 28 January 2021. https://www.theguardian.com/business/2021/jan/28/us-economy-shrank-2020-worst-year-since-second-world-war.

19 Crutsinger, Martin. "US economy grows 6.4% in Q1, and it's likely just the start." AP News, 24 June 2021. https://apnews.com/article/consumer-spending-gross-domestic-product-economy-business-ea9f24b146848b0821b549abb6cf78c8.

20 Bovino, Beth Ann and Satyam Panday. "Economic Outlook US Q3 2021: Sun, Sun, Sun, Here It Comes." S&P Global Ratings, 24 June 2021. https://www.spglobal.com/ratings/en/research/articles/210624-economic-outlook-u-s-q3-2021-sun-sun-sun-here-it-comes-12014595.

21 Popkin, Helen et al. "Covid-19 Devastated Some Industries But Accelerated AI Use By Companies Across The Country." Forbes, 26 April 2021. https://www.forbes.com/sites/alanohnsman/2021/04/26/ai-50-americas-most-promising-artificial-intelligence-companies

22 "Coronavirus Accelerates US Bank Digital Banking, Branch Optimization." Fitch Ratings, 31 March 2021. https://www.fitchratings.com/research/banks/coronavirus-accelerates-us-bank-digital-banking-branch-optimization-31-03-2021.

23 "US output surging amid pandemic due to digitization – Goldman." Reuters, 13 July 2021. https://www.reuters.com/world/us/us-output-surging-amid-pandemic-due-digitization-goldman-2021-07-13/.

24 Chakravorti, Bhaskar. "How to Close the Digital Divide in the US" Harvard Business Review, 20 July 2021. https://hbr.org/2021/07/how-to-close-the-digital-divide-in-the-u-s.

25 Tellez, Anthony. "Fed Chairman Suggests That Bitcoin Could Become Obsolete If US Digital Currency Existed." Forbes, 14 July 2021. https://www.forbes.com/sites/anthonytellez/2021/07/14/fed-chairman-suggests-that-stablecoins-and-cryptocurrencies-could-become-obsolete-if-us-digital-currency-existed/?sh=3c2e3b52357a.

26 Marte, Jonnelle. "Powell says a Fed digital currency could undercut need for cryptocurrencies." Reuters, 14 July 2021. https://www.reuters.com/business/feds-powell-says-stablecoins-need-appropriate-regulatory-framework-2021-07-14/.

27 Rippy, Sarah. "US State Privacy Legislation Tracker." The International Association of Privacy Professionals, 08 July 2021. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

28 "Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies." The Daily Journal of the United States Government, 08 October 2021. https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies.

29 "Authentication and Access to Financial Institution Services and Systems." Federal Financial Institutions Examination Council, 11 August 2021. https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

30 "Brief #2: Fraud Types and Authentication for Remote Payment Use." The Federal Reserve, 03 August 2021. https://fedpaymentsimprovement.org/wp-content/uploads/brief-2-fraud-types-and-authentication-for-remote-payment-use-cases.pdf.

31 Aschettino, Stephen A. "2nd Circuit Clears the Way for OCC's 'FinTech Charter.'" Lexology, 04 June 2021. https://www.lexology.com/library/detail.aspx?g=0deecf73-5209-42e0-a69a-4441113b63c3.

32 "Rubio-Feinstein Sanction and Stop Ransomware Act of 2021." rubio.senate.gov, 05 August 2021. https://www.rubio.senate.gov/public/_cache/files/671937f9-f463-45ef-8995-44bfb08c5c6b/A4CE60BFC099E755B82927640E0B6308.sanction-and-stop-ransomware-act-section-by-section-final-8.5.21-.pdf.

33 "Wicker, Blackburn Introduce Federal Data Privacy Legislation." US Senate Committee on Commerce, Science & Transportation, 28 July 2021. https://www.commerce.senate.gov/2021/7/wicker-blackburn-introduce-federal-data-privacy-legislation.

34 "Wicker, Blackburn Introduce Federal Data Privacy Legislation." US Senate Committee on Commerce, Science & Transportation, 28 July 2021. https://www.commerce.senate.gov/2021/7/wicker-blackburn-introduce-federal-data-privacy-legislation.

35 "Wicker, Blackburn Introduce Federal Data Privacy Legislation." US Senate Committee on Commerce, Science & Transportation, 28 July 2021. https://www.commerce.senate.gov/2021/7/wicker-blackburn-introduce-federal-data-privacy-legislation.

36 De, Nikhilesh. "US Lawmakers Introduce Bill That Would Require Stablecoin Issuers to Obtain Bank Charters." Coindesk, 02 December 2020. https://www.coindesk.com/us-lawmakers-introduce-bill-that-would-require-stablecoin-issuers-to-obtain-bank-charters.

37 Tank, Margo H. K. "[UPDATED] Coronavirus: Federal and state governments work quickly to enable remote online notarization to meet global crisis." DLA Piper, 15 August 2021. https://www.dlapiper.com/en/us/insights/publications/2020/03/coronavirus-federal-and-state-governments-work-quickly-to-enable-remote-online-notarization/.

38 "Hawaii and Minnesota Enact Insurance Data Security Laws." Thomson Reuters Practical Law, 01 July 2021.

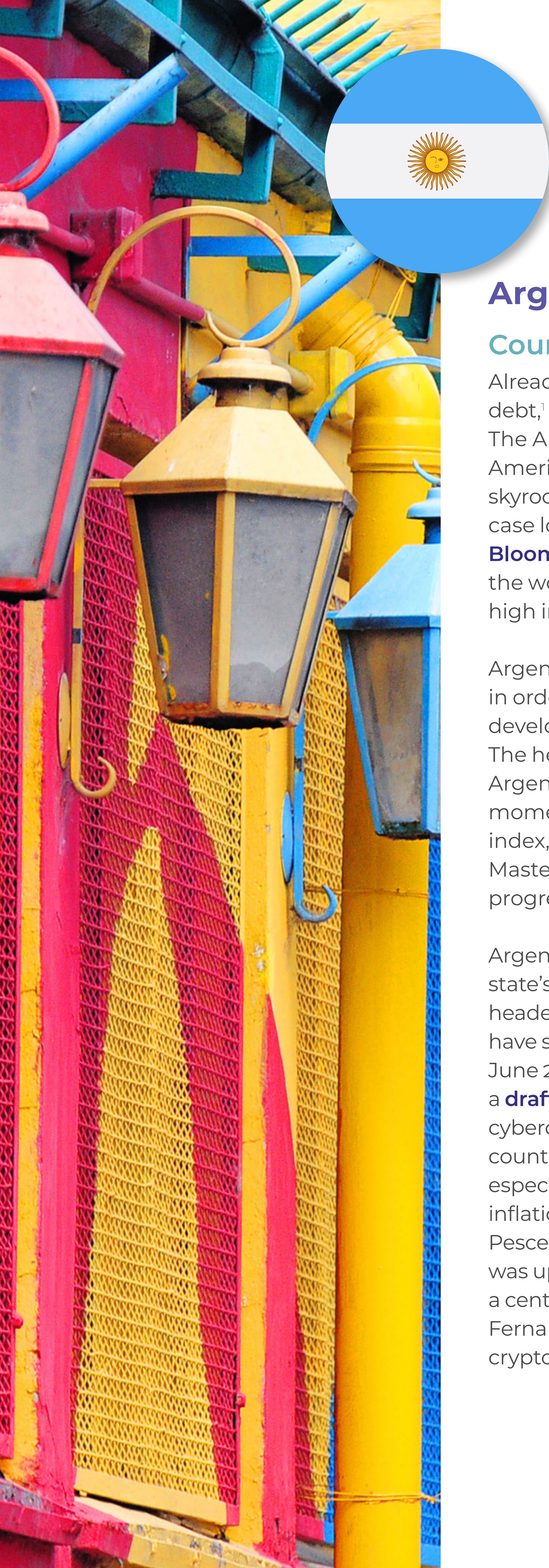
https://content.next.westlaw.com/Document/I3e5385dad9b511ebbea4f0dc9fb69570/View/FullText.html.
39 “Hawaii and Minnesota Enact Insurance Data Security Laws.” Thomson Reuters Practical Law, 01 July 2021. https://content.next.westlaw.com/Document/I3e5385dad9b511ebbea4f0dc9fb69570/View/FullText.html
40 “California Consumer Privacy Act 2.0 – What You Need to Know.” JD Supra, 27 November 2020. https://www.jdsupra.com/legalnews/california-consumer-privacy-act-2-0-93257/.
41 “BREAKING: Ohio’s Legislature Considering Passing the Ohio Personal Privacy Act with Support of Governor DeWine and Lt. Governor Husted.” The National Law Review, 14 July 2021. https://www.natlawreview.com/article/breaking-ohio-s-legislature-considering-passing-ohio-personal-privacy-act-support.
42 “North Carolina Proposes Expansive Consumer Privacy Protections.” JD Supra, 21 April 2021. https://www.jdsupra.com/legalnews/north-carolina-proposes-expansive-7005596/.
43 Seals, Mike. “New Law enables Electronic Titles, saving time and money.” Ponca City Now, 11 May 2021. https://www.poncacitynow.com/new-law-enables-electronic-titles-saving-time-and-money/.

Latin America

Latin America is the global region most devastated by the COVID-19 pandemic, which struck amidst a region-wide slump in economic growth and social development progress.[1] In 2020, GDP in Latin America and the Caribbean plunged by 6.3%,[2] poverty and inequality deepened, and political unrest swept through several countries. Although the Economic Commission for Latin America and the Caribbean (ECLAC) forecasts the regional economy to expand by 5.2% in 2021, poverty, inequality and other structural problems will continue to worsen.[3]

Meanwhile, the health crisis spurred on accelerated digitalization as restrictions shifted business and government operations online, consumer preferences changed and the regulatory landscape developed. This year, Latin American governments, international organizations and fintechs are seeking to drive digital transformation and financial inclusion, which will help to support recovery and other development goals. Brazil and Guatemala are investigating central bank digital currency (CBDC); Colombia is poised to be the third Latin American country to introduce open banking, after Mexico and Brazil; and Colombia and Mexico are launching national digital IDs. Fintech will be especially instrumental in expanding access to financial services, offering consumers more choice and simplifying payment services.

A key challenge will be ensuring that digitalization initiatives are accompanied with appropriate data protection and cybersecurity standards, and that digital transformation does not widen the digital divide. In Latin America, approximately 55.5% of households lack broadband access, and this disparity widens along socioeconomic and geographic lines.[4]



Argentina

Country Overview

Already grappling with high inflation and sovereign debt,[1] Argentina was hit hard by the COVID-19 pandemic. The Argentine economy—the third-largest in Latin America[2]—contracted by 9.9% in 2020,[3] urban poverty skyrocketed to 42% in the second half of 2020,[4] and severe case loads have strained the healthcare system.[5] The **Bloomberg Misery Index** for 2020 ranked Argentina as the world's second-most miserable economy due to high inflation and unemployment rates.

Argentine regulators must accelerate digitalization initiatives in order to stabilize the economy, achieve its sustainable development goals and guide the post-pandemic recovery. The health crisis has already boosted digital transformation in Argentina, and Argentina ranked high on digital evolution momentum in the 2020 **Digital Intelligence Index (DII)**. The index, developed by Tufts University's Fletcher School and Mastercard, praised the state for continuing to make progress in strengthening its "digital friendly institutions."

Argentina's 2021 digital agenda, though scant, shows the state's commitment to digital transformation. ATMs are headed towards biometric authorization, and regulators have signaled an interest in bolstering cybersecurity. In June 2021, the Chamber of Deputies of Argentina issued a **draft resolution** seeking feedback on questions related to cybercrimes, in reaction to the rise of cybercrime in the country. Digital payments are likely to be an issue to watch, especially as cryptocurrency investments soar amidst high inflation. On 11 August 2021, central bank president Miguel Pesce stated that a possible regulation on bitcoin transactions was upcoming,[6] and that the bank did not plan on developing a central bank digital currency (CBDC).[7] President Alberto Fernandez, however, has expressed openness towards cryptocurrencies and their possible advantages.[8]

Support for fintech, a modern and revamped payments system, improvements to digital infrastructure and expansion of digital access will be crucial in promoting financial inclusion, competitiveness and innovation. Regulators must especially look towards developing a national digital identity system in securing the digital economy and society. Although figures vary widely, the most recent World Bank data revealed that a mere 49% of the adult population in Argentina was banked in 2017.[9]

Financial Regulatory Authorities

- The **Central Bank of the Argentine Republic (BCRA)** is the central bank of Argentina.
- The **National Directorate for Personal Data Protection (PDP)** is Argentina's national data protection authority, established by the National Data Protection Act.
- The **National Securities Commission (CNV)** supervises and regulates equity markets in Argentina.

Policy, Laws and Regulations

Verification Measures for Digital Wallets, 01 August 2021

The central bank issued Communication A 7326, which requires that financial entities and payment service providers offering payment accounts through a digital wallet or a similar service to adhere to certain verification measures. Obliged entities must verify the identity of a person who opens an account; associate with the digital wallet only the payment instruments or accounts of the holder of the wallet; conduct user authentication and identification per access to the wallet; and allow more than one owner per payment account. The measures must be traceable and auditable.[10] The communication went into effect 01 August 2021.

Missionary Financial Innovation Program with Blockchain and Cryptocurrency Technology, 15 July 2021

The province of Misiones approved the Missionary Financial Innovation Program with Blockchain and Cryptocurrency Technology law, which seeks to harness innovative technologies in digitalizing government services, boosting efficiency and confronting climate change. Blockchain will be utilized to issue government certificates and other documents currently issued by paper,[11] and the law also outlines a plan to issue a provincial stablecoin.

Alert on Risks and Implications of Cryptoassets, 20 May 2021

The central bank and the National Securities Commission (CNV) issued a joint alert on the risks and implications of cryptoassets. The alert notes that cryptoassets are not legal tender, are highly volatile, can facilitate operational disruptions and cyberattacks, do not have safeguards and can facilitate money laundering and terrorist financing. Providers of cryptoasset services may also fail to disclose information and risks, and investors may be susceptible to fraud. Due to the cross-border nature of cryptocurrency operations, Argentine investors have less recourse to Argentine authorities and courts in the case of a conflict.

In April 2021, the central bank issued a note requesting that banks identify clients who conduct operations using cryptoassets. Banks must supply the client's name, address and number and type of account.[12]

Guidelines for Response and Recovery from Cyber Incidents, 17 April 2021

The central bank published a communication—applicable to financial institutions, payment service providers and financial market infrastructures—on Guidelines for Response and Recovery from Cyber Incidents. Per the communication, management is responsible for defining cyber resilience objectives and implementing the related policies and controls. Management must cultivate an organizational environment in which cyber incidents are properly reported or escalated, establish training programs for all staff levels and "[p]romote continuous and sustained actions with suppliers and third parties in preparing cyber-incident response and recovery tasks, so that they can be timely and adapt to different situations." Metrics must be established in evaluating the impact of cyber incidents and the subsequent responses, and contact lists of internal and external stakeholders must be made so that cyber incidents are properly disclosed to relevant parties, when appropriate.

Biometric Access to ATMs, 22 January 2021

The central bank issued a circular outlining rules on ATM access through the use of fingerprint readers. Per the new rules, users shall access ATMs through "something you know"—a PIN or identity card (DNI)—alongside fingerprints. The rules will be implemented through a phased approach. By 31 December 2021, 35% of ATMs are required to include a biometric reader; that number increases to 60% by 30 June 2022, and by 31 December 2022, all ATMs will be required to include a biometric reader.

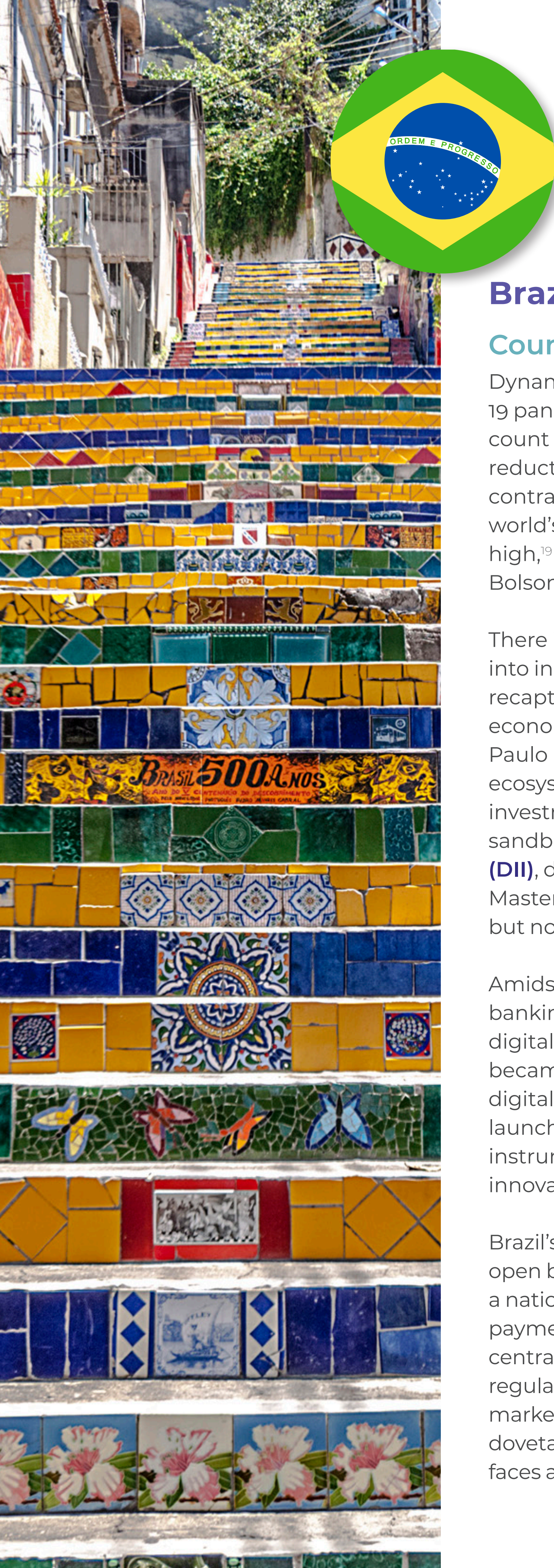
Legislation

Wage Perception Regime in Cryptocurrencies, 05 July 2021

Congressman José Luis Ramón introduced a bill on the *Wage Perception Regime in Cryptocurrencies* to the Senate and the Chamber of Deputies of Argentina. If enacted, the bill would allow Argentine employees—including self-employed workers who export services abroad—to receive full or partial payment in cryptocurrency. Employers would have to take on the costs of the cryptocurrency transfer.[13] The Argentine annual inflation rate reached 50% in 2021,[14] and citizens have flocked to cryptoassets as a hedge against inflation and an uncertain future.

Crime of Impersonation of Digital Identity, 06 May 2021

The Senate and the Chamber of Deputies of Argentina introduced a bill seeking to include the crime of impersonation of digital identity in Article 139 of the National Penal Code. Anyone who adopts, creates or appropriates the digital identity of a person or legal entity—without their consent—with the intention to commit a crime shall face imprisonment from one to three years. In the case that the crime occurs continuously, forces the victim to alter their life or the victim is under the age of 18 years old, the perpetrator shall face a prison sentence of four to six years.



Brazil

Country Overview

Dynamic and diversified Brazil was devastated by the COVID-19 pandemic, which led to the world's second highest death count at over half a million people,[15] undid years of poverty reduction[16] and battered the economy. Brazil's GDP contracted by 4.1% in 2020,[17] bringing it down from the world's ninth largest economy to the twelfth.[18] Inflation is high,[19] and protests have erupted in reaction to President Jair Bolsonaro's management of the health crisis.

There is hope yet for Brazil, which has the opportunity to tap into incredible digitalization and fintech potential in recapturing lost development progress, revamping the economy and promoting financial inclusion. The city of São Paulo is home to the world's fourth largest fintech ecosystem,[20] Brazil receives half of South America's fintech investments[21] and the central bank launched a fintech sandbox in November 2020.[22] The **Digital Intelligence Index (DII)**, developed by Tufts University's Fletcher School and Mastercard, ranks Brazil low on digital evolution momentum, but notes that Brazilians are highly technologically engaged.

Amidst the pandemic, Brazilians have flocked to digital banking,[23] and the state is forecast to reach over 200 million digital bank accounts in 2021.[24] In 2020, 14 million Brazilians became banked[25] and low-income Brazilians' demand for digital services soared.[26] The instant payments system PIX, launched in November 2020 by the central bank, has been instrumental in making the national payments sector more innovative and competitive than ever.

Brazil's 2021 digital agenda focuses on the implementation of open banking, a possible central bank digital currency (CBDC), a national artificial intelligence strategy, cybersecurity in payments and a national data protection framework. The central bank is reportedly developing a framework to provide regulatory clarity for the increasingly popular digital currency market.[27] Regulators must ensure that digitalization initiatives dovetail with efforts to boost national cybersecurity, as Brazil faces a high risk of cybercrime.[28]

Financial Regulatory Authorities

The **Central Bank of Brazil (BCB)** is Brazil's central bank.

The **National Data Protection Authority (ANDP)** oversees and enforces compliance with the General Data Protection Law (LGPD).

The **Brazilian Securities and Exchange Commission (CVM)** regulates the Brazilian capital markets and its participants, including stock exchanges, public companies and financial intermediaries. It aims to promote fairness and transparency and protect consumers.

The **National Monetary Council (CNM)** formulates monetary and credit policies.

Policy, Laws and Regulations

Open Banking Implementation, 13 August 2021

Brazil's open banking scheme, which was approved in 2019, aims to boost competition and innovation, promote financial inclusion and modernize the national financial and payments sectors. Participation is mandatory for large and medium-sized Brazilian banks, and voluntary for other entities.[29] It is being implemented through a phased approach, covering four major dates from February to December 2021. On 24 June 2021, the central bank issued **Resolution No. 109**, which established a timeline for the implementation of open banking services outlined in the 04 May 2020 **Joint Resolution No. 1** and the technical requirements and other operational procedures outlined in the 04 May 2020 **Circular No. 4015**. The resolution has been updated twice in line with the second and third phases of open banking implementation, and includes deadlines up until 30 September 2022. Key dates are included in the following table:

OPEN BANKING IN BRAZIL: KEY DATES

01 February 2021: Phase 1	Phase 1 covers the sharing of data for savings accounts, prepaid payment accounts, credit cards and credit operations; and the development of infrastructure in the implementation of the participant directory, service desk and Open Banking portal.
13 August 2021: Phase 2	Initially scheduled for a 15 July 2021 implementation date, Phase 2 of open banking was postponed to 13 August 2021.[30] It covers the sharing of customer registration and transaction data for demand and savings accounts, as well as procedures for the resolution of disputes between participating entities.
30 September 2021: Submission of plans to central bank	Obliged entities must have submitted plans on the sharing of data on products and services per Article 2, Item III of the Joint Resolution.
29 October 2021: Technical requirement	Obliged entities must have shared the PIX payment transaction initiation service, per Article 5, Item II, Sub-item "a" of the Joint Resolution and Article 6, Item IV of the Circular.
29 October 2021: Phase 3	Initially scheduled for a 30 August 2021 implementation date, Phase 3 of open banking was postponed to 29 October 2021 to allow financial institutions and fintechs more time to integrate payment services.[31]
16 November 2021: Submission of plans to central bank	Obliged entities must have submitted plans on the payment transaction initiation service per Article 2, Item IV of the Joint Resolution.
15 December 2021: Technical requirement	Obliged entities must have shared data on products and services per Article 5, Item I, Sub-item "b" and Items VI to X of the Joint Resolution.
15 December 2021: Phase 4	Phase 4 expands the scope of covered data, and will allow for the sharing of extra customer information across foreign exchange services, investments, insurance and salary accounts.[32]

17 December 2021: Submission of plans to central bank	Obliged entities must have submitted plans on the sharing of the credit operation proposal forwarding service per Article 2, Item V of the Joint Resolution.
24 February 2022: Submission of plans to central bank	Obliged entities must have submitted plans on the sharing of customer transaction data per Article 2, Item VI of the Joint Resolution.
31 March 2022: Submission of plans to central bank	Obliged entities must have submitted plans on the sharing of the payment transaction initiation service per Article 2, Item VII of the Joint Resolution.
31 May 2022: Technical requirement	Obliged entities must have shared customer transaction data per Article 5, Item I, Sub-item "d" and Items VI to XI of the Joint Resolution.
30 June 2022: Submission of plans to central bank	Obliged entities must have submitted plans on the sharing of payment transaction initiation services per Article 2, Item VIII of the Joint Resolution.
30 September 2022: Technical requirement	Obliged entities must have shared the debt payment transaction initiation service per Article 5, Item II, Sub-item "a" of the Joint Resolution and Article 6, Item I of the Circular.

National Council for the Protection of Personal Data and Privacy, 09 August 2021

A presidential decree was issued to announce the members of the National Council for the Protection of Personal Data and Privacy (CNPD). The CNPD, which shall create guidelines on data protection rules, will be composed of 23 board members and deputies for a two-year term.[33] The decree follows other recent updates as part of Brazil's ongoing efforts to strengthen its national data protection framework. The Brazilian General Data Protection Law (LGPD) was approved 14 August 2018, and the National Data Protection Authority (ANDP) was created by a 28 December 2018 executive order.

On 29 June 2021, the Brazilian Chamber of Deputies amended **Decree-Law No. 2848** of 07 December 1940 (the Penal Code), which now criminalizes the disclosure, supply, sale or permission to access third-party personal data, whether unauthorized or for illicit purposes. Violations will incur a fine and a two-to-five-year prison sentence.

On 31 May 2021, the National Data Protection Authority opened a public **consultation** seeking feedback on the establishment of oversight mechanisms per the application of the LGPD. The ANDP aims to boost compliance, with a focus on evidence-based regulation, proportionality between risks and resources, transparent and just processes, and diverse approaches to promoting compliance. The consultation was closed 28 June 2021.

On 13 May 2021, the National Data Protection Authority issued a **guidance** on the reporting of security incidents involving personal data. Obliged entities must report security incidents within a "reasonable" timeframe, and include key information in their reports, including: the identity and contact details for the "entity or person responsible for the processing" and "the data officer or other control person;" and information on the security incident such as the date and time of detection, its duration and circumstances, a description of the personal data affected, possible consequences, a summary of response measures and "possible problems of a cross-border nature."

General Guideline for Brazilian CBDC, 24 May 2021

The central bank issued its general guideline for a Brazilian CBDC, which addresses the potential benefits in the issuance of a CBDC. Key benefits include a CBDC's capacity to facilitate new business models based on technological advances, boost efficiency in cross-border transactions and the retail payment system at large, and contribute to the "dynamic technological evolution of the Brazilian economy." The central bank has not yet developed a timeframe for a possible CBDC trial, noting that it must first conduct discussions with the private sector. In an email to CoinDesk, the central bank stated that a CBDC might be adopted within two to three years.[34]

National Artificial Intelligence Strategy, 12 April 2021

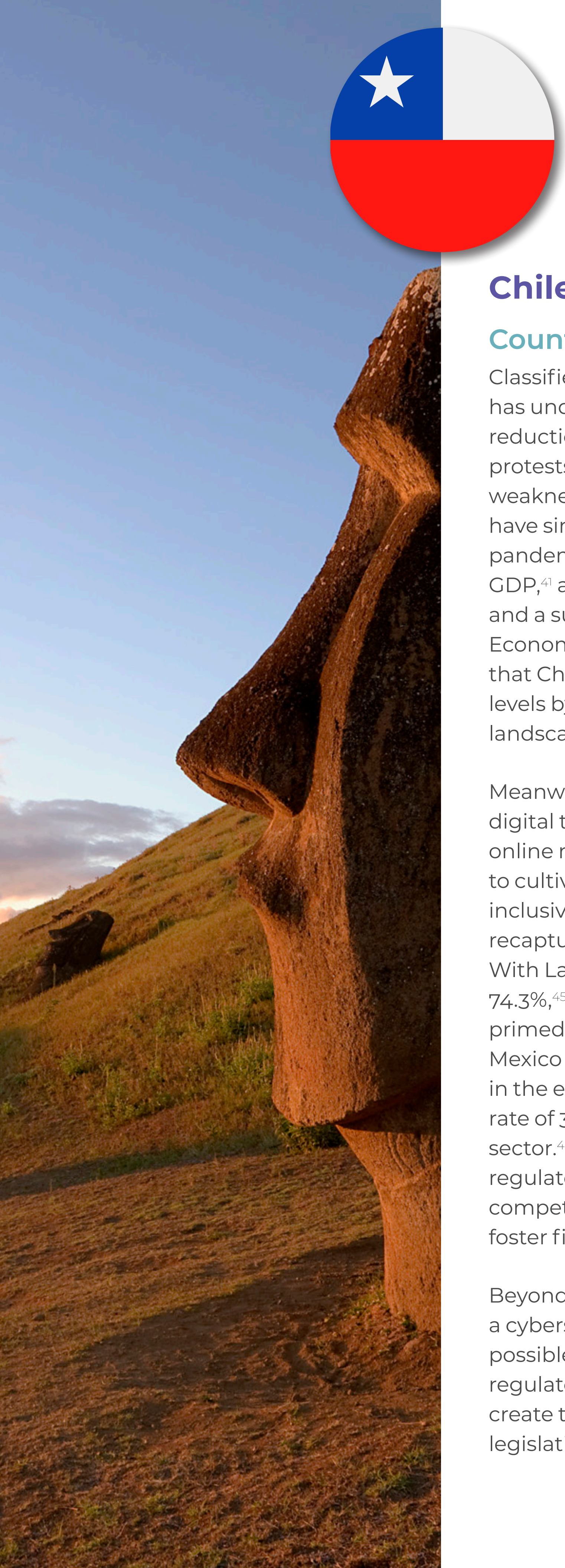
The Brazilian government launched its national AI strategy, which outlines six objectives in the development and adoption of AI solutions. The objectives seek to develop ethical principles in the use of AI; remove barriers to innovation; bolster collaboration between the government, private sector and researchers; develop AI skills; invest in technologies; and promote Brazilian tech abroad.[35] The strategy aims to implement AI solutions in at least twelve national public services by 2022 and establish a national digital literacy program for students.[36]

Cybersecurity Requirements for Payment Services, 08 April 2021

The central bank issued Resolution No. 85, which outlines cybersecurity requirements for the processing and storage of data, as well as cloud computing services, applicable to payment institutions. In the case that payment institutions contract services to third parties, payment institutions must report the contractual relationship to the central bank. Prior to entry into the contract, payment institutions must notify the bank of the country and regions where the service may be provided and provide alternatives for the continuity of the service should the contract end. Payment institutions are responsible for compliance, reliability, integrity and confidentiality. Regarding cybersecurity, payment institutions must implement monitoring and control mechanisms to ensure the effectiveness of their incident response and action plans. The central bank must have five-year access to payment institutions' documents related to their respective cybersecurity policies, minutes of meetings of the board of directors, documents related to the incident response and action plans, the annual plan, and data and records related to monitoring and control mechanisms. The resolution took effect 31 August 2021.

Launch of PIX Instant Payments Platform, 16 November 2020

The central bank launched its instant payments system, PIX, which enables wallets with QR codes to conduct real-time, 24/7 payments and transfers. The system is key in promoting financial inclusion, as it is free to use and end users are not required to have a bank account. As of May 2021, PIX had processed 1.549 billion transactions and had over 87.3 million users.[37] Central bank president Roberto Campos Neto stated in August 2021 that measures intended to boost the service's security were upcoming.



Chile

Country Overview

Classified as a "high income" state by the World Bank,[38] Chile has undergone significant economic growth and poverty reduction over the past several decades.[39] The 2019-2020 protests in response to inequality and corruption highlighted weaknesses in economic and social stability,[40] however; these have since been further compounded by the COVID-19 pandemic. In 2020, the health crisis drove a 6% contraction in GDP,[41] an estimated increase in poverty of 12.2% from 8.1%[42] and a surge in unemployment.[43] The Organisation for Economic Co-operation and Development (OECD) predicts that Chilean economic activity will return to pre-pandemic levels by late 2022, but the pandemic's ever-shifting landscape lends uncertainty to its recovery.

Meanwhile, the COVID-19 pandemic spurred on accelerated digital transformation in Chile, with increases in e-commerce, online marketing and streaming.[44] The government is eager to cultivate innovation, and an increasingly modern and inclusive digital economy will be key in helping the state to recapture its previously impressive development progress. With Latin America's highest rate of banking penetration at 74.3%,[45] and an internet penetration rate of 82.3%,[46] Chile is primed to compete with Latin American fintech hubs like Mexico and Brazil. Although the Chilean fintech ecosystem is in the early stages of development, it is growing at an annual rate of 38%,[47] with an especially promising digital payments sector.[48] Congress has been presented with an open finance regulatory framework, which will seek to promote competition and innovation, reduce barriers to entry and foster financial inclusion.[49]

Beyond open banking, Chile's 2021 digital agenda focuses on a cybersecurity regulation for the insurance industry and a possible National Artificial Intelligence Policy. A bill to regulate the protection and treatment of personal data and create the Personal Data Protection Agency remains in the legislative process. In spearheading further digitalization, regulators must ensure that efforts do not widen socioeconomic inequality, that access to high-speed broadband networks is increased and SMEs receive adequate support in the adoption of digital solutions.[50]

Financial Regulatory Authorities

The **Central Bank of Chile (CBoC)** is the primary monetary authority and policymaker and the central bank of Chile. The bank works autonomously and separately from national authorities, as mandated by the national Constitution.

The **Financial Market Commission (CMF)** is the country's primary capital market and insurance market regulator that partners with the Ministry of Finance to develop legislation.

Policy, Laws and Regulations

Cybersecurity Regulation for the Insurance Industry, 18 May 2021

The Financial Market Commission issued a regulation establishing standards on operational risk management and cybersecurity for insurance companies in a move to enhance supervision. Obliged entities must conduct a self-assessment regarding operational risk every two years, and an annual self-assessment regarding cybersecurity. The self-assessments are due 30 September, with the exception of 2021, when reports are due 31 December 2021. Obliged entities must also report cybersecurity incidents. The regulation went into effect 30 September 2021.

National Artificial Intelligence Policy, 15 December 2020

The Ministry of Science, Technology, Knowledge and Innovation launched a public consultation, which ended 06 January 2021, on a proposed National Artificial Intelligence Policy. According to Minister of Science Andrés Couve, "We want to promote an Artificial Intelligence Policy that addresses not only the socioeconomic opportunities, but also the ethical dilemmas and impacts that arise from its use, through consensus and commitments from the public and private sectors, academia and civil society so that this is a state policy, which can be updated and implemented by future governments."[51] The draft policy centers on six principles: "AI with a focus on people, AI for sustainable economic development, safe AI, inclusive AI, AI in society and globalized AI."[52] Specific strategies and objectives fall under one of three axes: "enabling factors, development and adoption, and regulatory and ethical aspects."[53] The Ministry is expected to release a document incorporating feedback from the consultation in 2021.

Legislation

Financial Innovation Bill, September 2021

The Financial Market Commission's long-awaited Fintech Act for the Securities Market, also known as the Financial Innovation Bill, was introduced to Congress. The Fintech Act seeks to provide a legal and regulatory framework for fintechs and pave the way for open banking. According to the CMF's 09 February **press release**, the Act "will promote innovation, financial inclusion, development of new funding sources [for] small-size enterprises, and greater competition in the financial market."[54]

The Act hinges on five pillars: proportionality, neutrality, integrity, flexibility and modularity. If enacted, it would apply to collective financing platforms, alternative trading systems, order routers and financial instrument intermediaries, safekeepers of financial instruments and loan advisors. The entities would be required to register in the CMF's new Registry of Providers of Financial Services, and must demonstrate compliance before being allowed to carry out any functions. The Act also seeks to amend the *Administration of Third Party Funds and Individual Portfolios*, *Corporations Law* and *Securities Market Law* in a move to maintain regulatory consistency. Amongst other changes, the amendments would grant the CMF greater authority in regulating securities intermediaries and the authority to request obliged entities to institute an API in order to facilitate the exchange of client information.[55]

Colombia

Country Overview

The COVID-19 pandemic, political instability and social unrest have devastated Colombia, which grappled with poor healthcare infrastructure and economic inequality even before the health crisis. Protests have erupted in response to corruption and proposed tax hikes, a subsequent crackdown has resulted in violence and death,[56] a third wave of infections has engulfed the country and 3.6 million Colombians have been driven into poverty.[57] The economy plunged by 6.8% in 2020,[58] and although it has shown signs of a rebound, the highly infectious Delta variant lends uncertainty to its recovery. Meanwhile, increases in poverty and economic inequality could take years to reverse.

Digital transformation will be key in safeguarding economic growth, promoting financial inclusion and boosting transparency in government. Colombian regulators have already made strides toward cultivating innovation, helped by a young, tech-savvy population[59] and shifting consumer preferences. In 2020, the Ministry of Finance and Public Credit issued a decree establishing Latin America's first fintech regulatory sandbox, which allows unlicensed startups the opportunity to test business models over a two-year period.[60] Digital banking in Latin America has soared since 2017, and neobanks in Colombia serve 1.5 million users.[61] The rate of unbanked individuals remains high, but slipped from 30.4% in 2015 to 23.3% in 2020, driven in large part by the pandemic.[62]

Colombia's 2021 digital agenda follows a broad pattern across Latin America as regional governments seek to modernize payments and introduce open banking while promoting financial inclusion, innovation and the digitalization of government services. Colombian regulators, in partnership with private sector entities,[63] are drafting an open banking regulatory regime to debut in late 2021 or 2022.[64] Colombia is also unrolling a national digital ID, which will allow citizens to vote electronically, obtain a driver's license, receive notifications and more.[65] In spearheading digitalization efforts, regulators must ensure that the digital divide does not widen, especially in rural and low-income communities. Internet penetration stood at a mere 65% in 2019,[66] although it has doubled in the past ten years,[67] and Colombia ranks as one of the globe's most expensive countries for mobile data use.[68]

Financial Regulatory Authorities

The **Central Bank of Colombia** is the primary financial policymaker and central bank of the country, issuing currency and regulating exchange rates. One of the bank's primary functions is to promote financial inclusion. It is a member of the international Financial Inclusion Alliance.

The **Superintendence of Industry and Commerce (SIC)** is a government regulatory agency that ensures fair competition and promotes economic growth in the private sector. Among its functions, the SIC issues technical standards and ensures compliance. It is divided into six departments, three of which are Consumer Protection, Personal Data Protection, and Technical Regulation.

The **Financial Superintendence of Colombia (SFC)** is an independent government agency that monitors and supervises the financial, insurance, and securities markets in Colombia, including implementing and enforcing financial data protection measures. The agency also provides investor protection.

The **Ministry of Finance and Public Credit** is the government ministry responsible for implementing financial policies approved by Congress and developing its own policies geared toward financial inclusion.

Other Regulatory Authorities

The **National Directorate of Taxes and Customs (DIAN)** seeks to support fiscal security and is responsible for tax collection in Colombia.

The **Superintendence of Corporations** oversees commercial companies in Colombia.

Policy, Laws and Regulations

E-Signatures in Electronic Invoicing System, 01 August 2021

On 09 February 2021, the National Tax and Customs Directorate (DIAN) issued Resolution 000012, which amends Resolution

000042. Resolution 000042, issued 05 May 2020, established a regulatory framework for electronic invoicing, and Resolution 000012 stipulates the addition of mandatory electronic signatures in electronic sales invoices. The update seeks to ensure the authenticity of invoices.[69] The resolutions went into effect 01 August 2021. The Resolution also mandates that electronic billers create and submit a "Documente Soporte" (support document) in the case that they purchase goods or services from a seller who is not mandated to issue electronic invoices.[70] Resolution 000063, issued 30 July 2021, postponed the implementation date of the support document requirement to 31 January 2022.[71] Colombian regulators have been quick to push for paperless services. The Organization for Economic Cooperation and Development (OECD) ranked Colombia third in its **Digital Government Index (DGI)** 2019 results, which include most OECD member and four non-member countries. Colombia, which ranked the highest in Latin America for digital government, scored high on the "user-driven" and "proactiveness" dimensions.

Blockchain Bond Pilot, 22 July 2021

The Central Bank announced its participation in a pilot experiment testing a blockchain bond through the use of smart contracts. Per the bank's press release, "This innovative pilot seeks to verify the benefits of this new technology in the life cycle of a security, from issuance to expiration. The benefits include the potential reduction of operational costs, the optimization of process times, greater efficiencies in the traceability and security of operations, the elimination of information asymmetries and a better management of financial risks, among others." The experiment will be conducted on the LACChain platform, developed by the Inter-American Development Bank Group's innovation lab IDB Lab. The IDB Group consists of the Inter-American Development Bank, the Multilateral Investment Fund and the Inter-American Investment Corporation; Banco Davivienda is also a participant.

Open Banking Regulatory Regime, May 2021

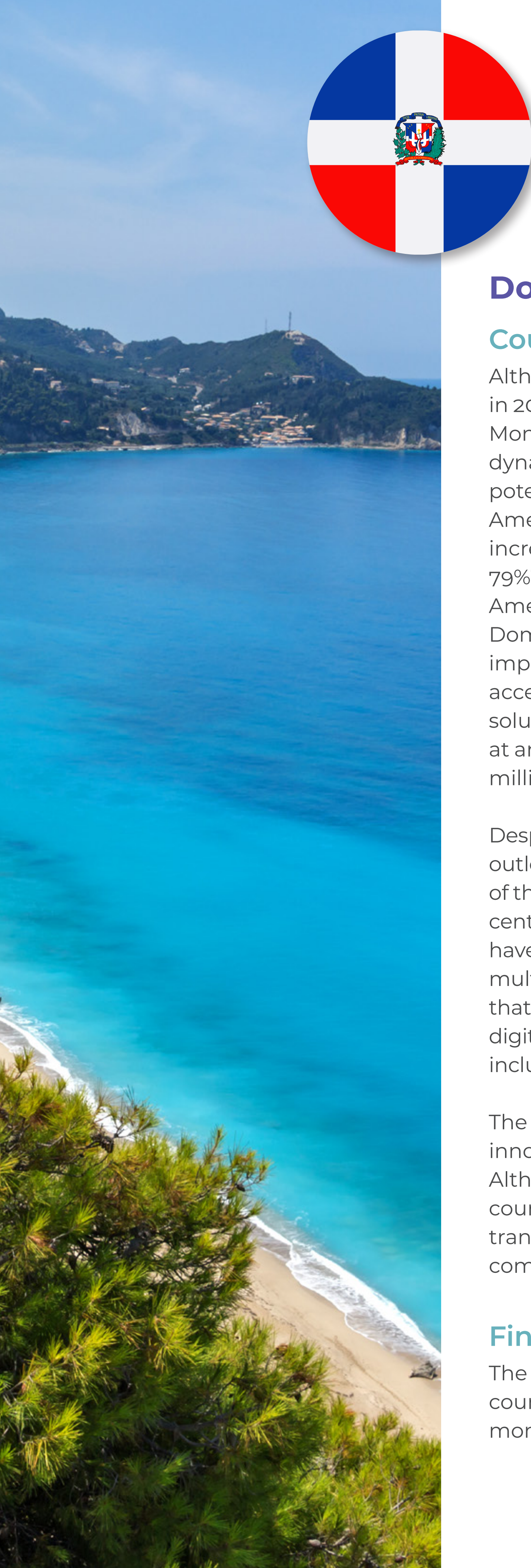
The Finance Ministry's financial regulations research unit Unidad de Proyección Normativa y Estudios de Regulación Financiera (URF) led a series of workshops with private sector entities from March to May 2021 on the development of an open banking regulatory regime. The voluntary regime is expected to be introduced in late 2021 or the beginning of 2022. In December 2020, the URF released a **white paper** addressing the benefits and risks of open banking alongside an overview of various implementation models. The paper notes that the existing national data protection framework is sufficient for the rollout of open banking. Colombia will likely be the third Latin America country to introduce open banking, after Mexico and Brazil.

Pilot Project on Crypto Platforms and Banking Services, 29 January 2021

The Financial Superintendence of Colombia (SFC) issued a press release announcing that its Evaluation and Monitoring Committee had selected nine cryptocurrency exchange platforms—including Binance—to partner with banks for a yearlong pilot on crypto use cases. The pilot, which began in March 2020, seeks to "measure the effectiveness of recent technological developments in the verification of digital identity and traceability in transactions" and will test cash-in and cash-out operations through the use of the crypto platforms. The program gives the SFC the opportunity to gather information in the development of future regulations.[72]

Circular on AML Guidelines for Financial Institutions, 24 December 2020

The Superintendence of Corporations issued AML guidelines for financial institutions in line with Financial Action Task Force (FATF) recommendations. The guidelines note that obliged entities must take a risk-based approach to due diligence, and certain sectors—including the virtual asset sector—must apply the "Enhanced Due Diligence process to know your Counterparty and Virtual Assets." Requirements of due diligence include ongoing due diligence, transaction monitoring, identification of the ultimate beneficiary of the counterparty, and obtaining information on the purpose and nature of the commercial relationship. Obliged entities must institute a "comprehensive risk management system" against ML/TF, referred to as SAGRILAFT and outlined in Chapter 10. SAGRILAFT must include, at the minimum, the identification of risk factors, the qualitative or quantitative evaluation of risk factors, the application of a risk matrix toward defining control mechanisms and their applications, monitoring the risk landscape, due diligence, enhanced due diligence, risk alerts, documentation of SAGRILAFT activities and suspicious operations reports.



Dominican Republic

Country Overview

Although the Dominican Republic's GDP contracted by 6.7% in 2020[73] amidst the COVID-19 pandemic, the International Monetary Fund (IMF) has praised the island country for its dynamic economy, policy response to the crisis and recovery potential.[74] One of the fastest-growing economies in Latin America and the Caribbean,[75] the Dominican Republic has increasingly digitalized, with an internet penetration rate of 79%[76] and ambitious plans to expand digital access. The Inter-American Development Bank IDB has granted the Dominican Republic a USD$115 million loan toward improving connectivity,[77] which will dovetail well with the accelerated adoption of digital banking and other innovative solutions. In February 2021, over 820,000 mobile transactions at an accumulated DOP 799 million (approximately USD$14 million) were made, a 16.6% year-on-year surge.[78]

Despite the Dominican Republic's progress and optimistic outlook, poverty and income inequality persist. Forty percent of the population lives in poverty[79] and a 2019 survey by the central bank revealed that 53.69% of the population did not have a bank account.[80] The government has instituted multiple temporary and permanent social programs to ensure that the COVID-19 pandemic does not deepen poverty,[81] and digitalization will be instrumental in promoting financial inclusion and strengthening the economy.

The 2021 Dominican digital agenda focuses on financial innovation and digitalization of the economy and society. Although the Dominican fintech ecosystem is small, the country's robust economy and continuous digital transformation could encourage new entrants and foster competition.

Financial Regulatory Authorities

The **Central Bank of the Dominican Republic** is the country's central bank and is responsible for regulating the monetary and banking system.

The **Superintendency of Banks (SB)** supervises and regulates the banking sector.

Law, Policy and Regulations

Financial Innovation Hub, 19 May 2021

In a virtual conference, central bank Governor Héctor Valdez Albizu announced that the bank was developing a financial innovation hub that would operate as a sandbox for private sector initiatives. Valdez noted that, "These innovation hubs already exist in countries such as the United Kingdom, Israel, Chile, and Mexico, to name just a few, and they have proven to be a very useful platform for exchanging information and experiences, which serves both the regulator as well as those regulated to jointly promote novel ventures that benefit the population, and support equitable access to financial services."[82]

2030 Digital Agenda, May 2021

The 2030 Digital Agenda was released by the Presidential Office for the Digital Transformation of the Dominican Republic, which was established by President Luis Abinader's Decree 71-21, issued in February 2021. The agenda centers on five axes: governance and regulatory framework, connectivity and access, digital education and capabilities, digital government and digital economy, all of which are underpinned by two overarching axes—cybersecurity and technological innovation. The agenda envisions a 2030 where the Dominican Republic is connected, the digital divide has closed, and technology is harnessed towards the achievement of sustainable economic and social development. Toward strengthening the digital economy, the agenda outlines several objectives, including to:

- "Strengthen the national development of ICT tools and solutions that support all economic sectors
- Boost digital business and e-commerce to promote productivity and competitiveness of companies
- Stimulate and facilitate the development of technology-based financial services
- Strengthen the legal and regulatory framework to facilitate digital transformation processes"[83]

Guatemala

Country Overview

Guatemala has been ravaged by the COVID-19 pandemic, which drove a 1.8% contraction in GDP in 2020,[84] aggravated income inequality and poverty, strained the healthcare system, highlighted political corruption and led to unrest. Although the Guatemalan economy is the largest in Central America, it is the fifth poorest in Latin America and the Caribbean,[85] and socioeconomic inequalities often fall along ethnic and geographic lines. Although the International Monetary Fund predicted a 4.5% GDP growth in 2021,[86] the advent of the Delta variant lends uncertainty to the state's fragile recovery. Summer 2021 brought the worst COVID-19 surge yet to Guatemala, which declared a state of emergency as it recorded over 4,000 deaths per day.[87]

Guatemalan regulators must spearhead further digitalization efforts in addressing persistent inequalities, securing the post-pandemic recovery and strengthening the economy. Although the state has made progress in expanding digital access, smartphone ownership is prohibitively expensive for many households,[88] and internet penetration is around 65%.[89] Fintech could be key in onboarding new customers, making banking more convenient and accessible, and spurring on cheaper and more competitive digital solutions across the banking sector. Fifty-six percent of Guatemalans are unbanked,[90] and in 2017, only 13.26% of Guatemalans had a credit card.[91]

The 2021 digital agenda focuses on a possible digital quetzal and the digitalization of government services. Alongside investments in digital infrastructure and innovative technologies, Guatemalan regulators must ensure that digital transformation does not exacerbate data protection concerns. The state does not have a national data protection framework, and in 2020, privacy alarms were raised regarding a contact tracing app used to collect and store users' geolocation data.[92]

Financial Regulatory Authorities

The **Bank of Guatemala (Banguat)** is Guatemala's central bank.

The **Superintendency of Banks (SIB)** is the primary financial services regulatory for the country of Guatemala. The Bank issues legislative decrees and standards aimed at increasing financial inclusion and protecting consumers.

Policy, Laws and Regulations

Law on the Simplification of Procedures, 31 August 2021

The Law on the Simplification of Procedures, published 01 June 2021 in the Official Gazette, aims to modernize executive branch administrative management through the simplification and digitalization of administrative procedures. It also seeks to "facilitate interaction between individuals or legal entities and government agencies."[93] The Law, which went into effect 31 August 2021, requires public institutions to utilize an advanced electronic signature in the issuance of resolutions and certifications, and prohibits public institutions from requiring that physical documents be uploaded if they bear an advanced electronic signature. Public institutions must also provide easy access to public records, which shall be stored in electronic databases, and administrative procedures must be conducted electronically, and be electronically traceable.[94]

Investigation Phase on Digital Quetzal, August 2021

Since early 2021, a technical team has been investigating the possible development—including technical and legal frameworks—of a central bank digital currency (CBDC). The digital quetzal would complement, rather than replace, physical notes and coins. Central bank president Sergio Recinos stated, "We are in the investigation phase. Then a platform will be sought (software and hardware, it could be blockchain technology), a pilot test will be carried out and finally the issuance will be carried out."[95] Recinos noted that a main challenge in the issuance of a digital quetzal would be internet access, especially in rural areas. According to ex-president of the central bank María Antonieta del Cid, a CBDC would boost financial inclusion, help to stabilize the payments system and foster discipline and competition in the market.[96]

On 24 June 2021, Recinos issued a warning on cryptocurrency investments during a news conference, stating, "There is a big difference between a digital currency issued by a central bank and a cryptocurrency issued by private actors that doesn't have government backing or oversight."[97]

Mexico

Country Overview

Mexico has been ravaged by the COVID-19 pandemic, which has led to one of the world's highest death tolls, destabilized development goals and battered the economy. The Mexican economy, the fifteenth largest in the world and the second largest in Latin America,[98] plunged by 8.3% in 2020,[99] its largest contraction since the Great Depression.[100] Average income dipped by 7% in 2020 from 2018,[101] and 3.8 million Mexicans were driven into poverty.[102] The International Monetary Fund (IMF) forecasts a growth rate of 6.3% in 2021,[103] but surging infections could endanger the emerging market's fragile recovery.

Digitalization will be key in securing Mexico's post-pandemic recovery, strengthening its regional and global competitiveness, and reaching its poverty reduction goals. Although Mexico scores low on digital evolution momentum per the Digital Intelligence Index (DII) 2020, developed by Tufts University's Fletcher School and Mastercard, its citizens are increasingly technology engaged. The Mexican population is young and tech-savvy, citizens and businesses have flocked to digital solutions amidst the health crisis, and fintech is well-positioned for growth. Foreign direct investment rose by 6.6% in 2020 from 2019,[104] the fintech startup ecosystem grew by 14% in 2020 from 2019[105] and biometric applications have been increasingly adopted.[106] Ninety-three fintech companies are in the process of acquiring a Financial Technology Institution (FTI) license[107] per the 2018 Law to Regulate Financial Technology Institutions (the "Fintech Law").

Although the Mexican government has been slow to nurture the digital economy, it has the opportunity to partner with this increasingly sophisticated fintech sector in spearheading longstanding goals like financial inclusion. A mere 37% of Mexican adults have a bank account, only 32% have utilized digital payments and lack of access to credit persists, all of which are compounded across geographic and gender divides.[108] Digital onboarding has promoted financial inclusion

TOP 3 REGULATORY CONCERNS FOR 2022

64%

Expansion of biometric database to include facial, voice data and possibly iris

38%

Geolocation database regulation

30%

Full compliance with open banking regulations

in Mexico, but the process requires fine-tuning; fintech could be instrumental in making banking cheaper, faster, more convenient and more accessible.

Beyond financial inclusion, Mexico's 2021 digital agenda focuses on promoting digital payments, strengthening the national AML/CTF framework, developing the fintech ecosystem and open banking, and rolling out a national digital ID system. In laying the foundation for a competitive, modern and inclusive digital economy, regulators must look to support small and medium-sized enterprises, strengthen digital infrastructure and promote use of the Cobro Digital Collection and Payment Platform (CoDi). As digital transformation accelerates, regulators must also ensure that stronger national cybersecurity measures are implemented.

Financial Regulatory Authorities

The **Bank of Mexico (Banxico)** is the central bank of Mexico and the country's primary monetary authority.

The **National Institute of Transparency for Access to Information and Personal Data Protection (INAI)** is the independent data protection agency of Mexico. The INAI is constitutionally mandated to defend and expand the right of access to public information and the protection of personal data.

The **Secretariat of the Economy (SE)** is the federal government office responsible for all matters related to Mexico's economy and commercial industries. Additionally, the SE issues guidelines regarding privacy notice requirements in partnership with the INAI.

The **Secretariat of Finance and Public Credit (SHCP)** houses the country's finance ministry and operates as a member of the federal executive cabinet. The SHCP is the head of the Office for the Treasury and Public Credit.

The **National Banking and Securities Commission (CNBV)** is an independent agency operating under the Secretariat of Finance and Public Credit and is the executive authority supervising Mexico's financial system. The CNBV is technically autonomous and regulates financial institutions and banks to ensure national financial system stability.

MEXICAN BANKS #1 COMPLIANCE CHALLENGE IS PREVENTING CYBERATTACKS AND FRAUD

54%

Reducing or preventing cyberattacks and fraud

42%

Safeguarding sensitive data

32%

Keeping pace with changes in consumer privacy laws, industry regulations

Policy, Laws and Regulations

Financial Regulators Issue Joint Statement on Cryptocurrency, 28 June 2021

Banxico, the Finance Ministry and CNBV issued a joint statement noting that cryptocurrency is not legal tender and that financial institutions are not authorized to offer services involving cryptocurrency. Financial institutions that do so are subject to sanctions. Per the Fintech Law, credit institutions may carry out certain internal operations using virtual assets, but these must be prescribed in provisions issued by Banxico. Banxico must then grant prior authorization to institutions looking to conduct operations with virtual assets. The statement also notes that entities conducting operations utilizing stablecoins must first obtain authorization from Banxico. The regulators address the volatility in cryptocurrency, its lack of inherent value and its speculative nature.

Cryptocurrency use has soared in Mexico, home to Latin America's largest cryptocurrency platform and its first crypto unicorn, Bitso.[109]

Provisions of Law to Regulate Financial Technology Institutions in Effect, 28 April 2021

The provisions of the Law to Regulate Financial Technology Institutions relevant to electronic payment fund institutions (EPFIs) have gone into effect. EPFIs must obtain users' express consent through an authentication process upon entering into an agreement. Users must be informed of the inherent risks in the use of the platforms, as well as recommendations on preventing unauthorized actions, and terms and conditions must be available at any moment for users' viewing. If the user wishes to contract operations and services other than those originally agreed upon, the terms and conditions shall be modified with express consent of the user. EPFIs must also notify users, in a period not exceeding five seconds, in the case that certain operations are executed:

- The daily accumulated amount of operations exceeds the equivalent in national currency to 60 investment units, or an individual operation exceeds the equivalent in national currency to 25 investment units
- "Registration or modification of the means of notification" to the user
- The contracting of another service
- "Deactivation, blocking, reactivation and modification of the authentication factor."

TOP COMPLIANCE TECHNOLOGIES FOR MEXICAN BANKS

50%

Mediated digital agreement technology

(electronic signatures with video conferencing/ collaboration and remote online notarization)

46%

Digital remote identity verification

(i.e., technologies allowing the verification of identity of natural or legal persons online)

46%

Classic biometrics

(e.g., voice, face, fingerprint)

The 2018 Fintech Law, which regulates EPFIs and crowdfunding institutions, aims to develop innovative companies in Mexico. It established an open banking regulatory regime and a licensing regime, and allows for regulated entities to perform certain internal operations with the use of virtual assets, upon authorization by Banxico. Though Mexico was the first Latin American country to introduce an open banking framework, it has been slow to enact provisions.[110]

National Registry of Mobile Phone Users to Collect Biometric Data, 13 April 2021

The Senate approved the passage of a reform to the Federal Telecommunications and Broadcasting Law, which will establish a national registry of mobile phone users and their biometric data. When citizens purchase a SIM card or activate a prepaid mobile phone, they will be required to present their ID, proof of address and one biometric identification, which can include fingerprints, an iris scan or facial features.[111] Once the Federal Telecommunications Institute has issued the administrative provisions in the establishment of the registry, mobile phone users will have two years to register and submit their biometric data, or their phone service will be cancelled.[112]

Implementation of Databases Containing Biometric Data, 31 March 2021

Effective 31 March 2021, banks must establish databases containing customers' biometric data, including at least fingerprints. The databases will eventually expand to include facial and voice data, with the possibility of iris data, by 2023.[113] Although the move aims to strengthen security, Mexican financial institutions remain vulnerable to cyberthreats. In January 2021, databases of Santander, BBVA and the Mexican Institute of Social Security were leaked and put up for sale online.[114] A compromise of biometric data could prove even more devastating. Mexico does not have a national cybersecurity law,[115] and the government has been slow to release information about past cyberattacks, which has left private companies less equipped to bolster cybersecurity measures.[116] From 01 November 2020 to 31 January 2021, the Mexican government led a **National Anti-Cyber Fraud Campaign**, which sought to raise awareness and boost cooperation between the government and society.

65%

of banks in Mexico are implementing mobile app shielding in anticipation of a Central Bank Digital Currency

Requirement on the Collection and Storage of Geolocation Data, 23 March 2021

Effective 23 March 2021, financial institutions must collect and store customers' real-time geolocation data in the cases of account opening, entry into contracts and operations conducted on digital platforms. Customers must provide consent for the collection and storage of their real-time geolocation data, or else be denied access.[117] The move comes as part of Mexico's efforts to bolster AML/CTF and aligns with recommendations from the Financial Action Task Force (FATF). CNBV noted in a statement that geolocation "is intended to have a client risk indicator that allows financial institutions to obtain information on the geographical area when executing non-face-to-face operations that are carried out on devices that the client has in their possession and from those whose location is unknown."[118] On 20 March 2021, the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) released a **statement** entreating financial institutions to exercise extreme caution in the processing of customers' real-time geolocation data.

National Digital ID System, 03 December 2020

The Chamber of Deputies approved the passage of the General Law on Population, Human Mobility and Interculturality, which will establish a national digital ID system. The Cédula Única de Identidad Digital (Unique Digital Identity Card), to be issued by the Mexican Secretariat for Home Affairs (SEGOB), will be the official ID document for all Mexican citizens. Available in both physical and electronic formats, the ID will include citizens' names, date and place of birth, nationality, biometric data and Population Registration Key (CURP) number. The ID will also note whether the holder belongs to an Indigenous or Afro-Mexican community.

Peru

Country Overview

Poverty in Peru has rapidly declined over the past seven years,[119] but the COVID-19 pandemic brought its development progress to a tragic halt. The Andean country has the world's highest COVID-19 death rate per capita,[120] its economy plunged by 11.1%[121] in 2020 and it has been engulfed in political turmoil in the wake of a divisive presidential election. The International Monetary Fund (IMF) predicts a growth rate of 8.5% in 2021,[122] but the ever-changing nature of the pandemic lends uncertainty to this economic outlook.

Meanwhile, Peru lags in its digitalization indicators. The use of cash dominates, 43.6% of adults have little to no computer experience,[123] and in 2019, smartphone penetration stood at 63.9%.[124] While digitalization sped up in response to the COVID-19 pandemic, it also highlighted digital divides across socioeconomic status and geography. Over 90% of rural households do not have an internet connection,[125] and Indigenous communities are especially at risk of being left behind by digital transformation. Going forward, regulators must ensure that digital transformation initiatives dovetail with financial inclusion ones. Innovative technologies like digital identity and mobile banking—alongside improvements to digital infrastructure and mobile broadband access—will be instrumental in helping the country to regain progress lost, foster a competitive and modern economy, and ensure financial inclusion.

The 2021 digital agenda centers on an instant payments network, the creation of a national data protection authority, a fintech sandbox and a national identity document savings account. The Peruvian Securities Market Superintendency (SMV), has approved a new **crowdfunding regulation**, and the country is expected to eventually issue its regulatory framework for fintech.[126] As Peru continues to digitalize, regulators must ensure that cybersecurity and data protection are strengthened in tandem. Peru ranked #85 of 194 states on the Global Cybersecurity Index 2020, developed by the United Nations' International Telecommunication Union (ITU).

Financial Regulatory Authorities

The **Central Reserve Bank of Peru** is the central bank and primary monetary authority in Peru. The bank issues the country's currency, and its main objective is to preserve monetary stability.

The **National Authority for Transparency, Access to Public Information, and Protection of Personal Data** oversees and enforces compliance with the national data protection framework.

OTHER AUTHORITIES

The **Bank of the Nation** represents the Peruvian government in financial transactions across the public and private sectors.

The **Superintendency of Banking, Insurance and AFP (SBS)** is the primary regulator for the financial services sector and provides operational guidance.

The **Superintendency of the Securities Market (SMV)** is the main regulator for the securities market sector in Peru.

The **Secretariat of Digital Government** is the governing body of the National Digital Transformation System and the regulatory authority overseeing digital transformation across the private and public sectors. The Secretariat issues technical standards and guidance on digital initiatives. The Secretariat is comprised of several government agencies, including the Ministry of Economy and Finance and the National Council for Science and Technological Innovation (CONCYTEC).

Policy, Laws and Regulations

National Identity Document Savings Account, 21 July 2021

The Ministry of Economy and Finance (MEF) issued Supreme Decree no. 184-2021-EF, which approved Law no. 31120. The Law establishes and regulates the National Identity Document Savings Account (DNI Account) at the Bank of the Nation, in a move to promote digitalization and financial inclusion. The **DNI** is an identity card issued to Peruvians over the age of 18, and it confers its holders with the right to vote. Individuals wishing to open a DNI Account must provide their DNI number, email, phone number and digital subscription of the account opening contract. The Bank of the Nation will conduct identity verification during the opening and activation of accounts. Public entities may utilize DNI Accounts for payments, transfers and refunds. The Bank of the Nation can close DNI Accounts in the event that they are utilized in illegal activities such as money laundering, terrorist financing, fraud and corruption.[127] As of August 2021, the Bank of the Nation was preparing to open 4 million DNI accounts.[128]

National Data Protection Authority, 09 June 2021

The Council of Ministers signed Law No. 337-2021, which strengthens and unifies national data protection legislation and establishes the National Authority for Transparency, Access to Public Information, and Protection of Personal Data. The agency is authorized to issue sanctions against entities that violate the Law on Transparency and Access to Public Information (Law 27806) and the Law on Protection of Personal Data (Law 29733). In an effort to strengthen the Law on Protection of Personal Data, Law No. 337-2021 also establishes a requirement for large companies that process and store personal data to maintain a Personal Data Officer and report security incidents that involve personal data.[129]

Instant Payments Network, 22 February 2021

Peru is developing an instant payments network connecting fintechs, banks and mobile wallet providers. The project has been spearheaded by Cámara de Compensación Electrónica (CCE), a private clearing house that introduced an Immediate Interbank Transfers (IIT) system in 2016. On 22 February 2021, CCE partnered with ACI Enterprise Payments Platform and Mastercard's Immediate Payments Service in developing the ISO 20022-based network. The ACI Enterprise Payments Platform and Mastercard's Immediate Payments Service collaboration aims to boost participants' connectivity to the system. The network, which seeks in part to bolster financial inclusion, will enter Industry Testing later in 2021[130] and is expected to launch in early 2022.[131]

Legislation

Fintech Sandbox, 26 May 2021

The Superintendency of Banking, Insurance and AFP (SBS) published a proposed law that would establish a financial regulatory sandbox for the development of innovative business models. The sandbox would allow for tests of a twelve-month period.[132]

ENDNOTES

1 Arnold-Parra, Samuel. "Cry for me, Argentina: COVID-19 and Economic Woe." Global Risk Insights, 26 January 2021. https://globalriskinsights.com/2021/01/cry-for-me-argentina-covid-19-and-economic-woe/.

2 Romero, Teresa. "Gross domestic product (GDP) in Latin America and the Caribbean in 2020, by country." Statista, 05 July 2021. https://www.statista.com/statistics/802640/gross-domestic-product-gdp-latin-america-caribbean-country/.

3 "The World Bank in Argentina." The World Bank, 05 April 2021. https://www.worldbank.org/en/country/argentina/overview.

4 "The World Bank in Argentina." The World Bank, 05 April 2021. https://www.worldbank.org/en/country/argentina/overview.

5 Alcoba, Natalie. "Argentina Is the Pandemic's Latest Hot Spot." Foreign Policy, 04 June 2021. https://foreignpolicy.com/2021/06/04/argentina-is-the-pandemics-latest-hot-spot/.

6 Goschenko, Sergio. "Central Bank of Argentina President Hints at Possible Regulation of Bitcoin in Payment Systems." Bitcoin.com, 14 August 2021. https://news.bitcoin.com/central-bank-of-argentina-president-hints-at-possible-regulation-of-bitcoin-in-payment-systems/.

7 Haig, Samuel. "President of Argentina open to Bitcoin and a CBDC, but central bank says no." Cointelegraph, 13 August 2021. https://cointelegraph.com/news/president-of-argentina-open-to-bitcoin-and-a-cbdc-but-central-bank-says-no.

8 Goschenko, Sergio. "President of Argentina Open to Adopting Cryptocurrencies as Legal Tender." Bitcoin.com, 16 August 2021. https://news.bitcoin.com/president-of-argentina-open-to-adopting-cryptocurrencies-as-legal-tender/.

9 "The Global Findex Database 2017." Demirgüç-Kunt, Aslı et al. https://globalfindex.worldbank.org/.

10 "Billeteras Virtuales: nuevas medidas de seguridad para pagos electrónicos." Editorial Errepar, 13 July 2021. https://blog.errepar.com/billeteras-virtuales-nuevas-medidas-de-seguridad-para-pagos-electronicos/.

11 Goschenko, Sergio. "Argentinian Province Misiones Plans to Issue Its Own Stablecoin." Bitcoin.com, 23 July 2021. https://news.bitcoin.com/argentinian-province-misiones-plans-to-issue-its-own-stablecoin/.

12 Malwa, Shaurya. "Argentina's central bank is asking citizens to disclose their Bitcoin." CryptoSlate, 06 April 2021. https://cryptoslate.com/argentinas-central-bank-is-asking-citizens-to-disclose-their-bitcoin/.

13 Engler, Andrés. "Argentine Lawmaker Proposes Bill for Businesses to Pay Employees in Crypto." CoinDesk, 07 July 2021. https://www.coindesk.com/argentine-lawmaker-proposes-bill-for-businesses-to-pay-employees-in-crypto.

14 Nessi, Hernan and Jorge Iorio. "Argentina's annual inflation rate tops 50% as global prices soar." Reuters, 23 July 2021. https://www.reuters.com/world/americas/argentina-inflation-seen-year-low-32-june-likely-reheat-2nd-half-2021-07-15/.

15 Guerin, Orla. "Covid-19 pandemic: 'Everything you should not do, Brazil has done'." BBC News, 09 July 2021. https://www.bbc.co.uk/news/world-latin-america-57733540.

16 "The World Bank in Brazil." The World Bank, 06 April 2021. https://www.worldbank.org/en/country/brazil/overview.

17 McGeever, Jamie. "Brazil GDP drops 4.1% in 2020, COVID-19 surge erodes rebound." Reuters, 03 March 2021. https://www.reuters.com/article/us-brazil-economy-gdp-idUSKBN2AV1FZ.

18 Fonseca, Iolanda. "Brazil out of world's top 10 economies and down to 12th, ranking shows." The Rio Times, 03 March 2021. https://riotimesonline.com/brazil-news/brazil/business-brazil/brazil-out-of-worlds-top-10-economies-and-down-to-12th-ranking-shows/.

19 "Emerging-market policymakers grapple with rising inflation." The Economist, 21 August 2021. https://www.economist.com/finance-and-economics/2021/08/21/emerging-market-policymakers-grapple-with-rising-inflation.

20 "São Paulo has world's 4th largest fintech ecosystem; Montevideo is 2nd fastest-growing fintech city." The Rio Times, 01 August 2021. https://riotimesonline.com/brazil-news/sao-paulo/sao-paulo-has-the-fourth-largest-fintech-ecosystem-in-the-world-montevideo-is-the-second-fastest-growing-fintech-city-globally/.

21 Ando, Lincoln. "A Look Into Brazil's Booming Fintech Scene." Forbes, 09 August 2021. https://www.forbes.com/sites/forbestechcouncil/2021/08/09/a-look-into-brazils-booming-fintech-scene/?sh=68f4d3c572b0.

22 "Brazil's central bank launches regulatory sandbox." Finextra, 06 November 2020. https://www.finextra.com/pressarticle/84854/brazils-central-bank-launches-regulatory-sandbox.

23 Prescott, Roberta. "Brazilian digital banks attract new customers amid pandemic." iupana, 24 June 2021. https://iupana.com/2021/06/24/brazilian-banks/?lang=en.

24 Ando, Lincoln. "A Look Into Brazil's Booming Fintech Scene." Forbes, 09 August 2021. https://www.forbes.com/sites/forbestechcouncil/2021/08/09/a-look-into-brazils-booming-fintech-scene/?sh=68f4d3c572b0.

25 Ando, Lincoln. "A Look Into Brazil's Booming Fintech Scene." Forbes, 09 August 2021. https://www.forbes.com/sites/forbestechcouncil/2021/08/09/a-look-into-brazils-booming-fintech-scene/?sh=68f4d3c572b0.

26 Mari, Angelica. "Digital Services Surge Among Poor Brazilians Amid Pandemic." Forbes, 10 November 2020. https://www.forbes.com/sites/angelicamarideoliveira/2020/11/10/digital-services-surge-among-poor-brazilians-amid-pandemic/?sh=397a65b568b0.

27 Kaaru, Steve. "Brazil's central bank eyes regulation for digital currencies." CoinGeek, 26 August 2021. https://coingeek.com/brazil-central-bank-eyes-regulation-for-digital-currencies/.

28 "Brazil continues to be a hotspot for cybercrime – Accenture." Smart Energy International, 12 January 2021. https://www.smart-energy.com/industry-sectors/cybersecurity/brazil-continues-to-be-a-hotspot-for-cybercrime-accenture/.

29 Mari, Angelica. "Open Banking kicks off in Brazil." ZDNet, 01 February 2021. https://www.zdnet.com/article/open-banking-kicks-off-in-brazil/.

30 "Brazil's cenbank postpones phase 2 of Open Banking to August." Latin America Business Stories, 14 July 2021. https://labsnews.com/en/news/economy/set-to-begin-this-thursday-brazils-cenbank-postpones-phase-2-of-open-banking/.

31 "Brazil's Central Bank postpones open banking's third phase at the request of institutions and fintechs." Latin America Business Stories, 27 August 2021. https://labsnews.com/en/news/economy/brazils-central-bank-postpones-open-bankings-third-phase/.

32 Mari, Angelica. "Customer data sharing under Open Banking commences in Brazil." ZDNet, 13 August 2021. https://www.zdnet.com/article/customer-data-sharing-under-open-banking-commences-in-brazil/.

33 Mari, Angelica. "Brazil announces national data protection council." ZDNet, 11 August 2021. https://www.zdnet.com/article/brazil-announces-national-data-protection-council/.

34 Sinclair, Sebastian. "BCB said the timeframe for a CBDC depends on the evolution of its current projects and the international landscape." CoinDesk, 24 August 2021. https://www.coindesk.com/markets/2021/06/11/brazils-central-bank-pushes-back-target-date-on-cbdc-by-two-years/.

35 Lowe, Josh. "Brazil launches national AI strategy." Global Government Forum, 13 April 2021. https://www.globalgovernmentforum.com/brazil-launches-national-ai-strategy/.

36 Lowe, Josh. "Brazil launches national AI strategy." Global Government Forum, 13 April 2021. https://www.globalgovernmentforum.com/brazil-launches-national-ai-strategy/.

37 Pompeo, Carolina. "Brazil's PIX: in six months, 87.3 million users and a 3.299% rise in P2B transactions." Latin America Business Stories, 21 May 2021. https://labsnews.com/en/articles/business/brazils-pix-in-six-months-87-3-million-users-and-a-3-299-rise-in-p2b-transactions/.

38 "Chile." The World Bank. https://data.worldbank.org/country/CL.

39 "OECD Economic Surveys: Chile." OECD, February 2021. https://www.oecd.org/economy/surveys/Chile-2021-OECD-economic-survey-overview.docx.pdf.

40 "The World Bank in Chile." The World Bank, 08 April 2021. https://www.worldbank.org/en/country/chile/overview.

41 "Chile: focus on reducing inequality to strengthen social and economic recovery from COVID-19." OECD. https://www.oecd.org/newsroom/chile-focus-on-reducing-inequality-to-strengthen-social-and-economic-recovery-from-covid-19.htm.

42 "The World Bank in Chile." The World Bank, 08 April 2021. https://www.worldbank.org/en/country/chile/overview.

43 "Chile: focus on reducing inequality to strengthen social and economic recovery from COVID-19." OECD. https://www.oecd.org/newsroom/chile-focus-on-reducing-inequality-to-strengthen-social-and-economic-recovery-from-covid-19.htm.

44 "OECD Economic Surveys: Chile 2021—2. Making digital transformation work for all in Chile." OECD, 2021. https://www.oecd-ilibrary.org/sites/4c7db951-en/index.html?itemId=/content/component/4c7db951-en.

45 Seminario, Fabiola. "Chile heads towards open finance regulation." iupana, 19 April 2021. https://iupana.com/2021/04/19/chile-heads-towards-open-finance-regulation/?lang=en.

46 Kemp, Simon. "Digital 2021: Chile." DataReportal, 11 February 2021. https://datareportal.com/reports/digital-2021-chile.

47 "Con 67 empresas nuevas, el ecosistema Fintech en Chile crece a un ritmo de 38% anual, llegando a las 179 startups en 2021." Finnovista, 04 May 2021. https://www.finnovista.com/radar/con-67-empresas-nuevas-el-ecosistema-fintech-en-chile-crece-a-un-ritmo -de-38-anual-llegando-a-las-179-startups-en-2021/.

48 Pasquali, Marina. "Statistics and facts on fintech in Chile." Statista, 02 July 2021. https://www.statista.com/topics/7831/fintech-in-chile/.

49 Seminario, Fabiola. "Chile heads towards open finance regulation." iupana, 19 April 2021. https://iupana.com/2021/04/19/chile-heads-towards-open-finance-regulation/?lang=en.

50 "OECD Economic Surveys: Chile 2021—2. Making digital transformation work for all in Chile." OECD, 2021. https://www.oecd-ilibrary.org/sites/4c7db951-en/index.html?itemId=/content/component/4c7db951-en.

51 "Chile to have a National Artificial Intelligence Policy." InvestChile, 01 February 2021. http://blog.investchile.gob.cl/chile-to-have-a-national-artificial-intelligence-policy.

52 "Ministerio de Ciencia abre consulta pública para la Política Nacional de Inteligencia Artificial." Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, 15 December 2020. https://www.minciencia.gob.cl/noticias/ministerio-de-ciencia-abre-consulta-publica-para-la-politica-nacional-de-inteligencia-artificial/.

53 "Ministerio de Ciencia abre consulta pública para la Política Nacional de Inteligencia Artificial." Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, 15 December 2020. https://www.minciencia.gob.cl/noticias/ministerio-de-ciencia-abre-consulta-publica-para-la-politica-nacional-de-inteligencia-artificial/.

54 "CMF publishes Fintech Act proposal for the securities market." Comisión para el Mercado Financiero. https://www.cmfchile.cl/portal/principal/613/w3-article-46998.html.

55 Guzmán, Francisco and Andrés Latorre. "CMF publishes "Fintech Law" proposal." Carey y Cía. Ltda, 14 February 2021. https://www.carey.cl/en/cmf-publishes-fintech-law-proposal/.

56 Daniels, Joe Parkin. "'They can't take it any more': pandemic and poverty brew violent storm in Colombia." The Guardian, 07 May 2021. https://www.theguardian.com/global-development/2021/may/07/colombia-protests-police-covid-poverty-violence.

57 "Pandemic pushes 3.6 million Colombians into poverty." The City Paper Bogota, 01 May 2021. http://thecitypaperbogota.com/news/pandemic-pushes-3-6-million-colombians-into-poverty/27316.

58 "Colombia: Overview." World Bank, 24 March 2021. https://www.worldbank.org/en/country/colombia/overview.

59 Lustman, Stu. "Colombia: Land of Fintech Opportunity." Colombia Fintech, 08 September 2021. https://www.colombiafintech.co/novedades/colombia-land-of-fintech-opportunity.

60 "Latin America Sees Booming Digital Banking Sector with Brazil at the Lead." FintechNews, 19 July 2021. https://fintechnews.ch/latin-america/latin-america-sees-booming-digital-banking-sector-with-brazil-at-the-lead/47312/.

61 "Latin America Sees Booming Digital Banking Sector with Brazil at the Lead." FintechNews, 19 July 2021. https://fintechnews.ch/latin-america/latin-america-sees-booming-digital-banking-sector-with-brazil-at-the-lead/47312/.

62 Yansura, Julia et al. "Is Online Banking Reducing Poverty in Latin America?" The Dialogue: Financial Services Advisor, 02 December 2020. https://www.thedialogue.org/analysis/is-online-banking-reducing-poverty-in-latin-america/.

63 "Colombia reportedly takes voluntary approach to Open Banking." The Paypers, 28 April 2021. https://thepaypers.com/online-mobile-banking/colombia-reportedly-takes-voluntary-approach-to-open-banking--1248657.

64 Seminario, Fabiola. "Open banking in Colombia is getting ready to take off." iupana, 08 February 2021. https://iupana.com/2021/02/08/open-banking-in-colombia/?lang=en.

65 García Santiago, Héctor José. "Transition to the digital ID card: closing the digital divide in Colombia." Digital Future Magazine, 20 January 2021. https://www.digitalfuturemagazine.com/2021/01/20/transition-to-the-digital-id-card-closing-the-digital-divide-in-colombia/.

66 "Individuals using the Internet (% of population) – Colombia." World Bank, 2019. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CO.

67 Ozores, Pedro. "Colombia betting on digital transformation to drive economic recovery." BNamericas, 30 April 2021. https://app.bnamericas.com/article/section/all/content/xolluh3kd-digital-transformation-colombias-bet-to-fuel-economic-recovery.

68 "The cheapest (and most expensive) mobile data packages." Telecom Lead, 09 August 2021. https://www.telecomlead.com/broadband/the-cheapest-and-most-expensive-mobile-data-packages-101215.

69 "Updates to Electronic Invoicing in Colombia: Digital Signature and New Technical Rules." Edicom, 31 March 2021. https://www.edicomgroup.com/en_US/news/15026-updates-to-electronic-invoicing-in-colombia-digital-signature-and-new-technical-rules.html.

70 "E-invoicing & Digital Reporting Global Updates." KPMG, 11 August 2021. https://assets.kpmg/content/dam/kpmg/us/pdf/2021/03/e-invoicing-digital-reporting-global-updates.pdf.

71 "E-invoicing & Digital Reporting Global Updates." KPMG, 11 August 2021. https://assets.kpmg/content/dam/kpmg/us/pdf/2021/03/e-invoicing-digital-reporting-global-updates.pdf.

72 Handagama, Sandali. "Colombia's Crypto Use Soars, and Local Regulators Step In." CoinDesk, 30 April 2021. https://www.coindesk.com/colombias-crypto-use-soars-and-local-regulators-step-in.

73 "The World Bank in Dominican Republic." The World Bank, 10 June 2021. https://www.worldbank.org/en/country/dominicanrepublic/overview.

74 "IMF Staff Completes 2021 Article IV Mission to the Dominican Republic." International Monetary Fund, 06 May 2021. https://www.imf.org/en/News/Articles/2021/05/06/pr21122-dominican-republic-imf-staff-completes-2021-article-iv-mission-to-the-dominican-republic.

75 "The World Bank in Dominican Republic." The World Bank, 10 June 2021. https://www.worldbank.org/en/country/dominicanrepublic/overview.

76 Chevalier, Stephanie. "Statistics and facts about internet usage in the Dominican Republic." Statista, 08 March 2021. https://www.statista.com/topics/6244/internet-usage-in-the-dominican-republic/.

77 "Dominican Republic to improve digital connectivity with $115 million IDB loan." Inter-American Development Bank, 13 July 2021. https://www.iadb.org/en/news/dominican-republic-improve-digital-connectivity-115-million-idb-loan.

78 Wirtz, Nic. "Fintech thriving in CentAm but legislative support needed." BNamericas, 15 April 2021. https://app.bnamericas.com/article/section/all/content/xwwvjsqov-fintech-thriving-in-centam-but-needs-legislative-support.

79 "Dominican Republic." United Nations World Food Programme. https://www.wfp.org/countries/dominican-republic.

80 "53.69% of Dominicans don't have a bank account; poll." Dominican Today, 24 March 2021. https://dominicantoday.com/dr/economy/2021/03/24/53-69-of-dominicans-dont-have-a-bank-account-poll/.

81 Sans, Mariana and Pamela Madrid. "Four Charts on the Dominican Republic's Crisis Response and Recovery." International Monetary Fund, 28 July 2021. https://www.imf.org/en/News/Articles/2021/07/08/na071221-four-charts-on-the-dominican-republics-crisis-response-and-recovery.

82 "Central Bank announces the creation of a Financial Innovation Hub." Dominican News, 20 May 2021. https://dominican.news/money/central-bank-announces-the-creation-of-a-financial-innovation-hub/.

83 "AGENDA DIGITAL DE LA REPÚBLICA DOMINICANA 2030." Digital Transformation Cabinet, May 2021.

84 "The World Bank in Guatemala." The World Bank. https://www.worldbank.org/en/country/guatemala/overview.

85 "The World Bank in Guatemala." The World Bank. https://www.worldbank.org/en/country/guatemala/overview.

86 "Guatemala." International Monetary Fund. https://www.imf.org/en/Countries/GTM.

87 "Guatemala declares state of emergency over Delta Covid surge." The Tico Times, 14 August 2021. https://ticotimes.net/2021/08/14/guatemala-declares-state-of-emergency-over-delta-covid-surge.

88 Drees-Gross, Franz and Pepe Zhang. "Less than 50% of Latin America has fixed broadband. Here are 3 ways to boost the region's digital access." World Economic Forum, 21 July 2021. https://www.weforum.org/agenda/2021/07/latin-america-caribbean-digital-access/.

89 "Latin American Economic Outlook 2020 : Digital Transformation for Building Back Better—Guatemala." OECD iLibrary, https://www.oecd-ilibrary.org/sites/af413327-en/index.html?itemId=/content/component/af413327-en.

90 "Digital aid becomes lifeline for unbanked Guatemalans during pandemic." Visa, 11 August 2021. https://usa.visa.com/visa-everywhere/blog/bdp/2021/08/10/digital-aid-becomes-1628637832007.html.

91 "Share of adult population with credit cards in Guatemala between 2011 and 2017, by gender." Statista. Statista Research Department, 02 July 2021. https://www.statista.com/statistics/865992/credit-card-ownership-rate-gender-guatemala/.

92 "Investigation reveals serious concerns over Guatemala COVID-19 app." Global Witness, 14 May 2020. https://www.globalwitness.org/en/press-releases/investigation-reveals-serious-concerns-over-guatemala-covid-19-app/.

93 "Ley para la simplificación de requisitos y trámites administrativos – Decreto 5-2021." Inbers, 26 June 2021. https://www.inbers.com/ley-para-la-simplificacion-de-requisitos-y-tramites-administrativos-decreto-5-2021/.

94 del Valle, Luis Pedro and Marco Tulio León. "The law for the simplification of administrative requirements and procedures was approved." Lexology, 28 July 2021. https://www.lexology.com/library/detail.aspx?g=0743a65d-27af-47a3-b2b3-0866df8bd332.

95 Curruchich, Selvyn. "Preparan camino del quetzal digital." Diario de Centro América, 03 August 2021. https://dca.gob.gt/noticias-guatemala-diario-centro-america/preparan-camino-del-quetzal-digital/.

96 Curruchich, Selvyn. "Preparan camino del quetzal digital." Diario de Centro América, 03 August 2021. https://dca.gob.gt/noticias-guatemala-diario-centro-america/preparan-camino-del-quetzal-digital/.

97 McDonald, Michael. "Guatemala Central Bank Weighs Launch of its Own Digital Currency." Bloomberg Law, 24 June 2021. https://news.bloomberglaw.com/banking-law/guatemala-central-bank-weighs-launch-of-its-own-digital-currency.

98 "The World Bank in Mexico." The World Bank, 29 March 2021. https://www.worldbank.org/en/country/mexico/overview.

99 Zaga, Daniel et al. "Mexico: An exports-led recovery." Deloitte, 17 June 2021. https://www2.deloitte.com/us/en/insights/economy/americas/mexico-economic-outlook.html.

100 Graham, Dave. "Mexico's economy in 2020 suffers worst slump since 1930s." Reuters, 29 January 2021. https://www.reuters.com/article/us-mexico-economy-gdp-idUSKBN29Y1OF.

101 "Poverty increases in Mexico amid COVID-19 pandemic." The Washington Post, 05 August 2021. https://www.washingtonpost.com/world/poverty-increases-in-mexico-amid-covid-19-pandemic/2021/08/05/ebd45206-f62b-11eb-a636-18cac59a98dc_story.html.

102 "Pandemic drove 3.8 million more Mexicans into poverty status: Coneval report 2018-2020." The Yucatan Times, 06 August 2021. https://www.theyucatantimes.com/2021/08/pandemic-drove-3-8-million-more-mexicans-into-poverty-status-coneval-report-2018-2020.

103 "Mexico." International Monetary Fund. https://www.imf.org/en/Countries/MEX.

104 "Foreign Direct Investment in Latin America and the Caribbean." The Economic Commission for Latin America and the Caribbean, 05 August 2021. https://repositorio.cepal.org/bitstream/handle/11362/47148/1/S2100464_en.pdf.

105 Arce Lozano, René and Dinorah Cantu. "Mexico: The Mexican Fintech Ecosystem." Mondaq, 01 March 2021. https://www.mondaq.com/mexico/fin-tech/1041174/the-mexican-fintech-ecosystem.

106 Mascellino, Alessandro. "Mexico approves rollout of national biometric digital ID card." Biometric Update, 07 December 2020. https://www.biometricupdate.com/202012/mexico-approves-rollout-of-national-biometric-digital-id-card.

107 "Latin America Sees Booming Digital Banking Sector with Brazil at the Lead." FintechNews, 19 July 2021. https://fintechnews.ch/latin-america/latin-america-sees-booming-digital-banking-sector-with-brazil-at-the-lead/47312/.

108 Belmont, Jessica. "Expanding Financial Access for Mexico's Poor and Supporting Economic Sustainability." The World Bank, 09 April 2021. https://www.worldbank.org/en/results/2021/04/09/expanding-financial-access-for-mexico-s-poor-and-supporting-economic-sustainability.

109 Bambysheva, Nina and Maria Abreu. "Mexican Bitcoin Exchange Bitso Raises $250 Million, Becomes Latin America's First Crypto Unicorn." Forbes, 05 May 2021. https://www.forbes.com/sites/ninabambysheva/2021/05/05/mexican-bitcoin-exchange-bitso-raises-250-million-becomes-latin-americas-first-crypto-unicorn/?sh=2ca0e37764af.

110 Seminario, Fabiola. "Open Banking in LatAm: The State of Play." iupana, 22 February 2021. https://iupana.com/2021/02/22/open-banking-in-latam.

111 "Senate approves cell phone users registry that will collect biometric data." Mexico News Daily, 14 April 2021. https://mexiconewsdaily.com/news/senate-approves-biometric-cell-phone-users-registry/.

112 "Cell Phone Users in Mexico Have Two Years to Submit Their Biometric Data to the Government or Lose Service." Vallarta Daily, 17 April 2021. https://www.vallartadaily.com/cell-phone-users-in-mexico-have-two-years-to-submit-their-biometric-data-to-the-government-or-lose-service/.

113 Young, James. "Mexican banks implement digital security requirements." BNamericas, 25 March 2021. https://app.bnamericas.com/article/section/all/content/xddfqszi4-biometrics-next-in-mexico-banking-security-regulatory-rollout.

114 "Data breaches in Mexico raises concerns about biometric requirements." NewTechMag.Net, 03 February 2021. http://newtechmag.net/2021/02/03/data-breaches-in-mexico-raises-concerns-about-biometric-requirements/.

115 Lechuga Perezanta, Cesar Armando. "Data Protection and Cybersecurity Laws in Mexico." CMS, 19 February 2021. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/mexico.

116 Rodríguez, Ariel. "What are Mexico's public sector vulnerabilities to cyber attacks?" BNamericas, 29 January 2021. https://app.bnamericas.com/article/section/all/content/x0f4bjibw-what-are-mexicos-public-sector-vulnerabilities-to-cyber-attacks.

117 Young, James. "Mexico banking watch: Geo-location rule, Sabadell unit, NBFI update." BNamericas, 19 March 2021. https://app.bnamericas.com/article/section/all/content/xb66dpzks-banking-watch-mex-geo-location-requirement-going-into-effect-march-23.

118 Young, James. "Mexican banks implement digital security requirements." BNamericas, 25 March 2021. https://app.bnamericas.com/article/section/all/content/xddfqszi4-biometrics-next-in-mexico-banking-security-regulatory-rollout.

119 "Poverty headcount ratio at national poverty lines (% of population) – Peru." The World Bank. https://data.worldbank.org/indicator/SI.POV.NAHC?locations=PE.

120 Horton, Jake. "Covid: Why has Peru been so badly hit?" BBC, 01 June 2021. https://www.bbc.co.uk/news/world-latin-america-53150808.

121 "The World Bank in Peru." World Bank, 09 April 2021. https://www.worldbank.org/en/country/peru/overview

122 "Peru." International Monetary Fund. https://www.imf.org/en/Countries/PER.

123 "Latin American Economic Outlook 2020 : Digital Transformation for Building Back Better—Chapter 3. The digital transformation for all." OECD iLibrary. https://www.oecd-ilibrary.org/sites/e7a00fd6-en/index.html?itemId=/content/component/e7a00fd6-en.

124 "Smartphone household penetration rate in Peru between 2012 and 2019." Statista Research Department, 02 July 2021. https://www.statista.com/statistics/802247/peru-smartphone-household-penetration/.

125 "Universalizing access to digital technologies to address the consequences of COVID-19." United Nations Economic Commission for Latin America and the Caribbean, 26 August 2020. https://repositorio.cepal.org/bitstream/handle/11362/45939/5/S2000549_en.pdf.

126 Seminario, Fabiola. "Crowdfunding in Peru: New rules add to LatAm's fintech regulation push." Iupana, 14 June 2021. https://iupana.com/2021/06/14/crowdfunding-in-peru-new-rules-add-to-latams-fintech-regulation-push/?lang=en.

127 "Banco de la Nación creará la Cuenta DNI para ciudadanos en base a información de Reniec." El Comercio, 21 July 2021. https://elcomercio.pe/economia/peru/cuenta-dni-banco-de-la-nacion-creara-cuentas-para-ciudadanos-en-base-a-informacion-de-reniec-nndc-noticia/.

128 “Banco de la Nación abrirá 4 millones de cuentas DNI.” El Peruano, 22 August 2021. https://elperuano.pe/noticia/127364-banco-de-la-nacion-abrira-4-millones-de-cuentas-dni.

129 “Aprueban proyecto que fortalece entidades y promueve la transparencia, el acceso a información pública y la protección de datos personales.” Gobierno del Perú, 10 June 2021. https://www.gob.pe/institucion/minjus/noticias/499840-aprueban-proyecto-que-fortalece-entidades-y-promueve-la-transparencia-el-acceso-a-informacion-publica-y-la-proteccion-de-datos-personales.

130 “Mastercard and ACI Worldwide to provide real-time payments plumbing in Peru.” Finextra, 22 February 2021. https://www.finextra.com/pressarticle/86264/mastercard-and-aci-worldwide-to-provide-real-time-payments-plumbing-in-peru.

131 Arnfield, Robin. “Peru plans instant payments network that links fintechs, mobile bank accounts.” American Banker, 31 March 2021. https://www.americanbanker.com/payments/news/peru-plans-instant-payments-network-that-links-fintechs-mobile-bank-accounts.

132 “The fintech industry is making inroads in Latin America with new legislation.” Garrigues, 06 June 2021. https://www.garrigues.com/en_GB/new/fintech-industry-making-inroads-latin-america-new-legislation.

Europe

Europe is home to some of the world's most digitalized societies and robust fintech hotspots, but it is at risk of losing ground to both established and emerging fintech powerhouses across Asia. Still, European governments are spearheading ambitious plans in central bank digital currency (CBDC), digital identity, artificial intelligence and digital transformation at large, which will be invaluable in spurring on intraregional and international competition. Northern European states like Denmark, Finland, the Netherlands and Sweden will be ones to watch as they increasingly attract investment funds and exciting new entrants to their respective fintech ecosystems. Poland has also become a major fintech player in Central and Eastern Europe, and the rise of digital payments in the traditionally cash-reliant country could promote financial inclusion and economic growth. Established fintech ecosystems like London and Berlin remain strong, and even Brexit has not deterred fintech growth in the United Kingdom. In the first half of 2021, the British fintech sector raised USD$5.7 billion—the world's second-highest amount of funds secured.[1]

Much of Europe's regulatory activity stems from the European Union, which has been particularly progressive in spearheading digital transformation. The European Commission's proposed European Digital Identity, AML/CFT legislative package, Digital Finance Strategy and Artificial Intelligence Regulation will continue through the legislative process in 2022, and could be enacted in just a few years. The effects of these regulations will not be confined to the member states, however, as EU regulations often become an international standard. Three years after the passage of the General Data Protection Regulation (GDPR), jurisdictions around the world have rushed to emulate it, and even businesses outside the EU are subject to its requirements. The proposed Artificial Intelligence Regulation will similarly have extraterritorial effect, and it is poised to have far-reaching influence regarding the legal and ethical implications of AI.

Going into 2022, digitalization initiatives will drive national pandemic recovery plans, and even states that have stalled in their digital transformation progress will have a chance to catch up. Although Europe faces steep competition in fintech, its strong cybersecurity and data protection standards, wealth, and political and financial stability will ensure that the region remains a key force in the global digital economy.

Regulatory Bodies

The European Central Bank (ECB) is the central bank for the Eurozone, the 19 EU countries that have adopted the euro. The ECB's main objective is to safeguard the purchasing power of the euro and maintain financial stability in Europe, though it gives occasional guidance regarding consumer data protection and privacy.

Other Financial Agencies

The European Banking Authority (EBA) is the EU's primary regulatory authority based in Paris. The EBA supervises financial institutions across the European banking sector and develops regulations to safeguard financial institutions from risk and address vulnerabilities.

The European Investment Bank (EIB) is a publicly-owned EU financial institution that was established as a "policy-driven bank" advancing various EU projects and programs, mostly related to social initiatives.

Other EU Agencies

The European Commission (EC) is the executive branch of the EU that sustains EU treaties, proposes legislation and manages day-to-day operations of the EU.

The European Union Agency for Cybersecurity (ENISA) is the EU's dedicated cybersecurity agency with jurisdiction across Europe. The agency was mandated by the EU Cybersecurity Act and established in 2004. The agency develops and disseminates cross-sectoral cybersecurity policies.

The European Data Protection Board (EDPB) is the EU's data protection agency with supervisory jurisdiction over 27 member states; Iceland, Liechtenstein and Norway are the most recent members. The EDPB's oversight includes supervision of uniform GDPR application and compliance. It accomplishes this through cybersecurity coordination between member states.

The European Data Protection Supervisor (EDPS) is another independent EU data protection authority. Headed by an elected supervisor, the EDPS's goal is to ensure personal data protection and privacy when any EU institution processes personal information; it also advises EU institutions on personal data processing.

Standards, Laws and Regulations

EUROPEAN COMMISSION

European Commission Unveils AML/CFT Legislative Package, 20 July 2021

The European Commission unveiled a comprehensive AML/CFT legislative package, which aims to strengthen the existing framework, improve the detection of suspicious transactions and activities, close loopholes that enable criminal activity and harmonize the AML/CFT approach across the EU. The package includes four legislative proposals:

1. The **Regulation** establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010: this regulation would establish an EU-wide Authority for Anti-Money Laundering (AMLA). AMLA would supervise financial transactions and spearhead cooperation with national supervisors and national financial intelligence units. The authority is expected to be operational in 2024, with its direct supervision work to begin in 2026.[2]
2. The **Regulation** on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing: this regulation would expand the list of obliged entities to include cryptoasset service providers, streamline beneficial ownership requirements, impose new requirements on the processing of certain categories of personal data and clarify requirements on customer due diligence.
3. The **Regulation** on information accompanying transfers of funds and certain crypto-assets (recast): this regulation would extend traceability requirements to cryptoassets.
4. The **Directive** on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/84: this directive aims to promote a harmonized approach to AML/CFT and strengthen cooperation amongst financial intelligence units (FIUs), supervisors and other authorities.

Jan Ceyssens, the European Commission's Head of the Digital Finance unit, stated that "[MiCA and the new AML/CFT legislative package] will be two sides of the same coin, so that operators in this space, whether that is issuers, service providers, wallet providers, or trading venues are subject to the same set of rules throughout the EU."[3] The package will now proceed to discussion between the European Parliament and the Council.

European Commission Proposes Framework for European Digital Identity, 03 June 2021

The European Commission proposed a framework for a European Digital Identity, which will allow citizens, residents and businesses to access public and private services across the EU, even offline. According to the press release, "Under the new Regulation, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (e.g. driving licence, diplomas, bank account). These wallets may be provided by public authorities or by private entities, provided they are recognised by a Member State. The new European Digital Identity Wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they will have full control of the data they share." The proposal aims to reduce fraud, promote trust in e-commerce and facilitate the access to services across member states.[4]

EU Adequacy Decision for the UK on Cross-Border Transfers of Personal Data, 28 June 2021

The European Commission adopted an adequacy decision under the GDPR allowing for the free flow of personal data between the EU and the UK. The adequacy decision includes a sunset clause, which caps the duration of the adequacy at four years, in the case that UK personal data protection standards diverge.

EU and US Release Joint Statement on EU-US Privacy Shield: Revamping Negotiations, 25 March 2021

Per a joint statement issued by European Commissioner for Justice Didier Reynders and US Secretary of Commerce Gina Raimondo, the EU and US have decided to revamp negotiations towards an EU-US Privacy Shield in compliance with the 20 July 2020 European Union Court of Justice (EUCJ) judgment in the Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II) case. The Schrems II case struck down the former EU-US Privacy Shield that allowed cross-border transfers between the jurisdictions. Per an argument by the Irish Data Protection Commission, the EU Standard Contractual Clauses for the transfer of personal data to processors outside the EU/EEA (SCCs) could not protect personal data from NSA and other US government agency surveillance. Increasing suspicion towards American interference was influenced in part by NSA whistleblower Edward Snowden's 2013 revelations.

European Commission Publishes Communication on the 2030 Digital Compass, 09 March 2021

The European Commission presented the 2030 Digital Compass: the European way for the Digital Decade, a vision that seeks to make Europe a digital leader by 2030. The vision hinges on four main tenets: digital empowerment of EU citizens, security and sustainability in digital infrastructures, the digitalization of business and digitalization of public services. Regarding digitalization in business, the EU aims to create a more attractive landscape functional for startups, which will include a more integrated and operational Single Market and boosting access to finance. With its usual mind towards fairness and leveling out the playing field, the communication also speaks to the importance of small and medium-sized enterprises (SME) in the growth of the digital ecosystem. By 2030, the vision aims for SMEs to have achieved fair and easy access to digital technologies through the support of over 200 Digital Innovation Hubs and industrial clusters. Furthermore, 75% of European enterprises will have adopted cloud computing services, big data and AI and 80% of EU citizens will be utilizing an e-ID per the Commission's goals. The fintech industry will especially benefit from this increasing amenability to and demand for the integration of technology into business and everyday life.

EUROPEAN PARLIAMENT

European Parliament Adopts Resolution on Commission Evaluation Report on Implementation of GDPR, 25 March 2021

The resolution on the European Commission's evaluation report, which comes two years after the GDPR's implementation, concludes that the regulation has been an "overall success," with no need for revisions or updates. The resolution pays particular attention to EU citizens' increasing awareness of their rights with regard to data protection, and the GDPR's influence in sparking similar initiatives worldwide.

COUNCIL OF THE EUROPEAN UNION

Adoption of Retail Payments Strategy, 22 March 2021

The Council adopted the **Retail Payments Strategy**, first proposed in September 2020 by the Commission as part of the Digital Finance Package. The strategy hinges on four pillars:

innovation and competition in payments markets, facility of cross-border payments, interoperable payment systems and digital, instant payment systems across the EU. Per the Council's press release, "The Council also highlights the many challenges to be taken into account when further developing and regulating the market, such as financial inclusion, security and consumer protection, data protection and anti-money laundering aspects."

Adoption of Cybersecurity Strategy, 16 December 2020

The Council adopted a cybersecurity strategy that "aims to safeguard a global and open Internet by harnessing and strengthening all tools and resources to ensure security and protect European values and the fundamental rights of everyone."[5] The strategy is ambitious and broad in scope. One of the primary initiatives includes an EU-wide Cyber Shield, a network of Security Operations Centres that will employ AI and machine learning to detect and deter cyberattacks at an early stage. The European Commission is also spearheading a **Joint Cyber Unit** to bolster cooperation between EU member states and EU authorities. The Joint Cyber Unit will help to share information on the threat landscape with relevant stakeholders, as well as coordinate responses to attacks, especially cross-border ones. The Commission aims for the Joint Cyber Unit to be operational by June 2022 and fully functional by June 2023.[6]

MEMBER STATES

Compliance with the 6th Anti-Money Laundering Directive, 03 June 2021

Regulated entities operating in the EU were required to be compliant with the 6th Anti-Money Laundering Directive (6AMLD) by 3 June 2021. The 6AMLD aims to expand the scope of previous AML directives, harmonize the AML approach across member states, impose stricter penalties and close loopholes in national legislation. It standardized the definition of money laundering across the EU, resulting in a list of 22 predicate offenses which must be criminalized by member states. This has required financial institutions to finetune their KYC, CDD and transaction monitoring processes to ensure its scope applies and encompasses the broadened money laundering definition. Harsher criminal liability will also crack down on any "legal persons" involved, which extends to companies, partnerships, consultants, accountants or others acting on behalf of an entity. Furthermore, because money laundering is often transnational, the 6AMLD implements information-sharing requirements to aid EU states in adopting a facilitated and harmonized approach to prosecution.

Member States Sign Berlin Declaration on Digital Society and Values-Based Digital Government, 08 December 2020

The Berlin Declaration—signed by relevant ministers of all member states—affirms the pursuit of an inclusive digital transformation and modernized Single Market, and outlines a generalized strategy in achieving progress by 2024. The EU's Fundamental Charter of Human Rights heavily underpins the declaration's vision, which spells out seven principles in guiding digitalization:

- Validity and respect of fundamental rights and democratic values
- Social participation and digital inclusion to shape the digital world
- Empowerment and digital literacy
- Trust and security in digital government interactions
- Digital sovereignty and interoperability
- Human-centred systems and innovative technologies in the public sector
- Towards a resilient and sustainable digital society

The declaration outlines strategies and member states' commitments towards each principle, alongside a call upon the European Commission and other EU institutions to implement actions per their competences. Key points include:

- "taking steps to make widely usable, secure and interoperable electronic identification and trust services for electronic transactions available for each European resident and providing trustworthy, user-centric, accessible and reliable public services and information"
- "agreeing on common European requirements for technology providers and solutions in the public sector (including security, data protection, interoperability, reusability) by accommodating existing requirements of the EU and Member States"
- "working towards developing an EU-wide Digital Identity framework allowing citizens and businesses to securely and seamlessly access online public and private services, while minimising disclosure and retaining full control of data"
- "agreeing on common European requirements for technology providers and solutions in the public sector (including security, data protection, interoperability, reusability) by accommodating existing requirements of the EU and Member States"[7]

The declaration reiterates its commitment to digital sovereignty, data protection, a secure cloud infrastructure, ethical AI and facilitating the flow of public-sector data. The EU's increasingly well-articulated digital vision and strengthening regulatory framework points to an attractive landscape for fintech, although stringent non-compliance measures and oversight—alongside strict data localization and other data protection measures—might dissuade some entities from entering the scene. On the user end, digital inclusion measures will be instrumental in increasing the use of cashless electronic payments, online banking and remote customer onboarding, and digital authentication.

EUROPEAN CENTRAL BANK

Investigation Phase on Digital Euro, 14 July 2021

The European Central Bank's Governing Council approved the investigation phase of a digital euro project, which will run for about two years with a subsequent three-year implementation period. The digital euro will function as legal tender issued by the ECB and complement the use of banknotes and coins in the 19-country Eurozone, and it could operate alongside a digital wallet. The endeavor seeks to counter the rising influence of privately-issued digital currencies like Bitcoin and Ethereum, especially as cash use continues to decline. The ECB will now focus on the technical design of the digital euro in consultation with a variety of stakeholders, and will confer with lawmakers in addressing the need for potential legislative changes.

On 14 April 2021, the ECB published the **Eurosystem report on the public consultation on a digital euro**. The consultation revealed that respondents most prioritize privacy, with 43% of them ranking it number one. Trailing behind are "security (18%), the ability to pay across the euro area (11%), no additional costs (9%) and offline usability (8%)."[8] Most people supported the integration of a digital euro into banking and payment systems already in existence. The consultation, which garnered 8,221 responses, revealed generally positive support for the development of a digital euro, and the ECB reiterated the importance of accommodating people's "evolving needs" and the economy as a whole. As for safeguarding against risks to financial stability, ECB board member Fabio Panetta has raised the possibility that digital euro accounts be capped at EUR 3000 (approximately USD$3548) to prevent bank runs.[9]

EUROPEAN BANKING AUTHORITY

European Banking Authority Launches Public Consultation on Draft Regulatory Technical Standards on AML/CFT, 06 May 2021

The European Banking Authority launched a public consultation on draft Regulatory Technical Standards (RTS) in the establishment of a central database on anti-money laundering and counter-financial terrorism. The draft RTS lays out rules safeguarding the effectiveness and confidentiality of the database, which would help to coordinate and harmonize the EU approach to AML/CFT. This is especially important as EU AML directives are discretionary—allowing member states to transpose them onto national law and implement them in different ways—which has not necessarily allowed for a pan-European approach. As cybercrime becomes more sophistication and international amidst increasing digitalization, a central database will streamline AML/CFT measures across the EU. The RTS will further ensure that the database adheres to data protection laws. The deadline for comments was 17 July 2021.

2021 may be referred to as the year of evaluation of Central Bank Digital Currencies. The European Central Bank is one of over a dozen jurisdictions that have invested resources to thoroughly research CBDCs, with many conducting pilots. A 2021 BIS survey found that "86% of central banks are actively researching the potential for CBDCs, 60% were experimenting with the technology and 14% were deploying pilot projects." The Bahamas was the first to launch a CBDC and we expect others to follow suit. We expect many CBDCs to be launched in the coming years with varying operating models.

European Banking Authority Publishes Revised Guidelines on Money Laundering and Terrorist Financing, 01 March 2021

The European Banking Authority (EBA) published final, revised guidelines outlining changes to the AML/CFT regulatory framework with regard to evolving ML/FT risks. The report aims to help financial institutions in compliance efforts and strengthen their ability to recognize and mitigate risks. The guidelines point to the importance of a business-wide risk assessment in supporting AML/CFT controls and procedures. They outline updated customer risk factors, including the customer's and customer's beneficial owner's reputation, nature and behavior, and business or professional activity.

Implementation of Strong Customer Authentication (SCA) Requirements, 01 January 2021

Per the European Banking Authority, the full implementation of SCA requirements according to PSD2 was supposed to have been accomplished by the first of the year. Enforcement and timeline concerns—alongside the complexity of B2B payments—have long plagued the requirements, and the verdict as to their feasibility and success remains uncertain. According to global payments consultancy CMS Payments Intelligence Limited, SCA requirements have caused **friction in online card payments** to the extent that CMSPI estimates the annual sales at risk of being abandoned or declined might reach EUR 102 billion.[10]

European Securities and Markets Authority Issues Guidelines on Outsourcing to Cloud Service Providers, 10 May 2021

The European Securities and Markets Authority (ESMA) issued guidelines on outsourcing to cloud service providers in an effort to help certain financial institutions understand and address the risk landscape. They lay out compliance measures, with an emphasis on a risk-based approach to assessment, pre-outsourcing analysis and due diligence. Guidance on a smooth exit strategy is also supplied. The guidelines went into effect 31 July 2021. The publication is crucial in helping firms to wade through an increasingly complex regulatory landscape and harsher non-compliance measures.

Legislation

EUROPEAN COMMISSION

European Commission Unveils Proposed Artificial Intelligence Act, 21 April 2021

As part of the European strategy for data, the European Commission published a far-reaching 108-page proposal regulating the use of AI, with particular regard to “high risk” systems and contexts. The regulation would apply to all providers and users located within the EU, as well as extra-territorial providers whose services are utilized within the EU. The Commission proposes a four-tired, risk-based approach. AI systems that pose a minimal risk—which includes the majority of such systems—will not be subject to further regulation. Limited-risk AI will be subject to transparency requirements, for example, a warning to a user that they are interacting with a chatbot. High-risk AI—defined as systems that pose a risk to users’ rights per the EU Charter of Fundamental Rights—will be subject to requirements on human oversight, transparency, quality of data sets used, technical documentation and record keeping. Should an AI system pose an unacceptable risk, it is to be banned altogether. Unacceptable risk applies to systems that implement “social scoring” and manipulate human behavior through subliminal methods. Fintech entities that operate in the EU, or outside of the EU with an effect on users within the EU, utilize AI systems that are already regulated by existing legislation. AI systems that have not yet been adopted will face increased scrutiny. The proposal must still advance through the EU legislative procedure, but it is expected to be a vanguard in global AI regulations in much the same way the GDPR has been with regard to data protection.

European Commission Submits Proposal for Digital Services Package, 15 December 2020

The European Commission submitted its proposed Digital Services Package—part of the “Shaping Europe’s Digital Future”—to the European Parliament and European Council. The proposal includes the Digital Services Act (DSA) and Digital Markets Act (DMA). Together, the legislative acts seek to promote online safety while safeguarding fundamental rights, review the liability regime of digital services acting as intermediaries, address issues derived from the gatekeeper power of digital platforms, strengthen the Single Market for digital services, bolster innovation alongside a rights-based approach, and address other emerging issues and opportunities, including online advertising and smart contracts. The EU Charter of Fundamental Rights strongly grounds the proposal, with its attention to fairness, inclusivity, transparency and accountability.

The Digital Services Act covers rules for online intermediary services—including obligations and sanctions—and seeks to strengthen the existing EU e-commerce regulatory framework. It calls for an improved approach to digital services mechanisms in removal of illegal content and the protection of user data. Indeed, this past year has seen a heightened focus on content governance and online safety, even amidst increased online privacy. On 28 April 2021, Parliament approved legislation that requires online platforms to institute a one-hour takedown of terrorist content. A day later, 29 April 2021, the Council and European Parliament agreed on a temporary measure allowing providers of electronic communications services to continue in their efforts to track and remove child abuse content until permanent legislation was announced.

The Digital Markets Act aims to cultivate a fairer business landscape by conferring a gatekeeper status upon large tech firms, and imposing obligations and non-compliance measures on them. Gatekeepers will be defined by three criteria, including stability over time, "a strong economic position" and "a strong intermediation position, meaning that it links a large user base to a large number of businesses".[11] This includes big tech firms like Google, Microsoft, Apple, Facebook and Amazon. In leveling competition and lessening unfair advantages, the EU would smooth the entryway for new and smaller firms and create a more inclusive market. This antitrust stance—support for SMEs, cultivating a level playing field, and loosening big tech's monopoly—has been central to the recent EU agenda. It will be key in diversifying the fintech landscape, spurring on innovation through competition, giving consumers more choice, and promoting its ideal of inclusive digitalization.

European Commission Publishes Proposal for Data Governance Act, 25 November 2020

The European Commission has issued its proposed Data Governance Act as part of the European Strategy for Data, "which aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU."[12] It offers an alternate method of data handling and processing than that employed by big tech, which will face increasingly stringent compliance measures. The proposal outlines rules for the access to and sharing of public sector data—both personal and non-personal (that which is unprotected by the GDPR)—that would have otherwise been protected, per commercial confidentiality and intellectual property rights, for example. A European Data Innovation Board would be established as an expert group to conduct oversight of data sharing service providers and advise the Commission. Furthermore, the act lays out the procedures for data altruism, wherein individuals or companies consent to having their data shared for the greater good. The reuse of data is especially key in advancing research. Despite concerns, the act is fully compliant with the GDPR. Similar to other acts within the EU's broad digital empowerment agenda, the proposal implements a rights-based approach premised on trustworthiness, privacy and accountability.

European Commission Publishes Fintech Action Plan, 24 September 2020

The European Commission published the FinTech Action Plan, a follow-up to the 2018 one. The plan outlines a Digital Finance Strategy Package that includes legislative proposals on crypto-assets, digital operational resilience and retail payments.

The proposed **Markets in Crypto-Assets Regulation** (MiCA) is broad and ambitious, aiming to establish a comprehensive crypto-assets regulatory framework and enhance legal certainty and harmonization across the EU. Main priorities include transparency, consumer protection, prevention of market abuse, authorization and supervision. The definition of crypto-assets is classified into three categories: e-money tokens, asset-referenced tokens, and a third group covering all other types like utility tokens and algorithmic stablecoins. Issuers will be subject to regulatory requirements based on which crypto-assets are sold, with all issuers of e-money tokens and asset-referenced tokens obligated to be authorized and established within the EU.

The Commission's **Retail Payments Strategy**, adopted by the Council of the European Union in March 2021, focuses on four tenets: innovation and competition in payments markets, facility of cross-border payments, interoperable payment systems and digital, instant payment systems across the EU. The pan-European approach seeks to boost integration amidst a fragmented payments landscape—as most payment systems only work within domestic borders—which also prevents fintech companies from successfully scaling-up across the Single Market.

The proposal on **Digital Operational Resilience for the Financial Sector** presents, for the first time, a comprehensive framework addressing digital risk in finance. The act calls for regular testing of Information and Communications Technology (ICT) systems by financial entities in order to expose vulnerabilities. It also requires a risk-monitoring system in the event that ICT services are outsourced to third-party services providers, an improved system for the reporting of ICT-related risks, and updated ICT systems that ensure both technological resilience and data processing. The risk-based approach will prove especially crucial as pandemic era cyberattacks have shown an increasing sophistication and breadth, with multiple EU and member state institutions having faced attacks. Meanwhile, the act will complement the soaring use of digital payment technologies and crypto-assets, alongside the possibility of a digital euro launch.

COUNCIL OF THE EUROPEAN UNION

Council of the European Union Agrees on Negotiating Mandate on e-Privacy Regulation, 10 February 2021

Four years after the regulation was initially proposed by the European Commission, the Council of the European Union ("the Council") has agreed on a negotiating mandate to replace the e-Privacy Directive 2002/58/EC with the e-Privacy Regulation. The draft legislation must now advance to trilogues between the European Parliament and European Commission, so its details can still change, but its main priorities outline rules for electronic communications, with regard to data protection and confidentiality of communications. It applies to both personal data and metadata, and extends to instant messaging apps, achine-to-machine communication and Voice over Internet Protocol (VoIP) platforms. Per the legislation, electronic communications data is private, and intrusion—such as listening to and monitoring—is forbidden. Before the processing of electronic communications metadata, electronic communications network and service providers must first obtain user consent. Like the GDPR, the legislation has extra-territorial scope in that it applies to any entity with EU users, regardless of location.

Belgium

Country Overview

Wealthy, innovative and fintech-friendly Belgium has become a European leader in digitalization and cybersecurity, ranking highly on several of the European Commission's Digital and Economy Society Index (DESI) 2020 indicators. DESI notes Belgium's strengths in the digitization of business and economy, use of big data and R&D expenditures in the ICT sector, although its promising trajectory has been significantly damaged by the COVID-19 pandemic.

Belgium was one of world's worst-affected countries by the pandemic, with the highest global mortality rate amidst two unrelenting waves of infection. The economy contracted by 6.2% in 2020,[13] and it is not expected to fully recover until 2022.[14] This economic downturn and long recovery period threaten to shrink its fintech landscape and deter new entrants, who might gravitate instead to comparatively unscathed Nordic innovation hubs like Stockholm and Oslo. Belgium's National Plan for Recovery and Resilience could help in safeguarding against a drastic setback, however, as the plan will allocate 31% (EUR 1.85 billion) of its funds from the EU's COVID-19 Recovery and Resilience Facility towards digital transformation.

The pandemic further exposed vulnerabilities in Belgium's cybersecurity. On 4 May 2021, a large-scale cyberattack targeted the Belgian parliament, government agencies, scientific institutions and universities. That same month, Belgium's Federal Public Service Interior revealed that it had been the victim of a two-year-long cyberattack, which first struck in April 2019. Phishing alone cost Belgians 43 million EUR in 2020,[15] and one survey found that 42% of Belgian companies were hit by a cyberattack.[16]

This growing sophistication and frequency in cybercrime has influenced Belgium's 2021 digital agenda, which focuses on strengthening its cybersecurity and AML frameworks, alongside raising awareness on data protection and ensuring

GDPR compliance. Unlike other advanced European states, Belgium has not launched exploratory research into the development of a central bank digital currency (CBDC).

FINANCIAL REGULATORY AUTHORITIES

- Central Bank: **The National Bank of Belgium** is the country's central bank.
- The **Belgian Data Protection Authority (APD)** oversees compliance with regulations on data protection such as the GDPR.
- The **Financial Services and Markets Authority (FSMA)** is Belgium's financial regulatory authority, and seeks to ensure the fair and transparent operation of the financial markets.

Policy, Laws and Regulations

National Security Council Approves Belgian Cybersecurity Strategy 2.0, 20 May 2021

The National Security Council (NCS) approved the new Belgian Cybersecurity Strategy 2.0, for 2021-2025. The strategy's overarching aim is to make Belgium one of the most cybersecure European nations, and it hinges on six main objectives:

- "Strengthen the digital environment and increase confidence in the digital environment
- Arm users and administrators of computers and networks
- Protect Vital Interest Organizations against all cyberthreats
- Respond to cyberthreats
- Improve public, private and university collaborations
- Affirm a clear international commitment"

Belgian Competition Authority Publishes Priority Policies for 2021, 09 March 2021

The Belgian Competition Authority published its strategic priorities for 2021. They include enhanced vigilance and action regarding digital platforms and continued oversight of the digital economy, with special attention to abuses and violations of the right of competition driven by algorithms and data. The focus on tech giants' dominance comes amidst an EU crackdown on big tech, with its Digital Markets Act and Proposal for Data Governance Act.

Central Bank Publishes Annual Report on Economic and Financial Developments, 11 February 2021

The Central Bank's Report 2020 — Economic and financial developments outlines major developments in 2020, with a primary focus on the impact of the COVID-19 pandemic alongside brief overviews of regulatory responses. Key areas include COVID-19's influence on the financial sectors, the rise of open banking and evolving cybersecurity challenges.

The COVID-19 pandemic brought Belgium to its worst economic performance since World War II, with an estimated loss of 41 billion EUR to its economy. Despite grim economic indicators, the National Bank of Belgium believes that central banks' responses helped to keep economic depression at bay in developed nations. Interest rates in the eurozone were already low, banks increased their purchases of financial assets (mainly sovereign bonds) and facilitated the funding of large companies and SMEs.

The main challenge in the payments sector was monitoring compliance with heightened security requirements for electronic payment card transactions in e-commerce, particularly regarding Strong Customer Authentication (SCA) requirements per the Revised Payments Service Directive (PSD2). This required the establishment of new technical protocols, which was difficult amidst a complex landscape with many players. Meanwhile, the bank sought to facilitate fintech companies' access to credit institution payment account systems.

Due to a rapidly changing risk landscape, the central bank recommends that financial institutions bolster their risk-awareness and take appropriate precautions in mitigating risks. The central bank has sought to strengthen the national cybersecurity framework over the past several years, even before the onslaught of the pandemic, and its 2015 **Circular** on expectations regarding continuity and operational security for financial institutions remains an important standard. Going forward, cybersecurity remains one of its top priorities, especially with regard to cultivating European and international cooperation.

Data Protection Authority Issues Recommendation on Cleaning Data and Destroying Data Media, 11 December 2020

The Data Protection Authority's Recommendation on data sanitisation and data medium destruction techniques seeks to help entities comply with GDPR requirements regarding accountability and prevention of the unauthorized disclosure of data. Aimed at data controllers, processors, information security advisors and data protection officers (DPOs), the recommendation outlines various techniques of sanitizing and destroying data, which make access to data impossible.

The recommendation was followed by the Data Protection Authority's 15 March 2021 release of **documents** seeking to simplify processes for data controllers, processors and DPOs. The batch of documents includes a personal data communication protocol template, a roadmap for the exchange of personal data by/with federal bodies and a model register of simplified treatment activities for the controllers and subcontractors.

Data Protection Authority Issues Management Plan 2021, 09 December 2020

The Data Protection Authority's Management Plan outlines strategic priorities for 2021, including raising awareness on data protection, promoting the effectiveness and visibility of the APD and ensuring timely and adequate processing of files. The plan delivers brief recommendations to government actors on optimizing existing techniques in ensuring GDPR compliance; undertaking monitoring of societal, economic and technological developments; coordinating cooperation; and raising awareness and increasing knowledge on data protection issues, amongst other recommendations. The APD has routinely touted the importance of awareness on data protection and has been especially keen to simplify compliance requirements.

Partial Implementation of GDPR and Exceptions Provided for in Article 23, 11 November 2020

The Ordinance of October 29, 2020 applying the exceptions provided for by Article 23 of the General Data Protection Regulation (GDPR) was published in the official gazette. Article 23 of the GDPR allows for member states to restrict, through legislative means, the scope of obligations and rights outlined in certain GDPR articles, as long as such restrictions respect "the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard" areas like national security and public security. Per the ordinance, the rights to erasure of personal data, access to personal data and rectification may be deferred or limited in certain cases.

Amending Royal Decree on Operations of the UBO Register Goes into Effect, 10 October 2020

The Royal Decree of September 23, 2020 amending the Royal Decree of July 30, 2018 regarding the operating modalities of the ultimate beneficial owner (UBO) register went into effect. The decree implements provisions of the 4AMLD and the 5AMLD and aims to facilitate access to the UBO register and ensure that its information is accurate and updated in a timely manner. Per the 5AMLD, each member state was mandated to create their own UBO register and have it operational by 10 January 2020. UBO registers were required to be interconnected via the European Central Platform by 20 March 2021, in line with the EU's goal to make AML/CFT measures increasingly harmonized across Europe.

Central Bank Publishes Financial Market Infrastructures and Payment Services Report 2020, 27 September 2020

The Financial Market Infrastructures and Payment Services Report 2020 addresses the payments sector, the central bank's supervisory role, priorities and landscape changes in 2020. The COVID-19 pandemic had a significant impact on the payments sector, with divergent effects due to the range of available means of payment. "Cash intensive payment services" plunged, while contactless payments rose in popularity. During the first month of the lockdown, e-commerce card transactions surged 20%—in both value and volume—compared to the previous timeframe in 2019. Meanwhile, in-store payments dropped 30%. The central bank predicts that the pandemic will continue to have repercussions across the sector, and some changes, like the trend towards contactless and e-commerce, will prove permanent. This will contribute in fast-tracking the digitalization of the payments sector alongside PSD2.

LEGISLATION

Bill on Various Financial Provisions Relating to Fight Against Fraud Submitted to Parliament, 07 April 2021

The Bill on various financial provisions relating to the fight against fraud was submitted to parliament. Its major change is an amendment to the AML Act, which requires that obliged entities report discrepancies between information available on the ultimate beneficial owner (UBO) register and the information available to them. This supports the recently implemented Royal Decree of September 23, 2020, which aims to ensure that the UBO register is updated with accurate information. An adequate UBO register, especially one that is interconnected across the EU through the European Central Platform, is key in helping EU and member state authorities to harmonize their approach to AML/CFT. The pandemic has highlighted increasing sophistication and transnational cybercrime and ML methodologies, which can be better identified and deterred through information sharing.

On 12 April 2021, the Federal Public Service (FPS) Finance published **user manuals** and FAQs to help individuals responsible for providing information to the UBO register in complying with regulatory requirements.

Legislative Proposal on Transparency and AI Systems, 06 April 2021

The legislative proposal seeking to amend a 1994 law on access to government information outlines requirements on the use of AI by public authorities. In a move to promote transparency and trust in AI, public authorities must publish algorithmic rules online, especially if they contribute to individual decisions. If administrative documents include individual decisions that were made on the basis of AI, citizens have the right to demand more information on the algorithmic processing and the data processed, amongst other factors. Authorities would also have to conduct and disclose impact assessments per the GDPR. The proposal dovetails with the European Commission's comprehensive regulatory framework on promoting trust in AI, released in April 2021.

Draft Law on the Modification of Data Protection Laws Introduced to Parliament, 04 March 2021

The draft law, amending both the law of December 3, 2017 and the law of December 3, 2017, aims to establish a mechanism by which the Data Protection Authority can issue advance rulings, or "privacy rulings." If passed, the DPA would be able to issue an advance ruling on how it might apply the law to specific situations regarding the processing of personal data. For an entity to be granted a privacy ruling, they would have to submit a formal request including information on the specific situation and legal or regulatory provisions forming the basis of the decision. A ruling would be issued in three months unless rejected or another timeline was agreed on. The draft law would be significant in providing legal clarity to data controllers, processors and others, and would ensure heightened compliance with the GDPR.

Denmark

Country Overview

Ranked by a 2021 study as the most cybersecure country in the world[17], Denmark has prioritized cybersecurity alongside ambitious digitalization goals. The country's Digital Growth Strategy, launched in January 2018, allocates EUR 134 million a year (approximately USD$159 million)—up until 2025—towards digital initiatives. The strategy aims to bolster Denmark's reputation as a strong digital economy and society, with initiatives seeking to attract foreign tech companies, tap into emerging technologies like AI and big data, strengthen cybersecurity and further incorporate digital technologies into citizens' and companies' routines. With its social and political stability, wealth and tech-friendly populace, Denmark is well on its way to achieving its mission and solidifying its status as a global innovation hub.

The rapid rise of fintech in Demark has further contributed to its digital transformation. Fintech has increasingly integrated into the financial sector, driving competition and innovation in the Nordic country. Government initiatives like the Fintech Forum and FT Lab, a regulatory sandbox, have been instrumental in ensuring the sector is well-supported.

Although the COVID-19 pandemic powered a 3.3% contraction in Denmark's GDP, its post-COVID recovery has been strong and swift—with a forecasted GDP expansion of 2.8% in 2021[18]. This resilient landscape will draw startups away from harder-hit European hubs, especially as the Danish recovery package includes noteworthy financial support for SMEs.

The Danish 2021 digital agenda focuses on strengthening AML measures, the digital economy and post-pandemic recovery. The NemID digital identity will be replaced by the MitID, an upgraded digital identity infrastructure that will phase out the old one by 2022. The Project 27 (P27) initiative—a collaboration between Danish, Finnish and Swedish banks which seeks to establish the globe's first real-time, cross-border and cross-currency payment system—has stalled, but could revolutionize the payments industry at its expected launch in 2022. Denmark has already abandoned the idea of a central bank digital currency following a 2016-17 study.

As MitID is being rolled out, Denmark — along with the other EU member states — is preparing for the EU's European Digital Identity wallets as part of the eIDAS reform. It remains to be seen what happens with MitID. A likely scenario is that MitID could be enhanced to conform to the EU digital wallet scheme. At the time of this report's publishing date, however, it is unclear.

FINANCIAL REGULATORY AUTHORITIES

- Central Bank: **Danmarks Nationalbank** is the central bank of Denmark. A non-eurozone member of the European System of Central Banks, it is responsible for issuing currency and ensuring monetary stability.
- Data Protection Agency: **The Danish Data Protection Agency (Datatilsynet)** oversees compliance with protection of personal data rules.
- The **Danish Financial Supervisory Authority (Finanstilsynet or DFSA)** is responsible for the regulation of financial markets in Denmark.

Policy, Laws and Regulations

Amended Executive Order on Reporting Information in Risk Assessment per Money Laundering Act Goes into Effect, 01 July 2021

The executive order on "Reporting information for use in the Danish Finanstilsynet's risk assessment of companies and persons covered by the Money Laundering Act" was amended and went into effect. The executive order was expanded to apply to virtual asset service providers (VASPS), which include digital wallet providers, cryptocurrency exchanges and banks handling cryptoassets. A February 2021 Financial Action Task Force (FATF) report on Denmark's progress in strengthening its AML/CFT framework noted that the country had resolved most of the technical deficiencies identified in a 2017 Mutual Evaluation Report. However, FATF downgraded Denmark to "partially compliant" on a recommendation pertaining to the regulation of new technologies, with regard to compliance requirements for VASPs. The agency critiqued Denmark's lack of action in identifying unregistered VASPs and in excluding from its scope exchanges between or more types of virtual asset, transfers of virtual assets and financial services related to an issuer's offer and/or sale of virtual assets. The amended executive order is a key step in ensuring full compliance with the FATF's recommendation and strengthening AML measures as cryptocurrencies surge in popularity. Both the EU and individual member states are rapidly expanding regulatory frameworks to apply to virtual currencies, as with the 5AMLD and MiCA.

Hvidbjerg Bank Completes First Payment Utilizing New Digital Identity Infrastructure, 12 May 2021

Hvidbjerg Bank and BEC Financial Technologies conducted the first payment utilizing MitID, the long-awaited digital identity infrastructure that will replace NemID. MitID, which will be more flexible and secure than its predecessor, is an app that can be used for approving logins and payments. Once MitID has been sufficiently tested, it will launch across Denmark, with a six-month transition period until NemID is completely phased out. Due to delays, the solution will most likely be ready in summer 2022.

Data Protection Agency Updates Guidelines on Consent, 09 May 2021

The Danish Data Protection Agency published its updated guidelines on consent, per the processing of personal data under the EU's General Data Protection Regulation (GDPR). The updates include the clarification that, "It is now clear that public authorities cannot, in principle, process personal data on the basis of consent." Indeed, the guidelines stress that consent is merely one of "several equal legal bases that the data controller can use to process personal data," so the giving of consent does not supersede these other means. The guidelines provide further guidance on determining legal consent.

Financial Supervisory Authority Issues Report on AML and Technology Project, 28 April 2021

The Danish Financial Supervisory Authority (DFSA) published a report on an AML and technology (AML/TEK) project, which proposes seven initiatives in support of streamlined customer due diligence procedures. The project's overarching theme is improved cooperation and communication between sectors in combating money laundering. The seven initiatives include:

1. Support for the establishment of a common shared infrastructure in undertaking KYC measures, with a focus on dialogue and decision-making in ensuring compliance with the Money Laundering Act
2. Creation of a mechanism for the validation of company data in the Central Business Register
3. Use of the MitID digital identity solution in identity verification
4. Creation of a digital solution in undertaking PEP (politically exposed person) screenings
5. Inter-sector collaboration in the identification of generalized scenarios regarding transaction monitoring
6. Greater access to government data
7. Sharing of risk flags

The proposals have been issued for a public consultation.

Proposal on Supplemental Provisions to the Regulation on ENISA, 23 February 2021

The Ministry of Trade and Industry introduced the L 174 Proposal, which adds supplemental provisions to the Regulation on ENISA (European Union Agency for Cybersecurity) on cybersecurity certification of information and communication technologies and repeals Regulation (EU) No 526/2013. Unanimously adopted, the proposal establishes a European scheme for cybersecurity in Denmark. Danish companies must obtain certification for their products, services and processes that rely on information and communication technologies. The Danish Safety Technology Authority will conduct the certification process, and has the power to revoke certifications if requirements are not met.

Danish Act on Payments Published in Official Gazette, 27 November 2020

The Danish Act on Payments, which supplements the Revised Payment Services Directive (PSD2), outlines the requirements for issuers of electronic money and providers of payment services to apply for a license with the Financial Supervisory Authority. Companies providing credit information services must also apply for a license with the DFSA through a similar, but less rigorous, process. Upon receipt of a license, companies providing credit information will be treated as payment service companies and must comply with the Payments Act. The act allows for better accommodation of an increasing variety of players in the rapidly evolving payments industry, especially as fintech companies flock to Denmark and the Nordic region.

In response to questions on the implementation of the Payments Act, the Danish Financial Supervisory Authority and the Danish Competition and Consumer Authority published guidelines on Section 63, on 11 February 2021. Section 63 outlines a requirement for banks to give payment institutions access to payment account services so that the institutions can perform transactions. The guidelines stress the importance of this access and the role of payment institutions in strengthening competition. Although Section 63 does not prevent banks from terminating payment institutions' access to payment account services, such terminations must not be conducted on an arbitrary basis.

Financial Supervisory Authority Publishes Guidance on Prevention of Money Laundering and Terrorist Financing Act, 02 November 2020

The DFSA published its revised guidelines on the Money Laundering Act. Changes include a more a stringent KYC process, reporting obligations to companies' boards of directors and modifications for obtaining and verifying identity evidence of beneficial owners. The guidelines also address the technical infrastructure of APIs, which can limit the amount of information viewable to payment initiating service providers (PISPs), such as the identity of the payer. PISPs must still monitor and assess customers' transactions for money laundering risks. Although PISPs do not pose as high a risk for money laundering in comparison with other payment service providers, they are still obligated to conduct a risk assessment of the customer relationship. Companies providing account information services (AISPs) do not fall under the purview of the Money Laundering Act.

Although Denmark has traditionally enjoyed a low rate of financial crimes, Danske Bank and Nordea nevertheless face investigations over lapses in their respective AML frameworks. With the increase of pandemic-driven financial crime and a rapid growth in sophisticated criminal methods, Denmark is especially keen on bolstering its AML/CFT measures.

In conjunction with seven other Nordic and Baltic countries, Denmark has entered into an agreement with the International Monetary Fund (IMF), which has been tasked with conducting an assessment of the region's ML/TF landscape. It is expected to deliver its results and recommendations in mid-2022.

New National Strategy for Cyber and Information Security, 16 November 2020

Denmark published the terms of reference for its new national strategy for cyber and information security, which is expected to be released in 2021. The four overarching principles include management anchoring and competence building, robustness and resilience, cooperation and organization, and international efforts and contributions. This focus on a harmonized, cross-sector approach has been increasingly adopted across the EU and individual member states.

France

Country Overview

France has the world's seventh-wealthiest economy[19] and is a leading European fintech hub, with a startup-friendly President and USD$5.2 billion raised in venture capital funding in 2020.[20] Although the COVID-19 pandemic uncovered vulnerabilities in French cybersecurity and financial stability, France remains undeterred in its ambition to become a global leader in disruptive technologies and digital transformation.

The pandemic drove the French economy into a deep recession in 2020, with a GDP contraction of 8.3%.[21] Meanwhile, a surge in cyberattacks targeted French institutions, including 27 hospitals,[22] and large-scale attacks on critical businesses soared by 400% from 2019[23]. Despite this grim landscape, the economy is projected to grow by 5.8% in 2021 and 4.0% in 2022,[24] and shifting consumer habits will fuel digitalization efforts and further develop the French fintech ecosystem.

A traditional affinity for cash lost ground amidst the pandemic as the French turned towards digital payments solutions, and the government is looking to invest more in R&D and startups. France is set to receive EUR 40.9 billion (approximately USD$48.6 billion) from the EU's Recovery and Resilience Facility and has allocated 25% of these funds towards digitalization.[25] Its France Relance plan emphasizes digital transformation and support for startups, with a grounding in technological sovereignty, simplified digital regulations and accelerated innovation.

Alongside its pandemic-recovery goals, France's 2021 digital agenda focuses on AML/CFT, multiple central bank digital currency experiments, strengthening the regulation of virtual assets and bolstering competition and compliance in the payment services industry.

TOP 3 REGULATORY CONCERNS FOR 2022

59%

Anticipated EU and individual member state artificial intelligence regulations

48%

Complying with AML requirements for virtual currencies/ cryptocurrencies

44%

Anticipated EU Digital Wallet

FINANCIAL REGULATORY AUTHORITIES

Central Bank: The Bank of France (Banque de France) is the independently run central bank of France. The Bank oversees multiple government and public accounts as well as public securities auctions of the European Central Bank. The Bank is a member of the Eurosystem of central banks. The Observatory for the Security of Payment Means is a unit operating under the Bank of France.

The French Data Protection Authority (Commission nationale de l'informatique et des libertés, CNIL) is the authority responsible for the protection of data.

The French Financial Markets Regulator (Autorité des marchés financiers, AMF) is an independent public authority regulating the French financial marketplace and its participants.

OTHER REGULATORY AUTHORITIES

The French Prudential Supervision and Resolution Authority (Autorité de contrôle prudentiel et de résolution, ACPR) is an independent arm of the Bank of France that supervises banks and insurance companies in the country. The ACPR is composed of three main committees: the Supervisory College, the Resolution College and the Sanctions Committee, in addition to several consultative bodies.

The Ministry of the Economy and Finance (Agence française de développement, AFD), informally known as Bercy, performs multiple functions related to the growth and stability of the country's economy. Primarily, the Ministry drafts taxation laws, oversees national funds, and develops regulations supervising the public and private sectors.

The French Competition Authority (Autorité de la concurrence) is the national competition regulator of France and an independent administrative authority. The agency's main purpose is to counteract anti-competitive practices in private markets. The National Commission on Informatics and Liberty (CNIL) is the national data protection authority in France.

The National Information Systems Security Agency (Agence nationale de la sécurité des systèmes d'information, ANSSI) is the national computer security agency of France operating under the Secretariat-General for national Defense and Security (SGDSN). Both agencies help the Prime Minister carry out defense and national security responsibilities.

PREVENTING CYBERATTACKS AND FRAUD COMPLIANCE IS TOP CHALLENGE

70%

Reducing or preventing cyberattacks and fraud

52%

Safeguarding sensitive data

41%

Keeping pace with changes in consumer privacy laws, industry regulations

The French Anticorruption Agency (Agence française anticorruption, AFA) is the national agency responsible for detecting and preventing corruption.

The Intelligence Processing and Action against Illicit Financial Networks Unit (TRACFIN), housed in the Ministry of the Economy and Finance, combats money laundering and the financing of terrorism.

Policy, Laws and Regulations

France-Singapore Partnership on Cross-Border CBDC Trial, 08 July 2021

The central banks of France and Singapore announced that they had successfully undertaken a CBDC-based cross-border payment experiment using JP Morgan's Onyx blockchain unit. The experiment simulated transactions with digital euro and Singapore dollar CBDCs on a common network and employed automated market-making and liquidity management capacities[26]. As Valérie Fasquelle, Director of Infrastructures, Innovation and Payments at Banque de France explained, "By experimenting the circulation of EUR CBDC in a shared corridor network, the MAS and the Banque de France tested the possibility to provide a link with other CBDCs all over the world. It is an opportunity to construct arrangements for multiple CBDCs models, improving cross-border payments and increasing harmonisation of post-trade procedures."[27] Cross-border payments are currently slow and expensive, and they rely on intermediary correspondent banks, which presents friction such as KYC requirements.

Also on 08 July 2021, Banque de France issued a **press release** outlining a successful experiment conducted in partnership with the Tunisian central bank, Banque Centrale de Tunisie. The investigation successfully completed wire transfers between French and Tunisian commercial banks utilizing a blockchain-based wholesale CBDC.[28]

On 06 June 2021, Banque de France, the Swiss National Bank and the Bank for International Settlements (BIS) Innovation Hub **announced** that they planned on conducting an investigation—called Project Jura—into cross-border settlements using wholesale CBDCs. The banks have partnered with Accenture, Credit Suisse, Natixis, R3, SIX Digital Exchange and UBS in executing the project. The experiment will involve a euro CBDC, a Swiss franc CBDC and a French digital financial instrument on a distributed ledger technology (DLT) platform.

TOP COMPLIANCE TECHNOLOGIES FOR FRENCH BANKS

56%

Trustworthy artificial intelligence

(i.e., technologies that aim to make artificial intelligence explainable, fair and robust)

48%

Digital remote identity verification

(i.e., technologies allowing the verification of identity of natural or legal persons online)

44%

Mediated digital agreement technology

(i.e., electronic signatures with video conferencing/collaboration and remote online notarization)

CBDC Experiment on the Settlement of Listed Securities, 18 June 2021

The central bank—in partnership with SEBA Bank, Banque Internationale à Luxembourg and Luxembourg central securities depository LuxCSD—successfully conducted an experiment on CBDC and the settlement of listed securities. The experiment involved the simulated issuance of CBDC on a public blockchain, employing a smart contract to trigger the delivery of the securities. The trial comes on the heels of a third successful experiment on CBDC and interbank settlements.

On 28 April 2021, a collaboration between the Bank of France, European Investment Bank (EIB) and Société Générale – FORGE successfully conducted its third experiment testing a blockchain-based interbank settlement. The experiment centered on investor subscription to EUR 100 million in EIB-issued digital bonds, with cash settlements represented by a blockchain-issued CBDC. A Bank of France **press release** states, "From a technological standpoint, the experiment required the development and deployment of smart contracts under secured conditions, so that the Banque de France could issue and control the circulation of CBDC tokens and so that CBDC transfer occurred simultaneously with the delivery of securities tokens to the investors' portfolio, in a Delivery versus Payment."

France has been a major proponent of the adoption of a digital euro, especially as tech giants' payments solutions threaten monetary sovereignty. French Finance Minister Bruno Le Maire adamantly opposed the advent of Facebook's Libra digital currency, now known as Diem, pointing to its "systemic risk" and "danger to consumers."[29] The central bank plans on continuing its experimentation on the uses of central bank digital currency in interbank settlements.

Data Protection Authority Publishes Annual Report 2020, 18 May 2021

The Data Protection Authority (CNIL) published its annual report for 2020, which provides an overview of regulatory changes and its supervisory activities. Major themes include enhanced cooperation with other European authorities, data protection and the future of payments. Cash use has declined with the advent of digital payments solutions, and the CNIL believes this trend will accelerate as new technologies emerge. This rapidly evolving landscape has required the authority to consider implications for data protection and increased means of committing fraud. The

CNIL plans on releasing a white paper in 2021 that will open a public consultation on compliance rules and guidelines for various actors in the payments sector. Its ultimate goal is to ensure GDPR compliance and increased user awareness of risk.

On 02 March 2021, the CNIL published an **announcement** on its main priorities for 2021, which include cybersecurity of websites, security of customer health data and the use of cookies. Data protection and cookies have become an increasingly important discussion in France and the EU as the COVID-19 pandemic alters the digital landscape.

Decree on Strengthening the AML/CFT Framework Regarding the Anonymity of Virtual Assets, 02 April 2021

The French Ministry of the Economy and Finance's Decree No. 2021-387 of April 2, 2021 relating to the fight against anonymity of virtual assets and strengthening the national system for the fight against money laundering and the financing of terrorism was issued. The decree builds upon and applies Ordinance No. 2020-1342 of 4 November, 2020 strengthening the mechanism for freezing assets and prohibiting their provision. In bolstering the AML/CFT framework, the decree aims to tamp down on the use of anonymous digital assets in illegal activity by expanding the scope of customer due diligence requirements. The decree modifies KYC measures for payment and e-money institutions and requires digital assets services providers (DASPs) to identify customers in advance of a transaction. E-money issuers are required to conduct customer due diligence when e-money is utilized in the purchase of digital assets, and thus anonymous e-money is prohibited in such sales.

France's regulatory action was likely spearheaded by the Financial Action Task Force, of which France is a member. In March, the FATF released a public consultation on a risk-based approach to virtual assets and virtual asset service providers. Loopholes in identity verification of customers are being plugged to thwart illicit activity. This is, in fact, a global trend and not isolated to France.

Government Publishes Action Plan on AML/CFT, 22 March 2021

The Plan to Fight Money Laundering and Terrorism Financing 2021-22 is centered on five main priorities: mobilize all stakeholders in preventing risks; guarantee financial transparency; prioritize detection, prosecution and sanctioning; hinder terrorists' access to the financial system; and reinforce coordination of national policy. A major theme is heightened supervision, coming amidst a spate of AML/CFT regulations cracking down on the anonymity of virtual assets. Indeed, a high-profile terrorist financing network in France, dismantled in September 2019, utilized cryptocurrency, and French Finance Minister Bruno Le Maire has repeatedly warned that the advent of decentralized finance will facilitate ML/TF. The action plan comes on the heels of a 18 January 2021 Financial Markets Regulator **announcement** that it had updated the Book III of its General Regulation and the four guidelines constituting its AML/CFT policy. The guidelines cover the risk-based approach to AML/CFT, due diligence obligations, relations with politically exposed persons and the obligation to report to TRACFIN.

The past year has seen an especially aggressive and innovative French approach to AML. On 22 January 2021, the French Anticorruption Agency published a **communication** on DATACROS, a prototype tool aimed at uncovering money laundering and other illicit activities. A collaboration between the Anticorruption Agency and other European entities, the tool detects anomalies in the ownership links between companies in the identification of risk indicators. Indicators include patterns of collusion, relations with politically exposed persons and abnormally complex relations with jurisdictions that do not adhere to the same standard of transparency.

France Begins Issuing Digital ID Cards, 16 March 2021

The French government launched its new national digital identity card, which include an electronic code, QR code and fingerprint. The QR code is an electronic seal that operates as a digital signature and authenticity stamp. The digital identities will be crucial in combatting identity theft and fraud, which soared amidst the COVID-19 pandemic, although concerns over data protection persist.

FRENCH BANKS ANTICIPATE CENTRAL BANK DIGITAL CURRENCY; IMPLEMENTATION OF MOBILE APP SHIELDING LIKELY

59%

Securing our mobile app

(e.g., application shielding)

44%

Investing in technology stacks that can support digital currency

41%

Drafting deposit and transfer rules for digital currency

Government Unveils National Cybersecurity Strategy, 18 February 2021

This ambitious national cybersecurity strategy outlines key objectives, including bolstering support for French R&D in cybersecurity and innovation; doubling the number of cybersecurity professionals in France by 2025; promoting a cybersecurity culture amongst businesses, especially small ones; tripling the annual sales of cybersecurity companies to EUR 25 billion in 2025; and supporting the emergence of three French cybersecurity unicorns by 2025. A new cybersecurity center will also be established in Paris, and will host 1500 researchers and representatives from public and private sectors.

The strategy comes on the heels of a challenging 2020 cybersecurity landscape for France, which saw a 225% increase in ransomware attacks compared to 2019[30] and a surge in large-scale incidents targeting critical businesses and hospitals. France's approach has been twofold in both bolstering national cybersecurity measures and in seizing the chance to grow its reputation as an innovation hotspot. French President Emmanuel Macron has routinely promoted a startup culture and high-tech dovetailed with economic growth, launching multiple billion-euro investment plans for startup funding throughout his presidency.

Financial Markets Regulator Publishes Action and Supervision Priorities for 2021, 11 January 2021

The French Financial Markets Regulator (AMF) published its action and supervision priorities for 2021, which include mobilization in recovery from the pandemic and economic recession, a rapid transition to sustainable finance, participation in financial regulation reforms and the strengthening of its monitoring and supervision approaches. Per France's startup-friendly landscape, the AMF details its commitment to support businesses, especially SMEs, by facilitating their access to capital markets and bolstering the mobilization of private funding. In ensuring the continued competitiveness of Europe's financial markets, the AMF points to the need for a more harmonized and transparent approach to EU regulation. Addressing regulatory fragmentation would make the EU more swift in responding to rapid changes in financial markets and strengthen the single market as a whole. EU and member state authorities have increasingly pointed to the benefits of cooperation and greater integration, especially in light of the COVID-19 pandemic and resultant challenges. The AMF especially welcomes EU legislation on the regulation of cryptoassets, particularly regarding strengthening the EU-wide approach to AML/CFT.

Legislation

Bill Ratifying Ordinance on Strengthening the AML/CFT Framework Applicable to Digital Assets, 21 April 2021

The French Ministry of the Economy and Finance submitted a draft law ratifying **Ordinance No. 2020-1544** of December 9, 2020 strengthening the framework for the fight against money laundering and the financing of terrorism applicable to digital assets. The ordinance broadens the scope of AML/CFT framework requirements to include services for the exchange of digital assets and digital asset trading platforms. Crypto-to-crypto exchange services and digital asset trading platforms must register with the Financial Markets Authority, and digital assets services providers (DASPs) are prohibited from maintaining anonymous accounts.

France has traditionally taken a hard line against virtual assets, especially cryptocurrencies like bitcoin that safeguard users' anonymity. In a **press release** accompanying the 09 December 2020 ordinance, Finance Minister Bruno Le Maire confirms that regulatory provisions will be introduced allowing for the speedy launch of digital identification solutions for digital asset transactions.

Bill on Contactless Mobile Payments Submitted to Parliament, 16 November 2020

Bill No. 3574 aiming to regulate contactless mobile payments was submitted to parliament. The draft law seeks to restore consumers' freedom of choice in contactless mobile payments, especially as the COVID-19 pandemic spurred on the rapid adoption of digital payments solutions. Meanwhile, the draft law speaks to the importance of increased regulation in cultivating more robust competition, as tech giants utilize their dominant stance to gain unfair advantages and deter smaller players. If passed, the bill would require "operating system suppliers to guarantee fair conditions of competition between its own payment service activity and the competing activities carried out directly or indirectly by credit institutions, electronic money institutions, payment service providers, institutions agents and agents within the meaning of Directive (EU) 2015/2366 [on payment services in the internal market]." Operating system suppliers would also have to ensure that their products and services do not prevent consumers from enjoying freedom of choice in selecting a contactless mobile payment service provider.

On 01 December 2020, the Bank of France published a press release by the National Cashless Payments Committee affirming its commitment to the European strategy on payments, welcoming support in the promotion of cashless payments and lauding the French payments sector in its response to the COVID-19 pandemic.

Germany

Country Overview

With the fourth-largest economy in the world and a robust regulatory landscape regarding data protection, AML and crypto, Germany is well-positioned for innovation in the fintech sector. Still, the COVID-19 pandemic highlighted a nationwide hesitancy towards digitalization—fax machines and handwritten checklists still utilized by government officials, low broadband access in schools and rural areas and the absence of an electronic patient database.[31] On the other hand, German authorities have reacted to these weaknesses by revamping the country's commitment to digital transformation, and it neither lacks in funds nor ideas.

Although its economy contracted by 5% in 2020[32] amidst the COVID-19 pandemic, the economic powerhouse remains undeterred in its modernization goals. Germany plans to spend 90% of its 28 billion-euro COVID-19 recovery package on climate change and digitalization,[33] far surpassing the EU's target goal of 20% towards digital transformation.[34] Key areas of focus include digitalization in the economy—as well as education, infrastructure and public health sectors—alongside a sovereign and scalable European cloud infrastructure and reducing barriers to investment.

Important steps have already been taken. One of Germany's longstanding digitalization goals has been the development of a convenient and efficient digital identity, which would simplify traditionally cumbersome bureaucratic processes. On 20 May 2021, the Bundestag passed a law allowing German citizens to access government services online using their mobile phones and existing identity cards. This could pave the way for increased use of digital identity in banking, which would dovetail with financial inclusion goals. Meanwhile, regulators have cracked down on big tech and cleared up legal uncertainties regarding crypto, which will attract more diverse players and financial investment to Germany's fintech ecosystem. Berlin, already a major site for fintech startups, is poised for immense growth.

Germany's digital transformation will not come without hurdles—like the rocky implementation of the PSD2's Strong Customer Authentication requirements—but its prospects remain rosy. Recent regulatory updates in blockchain, crypto and AI will spur on further innovation, while the strengthening of consumer protection and convenience will reinforce support for and trust in digitalization.

FINANCIAL REGULATORY AUTHORITIES

Central Bank: The Deutsche Bundesbank (BBk) is the independent central bank of Germany. The Deutsche Bundesbank is considered the most influential member of the European System of Central Banks and has helped shape the Euro system.

The Federal Financial Supervisory Authority (BaFin) is Germany's main financial regulatory authority working independently under the Federal Ministry of Finance. It supervises the banking, insurance, securities, and other financial services industries.

OTHER REGULATORY AUTHORITIES

Data Protection Authority: The Federal Commissioner for Data Protection and the Freedom of Information (BfDI) is the national data protection authority in Germany for telecommunications providers. However, in addition to the BfDI, there are multiple data protection authorities for all 16 states, each responsible for enforcing EU data protection laws and regulations.

The Federation of German Consumer Organizations (VZBV) is an independent consumer rights organization representing 42 consumer associations in Germany. The organization is non-governmental and works with legislators and the private sector to protect consumers.

The Federal Network Agency (Bundesnetzagentur) is the regulatory office for the telecommunications sector, as well as electricity, gas, post and railway markets.

The Federal Office for Information Security (BSI) is a federal agency providing IT security services to the German government, manufacturers and private and commercial users.

STANDARDS, LAWS AND REGULATIONS

Parliament Adopts Law on Data Protection and Privacy in Telecommunications and Telemedia, 20 May 2021

The Bundestag adopted the Telecommunications and Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutzgesetz, TTDSG), which seeks to unify previously contradictory national laws on data protection and further adhere to the EU's GDPR and ePrivacy directive. Almost ten years after the deadline, the new law transposes the ePrivacy requirement that users must consent to cookie settings, unless cookies and similar technology are "necessary to provide the service(s) requested by the end user" (Section 22).[35] Democrat MP Hansjörg Durz stated that the law established the "basis of the data economy of the future,"[36] although opposition members fear the law is not substantive enough.

Bundestag Passes Law on the Introduction of Electronic Securities, 06 May 2021

Parliament passed the Electronic Securities Act (elektronisches Wertpapiergesetz, RegE-eWpG), which enables blockchain-driven securities trading. The new law enables the dematerialization of securities, establishes the necessary legal certainty and application safety, adds detail to the previously-introduced crypto custody license and provides clarity on the emerging digital asset ecosystem. It also establishes mandatory licensing requirements for the administration of electronic registers and safekeeping of cryptographic keys. BaFin will supervise the administrators of crypto security registers. The law marks key progress in the country's blockchain technology strategy and overall digital transformation, and is expected to encourage further innovation in finance.

New Law Allows Institutional Investment Funds to Invest in Crypto, 22 April 2021

The Bundestag approved legislation allowing managers of wealth and institution investment funds (Spezialfonds) to invest up to 20% of their portfolios in cryptocurrencies. Under current regulations, Spezialfonds—which hold around EUR 1.2 trillion in investments [37]—have zero funds invested in crypto. The move could prove significant in bolstering Germany's status as an international financial investment hotspot and legitimizing the cryptocurrency sector. About 4000 funds would be eligible under the law, which is scheduled to come into effect 01 July 2021.

Germany Approves Use of AI in Identity Verification, 01 April 2021

The Federal Network Agency (Bundesnetzagentur, or BNetzA) and the Federal Office for Information Security (BSI) have approved the use of AI-driven identification verification methods, including biometric and document recognition systems. The decision, outlined in the "Identification of a natural person when applying for a qualified certificate using video transmission (video identification) with an automated process," is premised on the German Trust Services Act, which implements the EU's eIDAS Regulation. Germany is known for its affinity for cash, paper and pen, but its digitalization efforts show a commitment towards making everyday technologies accessible and convenient for users who might otherwise be wary.

The announcement by the BNetzA and BSI comes about one year after the Financial Action Task Force published its Digital Identity Guidance. The FATF recommends a risk-based approach to identity verification and notes the use of AI and machine learning for determining validity of government-issued ID. Germany is the latest in a long line of jurisdictions approving the use of AI for identity verification.

Digitalization Act Enters into Force, 19 January 2021

The Digitalization Act, which comprises the 10th Amendment of the German Competition Act (ACR), expands Germany's regulatory scope with regard to competition in the digital sector. The act targets digital platforms in an aim to bolster competition and tamp down on unfair practices. To this end, the German Federal Cartel Office (Bundeskartellamt), watchdog and antitrust authority, now has the power to prohibit companies from creating barriers to entry, initiating preferential treatment of its own services and putting constraints on interoperability of data, products and services. This comes amidst an EU-wide spate of antitrust regulations in an effort to reign in big tech. The German Federal Cartel Office has been embroiled in numerous cases against industry giants Amazon and Apple for suspected anti-competition practices, which have contributed to the crackdown.

Bundestag Adopts Draft Bill on Implementation of 6AMLD, 14 October 2020

The Draft Act for the Effective Prosecution of Money Laundering (Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche) transposes the EU's 6AMLD (Sixth Anti-Money Laundering Directive) onto national law and seeks to make AML measures more all-encompassing. The act does not impose significant regulatory changes on obliged entities, although processes and procedures will change. Obliged entities must still carry out transaction monitoring and reporting, but they do not have to determine a particular offense as this is the role of the prosecutor. Indeed, prosecutors' investigative powers are greatly enhanced, which is expected to make AML measures simplified and more effective.

BaFin Issues Announcement on Licensing for Crypto ATMs, 08 September 2020

Under the German Banking Act, new provisions mandate that the installation of crypto ATMs must acquire prior BaFin approval. ATMs operating without approval will be considered illegal and subject to prosecution. Germany has established itself as a vanguard in crypto regulation, both facilitating the use of crypto while enabling increased BaFin oversight. Germany was one of the first countries in the world to allow financial institutions to custody cryptoassets, classified as a financial service. As of 01 January 2020, all entities seeking to custody cryptoassets must apply for BaFin authorization. Per the implementation of the 4AMLD into German law, all entities engaging in the trade of crypto must also be licensed by BaFin. Many of these entities must apply for a banking business license in addition. The German Banking Act considers all crypto custodians and exchanges as financial institutions, so they must adhere to AML/CFT regulations.

Legislation and Policy

Parliament Submits Draft Law to Strengthen Data Protection Supervision, 18 May 2021

The Bundesrag, the lower house of parliament, submitted a draft law on strengthening data protection supervision (DSaufsichtsG), which would amend the Federal Data Protection Act (BDSG) and ensure compliance with EU law. The draft law seeks to bolster the powers of the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI), especially in the case of data protection violations that fall outside GDPR purview.

Parliament Adopts the IT Security Act 2.0, 07 May 2021

The upper house of parliament, the Bundesrat, endorsed the IT Security Act 2.0 (IT-Sicherheitsgesetz 2.0, IT-SiG 2.0), which had been adopted by the Bundesrag on 23 April 2021. The Act seeks in part to strengthen consumer protection, and expands the powers of the Federal Office for Information Security (BSI) towards this end. Upon passage into law, the BSI would be responsible for establishing binding minimum standards for IT security, and have heightened authority in receiving information on IT vulnerabilities and advising IT manufacturers. A special category of companies—and firms from the supply chains of such companies—would be established in order to deliver enhanced protection. Protected entities include defense industry companies and others that are consequential in upholding the German economy. This would require increased compliance measures on the part of those companies in meeting and recording stringent IT security requirements. The law also simplifies data protection requirements for the BSI with regard to federal communication technology and the processing of log data.

BaFin Publishes Paper on Supervisory Priorities for 2021, 03 May 2021

BaFin published its Supervisory Priorities for 2021, which include addressing compliance with PSD2's Strong Customer Authentication (SCA) requirements, IT and cyber risks, cryptoassets, the pandemic's impact on financial markets, consumer protection and AML/CTF. SCA compliance has been an especially weighty issue as member states across the EU have struggled in its implementation, with many states continuously delaying rollout of requirements. Germany fully implemented SCA requirements on 15 March 2021, and friction in payments services has caused problems for both users and merchants. The 3-D Secure authentication stage has an abandonment rate of 17-20% in Germany, often due to customers inputting an incorrect verification code or not completing a step in time, which leads to issuer decline. This has caused customer frustration and revenue loss for businesses,[38] proving merchants' pre-implementation concerns valid. President of the European Commission and German citizen Ursula von der Leyen has made cashless payments a top EU priority, but SCA difficulties might discourage Germans, who have been slower to adapt than many of their European counterparts. Indeed, the state has a reputation for digital shyness and cash use is still relatively high, though it has taken a dip in recent years.[39]

Central Bank Tests Blockchain in a Settlement Interface for Electronic Securities, 24 March 2021

Six years in the making, the Deutsche Bundesbank, Deutsche Börse and Germany's Finance Agency have successfully tested a blockchain-based settlement interface for electronic securities. The development shows that blockchain technology and traditional payment systems can be linked to settle securities without the need for a central bank digital currency (CBDC). Burkhard Balz of Bundesbank stated, "Following successful testing, the Eurosystem should be able to implement such a solution in a relatively short space of time—at least in far less time than it would take to issue central bank digital currency, for instance."[40]

BaFin Issues Warning on Cryptocurrency, 19 March 2021

The German regulator issued a warning to small investors that, despite soaring prices in virtual currencies like Bitcoin, cryptocurrency poses inherently high risks. The warning comes on the heels of a European Supervisory Authorities (ESA) caution on risks in crypto. Still, Germany is keen on cultivating the regulated use of cryptocurrency by large entities as it seeks to make the country more attractive to financial investment.

Germany Adopts Draft of the Act to Amend the Anti-Money Laundering Act, 10 February 2021

The German government adopted the draft of the Act to Amend the Anti-Money Laundering Act (Anti-Money Laundering Transparency Register and Financial Information Act, "Draft TraFinG Gw") in order to align with an EU draft act seeking to interconnect member states' beneficial owner registers per AML purposes. Should the draft become law, German companies will have to report their beneficial owners to the Transparency Register, which is currently not mandatory if information on the beneficial owner is readily viewable from other public registers. This marks an important step in harmonizing and coordinating the EU member states' approach to AML, especially as criminals' methods become more sophisticated and transnational. The move might also cause friction in light of increasing compliance measures to be undertaken by financial institutions.

Greece

Country Overview

Greece has seen a surge in cyberattacks amidst the COVID-19 pandemic and resultant economic recession, coming on the heels of an already-vulnerable digital landscape. In January 2020, Greece's four main banks had to cancel 15,000 debit and credit cards after a tourist services portal was hacked. Since then, an increase in remote work has made information systems even more open to attack, and Greece's strategic location has made it attractive to hackers looking to weaken the state. As vulnerabilities have been exposed, Greece has been slow to enact regulations in response.

Still, Greece has looked towards digitalization in strengthening and modernizing its floundering and cash-heavy economy. Indeed, Greece ranks second-to-last on the EU's Digital Economy and Society Index ranking for 2020, with only 40% of its internet users utilizing online banking.[41] Alongside an affinity for cash use, a 2017 Forbes study revealed that Greece has the number one shadow economy in the world.[42] Digital banking technology can help to cut down on illegal activities and rampant tax evasion, which has partly contributed to the country's dire financial straits.

Greeks' distrust of the central bank might prove an obstacle to the widespread adoption of online banking services. Between tax hikes, wariness of the Greek government and pandemic-driven uncertainty, many Greeks have turned towards cryptocurrency as an alternative to centralized finance. Bitcoin reported a 163.37% surge in Greek interest in 2020.[43] Although the Bank of Greece issued an announcement in 2018 per a European Securities and Markets Authority (ESMA) warning regarding the risks of virtual currencies, it has done little to regulate them.

Despite friction between the government and people, Greece's COVID-19 recovery plan could offer the state an opportunity to start anew, in a way more palatable to a traditionally cash-reliant populace. The EU has allocated EUR 30.5 billion in grants and loans towards Greece's Covid recovery.[44] The European Investment Bank (EIB) has partnered with the Greek Ministry of Finance to help manage 5 billion of the money with a focus on high-impact investment plans, including digital transformation.[45] Small financial institutions like Viva Wallet have already achieved successes in digital innovation, and tech giant Microsoft announced in October 2020 the "GR for Growth" initiative, which seeks to spearhead technological advancements in Greece. Both could prove useful in attracting more foreign direct investment towards Greece's digitalization efforts.

FINANCIAL REGULATORY AUTHORITIES

The **Bank of Greece** is the central bank of Greece.

The **Hellenic Data Protection Authority** (HDPA) is the primary data protection authority in Greece. It supervises the implementation of the application of the GDPR, national laws 4624/2019 and 3471/2006, and other relevant regulations.

The **Hellenic Capital Market Commission** aims to ensure the protection and operation of the capital market in Greece.

POLICY, LAWS AND REGULATIONS

Decision Establishing the eGov-KYC, 07 April 2021

Decision No. 9747 of 2021 has established the eGov-KYC, an online Know Your Customer application. It outlines the requirements for the identity verification of natural persons and procedures for obtaining and transferring their data to obligated financial and credit institutions. The decision marks an important step in the digitalization of banking and in mitigating ML/TF risks. Its convenience will help to enfranchise previously unbanked individuals.

Greece Launches Digital Transformation Strategy, December 2020

Minister of State and Digital Governance Kyriakos Pierrakakis has launched Greece's Digital Transformation Strategy—colloquially referred to as the Digital Transformation Bible—which outlines 450 projects to encourage digitalization across both public and private sectors. The strategy is underpinned by seven major goals, one of which is to incorporate digital technologies in all economic sectors. If successfully implemented, the framework could prove pivotal in attracting more foreign direct investment to Greece, which has lagged behind other EU member states.[46]

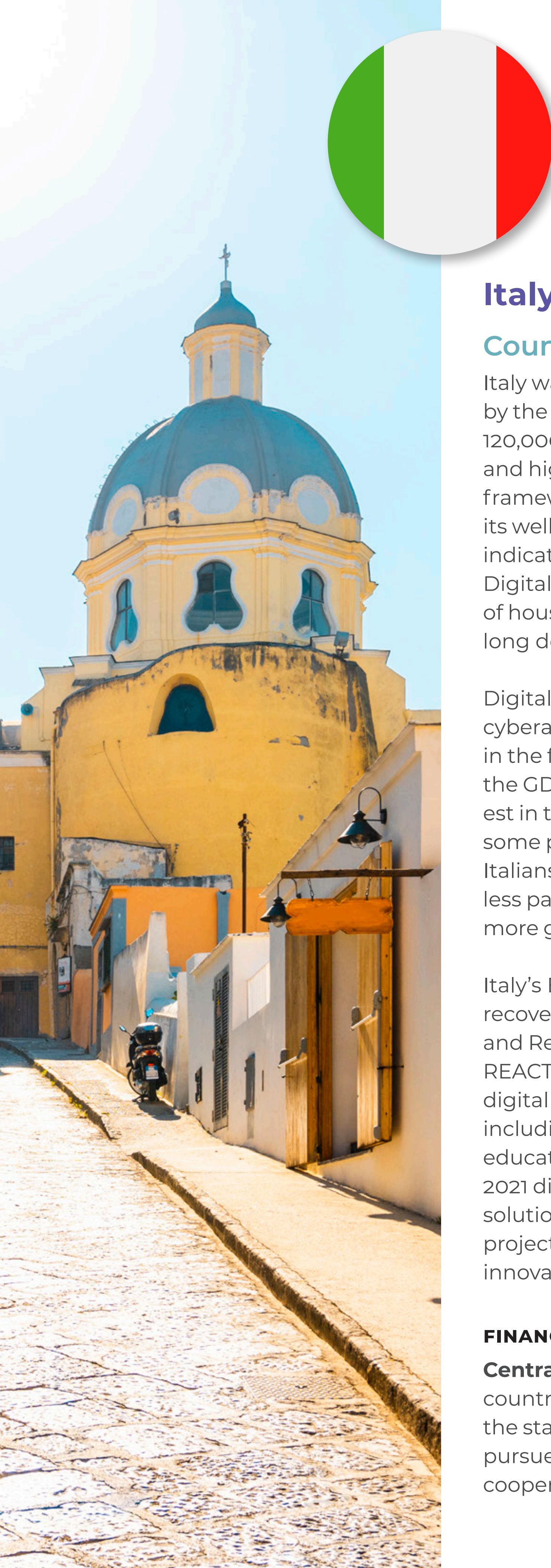
April's Decision No. 9747 to establish the eGov-KYC is part of Greece's wider Digital Transformation Strategy. In order to advance digital transformation, it is imperative to enable citizens to have their identities verified online. That, coupled with strong authentication and electronic signatures, is foundational for digital transformation.

Greece Publishes its National Cyber Security Strategy 2020-2025, 07 December 2020

Greece's updated National Cyber Security Strategy was driven by the dramatically shifting threat landscape in response to the COVID-19 pandemic. The strategy, signed off on by Minister of State and Digital Governance Kyriakos Pierrakakis, outlines 20 objectives, including balancing security with privacy, establishing and implementing policies and regulation capabilities, establishing incident reporting mechanisms, providing incentives for the private sector to invest in security measures, and a risk assessment approach. A risk-based approach will be especially crucial in a post-pandemic ecosystem, which will see more widespread adoption of remote services and the ever-present threat of cybercrime.

Establishment of Register of Exchange Services Between Providers, 05 December 2020

The Hellenic Capital Market Commission published Decision 5/898/2020 requiring registration for entities that seek to provide virtual currency exchange and digital wallet custody services. This signals an important move towards reining in Greece's tendency to shadow economic activities, which can be facilitated by untraceable cryptocurrency transactions. Cryptocurrency has previously faced little regulation in Greece, although this will change with the likely passage of the EU's MiCA and Greece's continued efforts to crack down on tax evasion and money laundering.



Italy

Country Overview

Italy was one of the world's worst-affected countries by the COVID-19 pandemic, which tragically led to over 120,000 deaths,[47] plunged the economy into recession and highlighted fragilities in the country's cybersecurity framework and digital readiness. Indeed, Italy lags far behind its well-developed European peers in digital transformation indicators, ranking 25th in the European Commission's Digital Society and Economy Index (DESI) 2020. A third of households do not have a computer,[48] cash use has long dominated, and ICT graduates are few.[49]

Digital unpreparedness made Italy susceptible to a surge in cyberattacks amidst the pandemic, with a 47% rise in attacks in the first quarter of 2021 compared with 2020.[50] Meanwhile, the GDP contracted by 8.9%[51] and public debt—the third highest in the world[52]—ballooned. The ensuing shift online has had some positive effects on Italy, however, as it has accelerated Italians' adoption of innovative technologies—especially cashless payment solutions and e-commerce—and spurred on more governmental efforts to digitalize.

Italy's EUR 235 billion (approximately USD$279 billion) recovery plan, which draws mostly from the EU's Recovery and Resilience Facility, with additional funds from the REACT-EU Initiative and public finance,[53] will help in its digital transformation goals. The plan hinges on six pillars, including digitalization, innovation, competitiveness, culture, education, and research.[54] Alongside its recovery plan, Italy's 2021 digital agenda focuses on promoting cashless payment solutions, continuing its experiments in blockchain-based projects, and supporting the emergence of fintech and innovative technologies.

FINANCIAL REGULATORY AUTHORITIES

Central bank: The **Bank of Italy (La Banca d'Italia)** is the country's central bank. The bank's main function is to ensure the stability and efficiency of Italy's financial system. The bank pursues its goals through secondary legislation, controls, and cooperation with government authorities.

Data protection authority: The **Garante per la Protezione Dei Dati Personali, or the Garante,** is the national data protection authority in Italy. The Garante is composed of an elected Council and an Office of 162 members.

Commissione Nazionale per le Società e la Borsa (CONSOB) is the government authority responsible for regulating the Italian securities market, including the stock exchange, Borsa Italiana.

The **Digital Italy Agency (AgID)** is a governmental agency that manages the implementation of the Italian Digital Agenda's objectives in line with the EU Digital Agenda. The agency defines regulations, standards, and guidelines to effectively provide online services to citizens.

OTHER REGULATORY AUTHORITIES

The Italian Competition Authority (AGCM) is an independent non-governmental organization in charge of enforcing consumer protection laws and anti-trust regulations.

The Financial Intelligence Unit (FIU) is an independent organization established under Legislative Decree 231 of 2007 that analyses financial information with the goal of preventing money laundering and combatting terrorist financing. The Bank of Italy issues the regulations and rules governing the FIU.

POLICY, LAWS AND REGULATIONS

Guarantee Blockchain Project Completes Pilot Phase, 10 May 2021

Fideiussioni Digitali, a blockchain project for issuing guarantees or surety bonds, successfully completed its 4-month pilot phase. The project seeks to crack down on fraud in the surety sector, and the pilot phase found a 30% reduction in fraud alongside a cost savings of 10% to 50%,[55] increased transparency and speed. A collaboration between CeTIF (Research Centre on Technology) and tech companies SIA and Reply, the project will undergo regulatory and technical improvements before an expected launch in the second half of the year. The Bank of Italy, Italian Finance Police, and insurance authority IVASS were also involved.

Italy recently saw another key development in its blockchain initiatives. The Spunta project, a DLT-based interbank reconciliation spearheaded by the Italian Banking Association (ABI) and its lab (the ABI Lab), went fully operational on 13 October 2021. About 100 banks are interconnected through nodes in a blockchain-based, automatic reconciliation of bilateral accounts, a process previously conducted through telephone calls and messages. The process uncovers mismatched transactions through a shared algorithm, which allows for a standardized approach across participant banks. This streamlined, automatic process enables daily reconciliations, rather than monthly ones, and strengthens transparency while reducing operational risks. The Italian Banking Association predicts that Spunta will have processed over 350 million transactions by the end of 2021.[56]

Bank of Italy and CONSOB Issue Warning on Investing in Cryptoassets, 28 April 2021

The Bank of Italy and CONSOB issued a warning, directed especially at “small savers,” regarding the high risks in dealing with cryptoassets. Due to the lack of a comprehensive regulatory framework, cryptocurrencies like bitcoin pose inherent risks like volatility, a lack of legal protections, a lack of information requirements for operators, protections for the invested money and more. Increased digitalization and the “spread of offers” has facilitated the purchase of cryptoassets. The communication reiterates its warning and notes that, although the European Commission has proposed its Markets in Crypto Assets (MiCA) regulation, cryptoassets are still insecure and lack substantive oversight.

In a January 2021 interview, Colonel Tommaso Solazzo of Italy’s Guardia di Finanza, a law enforcement agency responsible for financial crime, pointed to criminal exploitation of the anonymity offered by cryptocurrencies.[57] This comes on the heels of a December 2020 announcement by Italian police that a crypto exchange operator was responsible for a series of hacks that defrauded over 230,000 people of EUR 120 million (approximately USD$143 million). According to the police, “It is the biggest cyber-financial attack in Italy and one of the biggest in the world… For the first time in Italy and in Europe, we have documented fraudulent and rapacious conduct to the detriment of investors carried out entirely on IT platforms and via the use of virtual currencies.”[58] The central bank and CONSOB have long issued warnings to consumers regarding the risks in cryptocurrencies.

Communication on the Prevention of Financial Crimes Linked to COVID-19, 10 February 2021

The Financial Intelligence Unit released a communication on “Preventing financial crimes phenomenon linked to the COVID-19 emergency,” which details risks related to the increased use of digital solutions. The FIU notes that e-commerce and other instances in which digital payment solutions are utilized incur the risks of fraud and other cybercrime activities.

In 2018, e-commerce accounted for only 6.5% of all retail in the country,[59] but Italians have gravitated towards online shopping amidst strict lockdowns and other COVID-19-related safety measures. First-time online shoppers totaled 2 million in 2020, and the number of SMEs using e-commerce rose by 50%.[60] Internet penetration and smartphone use—the rates of which are still low in Italy—will be instrumental in further boosting e-commerce, as will government-led cashless incentives.

Data Protection Authority Publishes 2021 Objectives, 09 February 2021

The Data Protection Authority published its 2021 objectives, which include collaboration and cooperation with national data protection authorities of other EU member states; investigations into data breaches and the processing of personal data by "data brokers"; boosting transparency; and tracking developments in digitalization's impact on business regarding data protection. The authority is particularly concerned about the emergence of new technologies such as AI solutions, especially relating to the use of biometric data in facial recognition.

Italian Banking Association Announces Experimentation into Digital Euro, 22 December 2020

The Italian Banking Association (ABI) announced that it and its ABI Lab have begun experimentation on the possible development of a digital euro backed by distributed ledger technology (DLT). According to Silvia Attanasio, Head of Innovation at ABI, "The experiment is divided into two work areas: one involving the infrastructure and distribution model to analyse technical feasibility, and the second focusing on programmability to experiment with use-cases that can differentiate the central bank's digital euro from already-available electronic payments."[61] The first stage of experimentation will involve a partnership between SIA, Italian payments network firm, and the ABI Lab Chain, which has been crucial in developing the Spunta blockchain project. The second stage will rely on collaboration between working groups and banks, NTT Data, PwC and Reply.

Bank of Italy Launches Milano Hub to Encourage Innovation, 04 December 2020

The Bank of Italy launched its Milano Hub, an effort to address technological shortcomings in the financial services sector; attract international talent and investment; preserve financial stability; support banks amidst digitalization challenges; and convert Milan—and Italy as a whole—into a major innovation hotspot. Private sector entities will have an opportunity to utilize Milano Hub as a sandbox of sorts, with the central bank overseeing projects to ensure that solutions are safe and risk-free. A team of financial innovation experts has chosen 20 projects centered on machine learning and/or big data. Although the project is ambitious, it remains to be seen whether its goals will come to fruition.

Other recent developments point to Italy's serious intentions in cultivating a more robust fintech ecosystem. Law No. 178 (the "Budget Law 2021"), published 30 December 2020, offers tax credits for investments in research and development. The tax incentive, applicable until 31 December 2022, increased from 12% to 20%, and the expenses limit increased from EUR 3 to 4 million.[62]

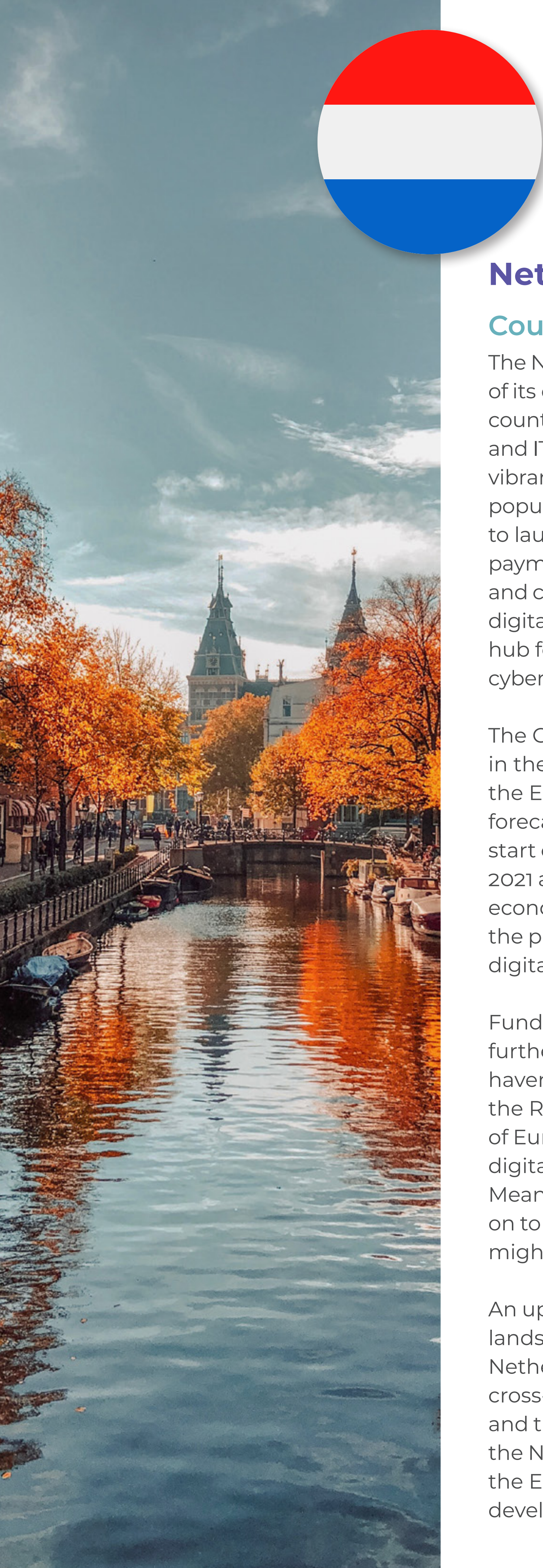
In February 2021, Prime Minister Mario Draghi appointed ex-Vodafone CEO Vittorio Colao—who had previously headed the pandemic-recovery task force—as the new Technological Innovation and Digital Transition Minister. Colao is particularly eager to onboard more citizens to the Sistema Pubblico di Identità Digitale (SPID), a digital ID infrastructure that allows Italians to access government services online. Says Colao, "If I had to say why Italy is behind today, it is because of legal and administrative complexity, which as a government we are determined to simplify."[63]

Italy Announces Cashless Plan, 01 December 2020

The Italian government launched its Italia Cashless plan to promote increased use of digital payment solutions. From 01 January 2021 onwards, users of cards and payment apps can receive a 10% refund on purchases from bars, restaurants, shops, supermarkets and other establishments. The rebate is calculated every six months and users must have made 50 or more cashless transactions to be eligible for it. The maximum reimbursement per six-month period is EUR 150.

As part of Italia Cashless, the Italian Ministry of Finance and Economy also instituted a **Lottery of Receipts**, which went into effect 01 February 2021. Each purchase of at least one euro by a digital payment solution such as a card or app automatically creates a virtual ticket, entering the user into the lottery. Each euro spent creates one virtual ticket, for a maximum of 1,000 tickets per receipt. Participants must register on the lottery portal and present their lottery code to retailers upon purchase.

The cashless incentives have further accelerated the increased adoption of the Sistema Pubblico di Identità Digitale (SPID), a digital ID system that allows citizens to access public administration services online. On 01 March 2021, all public administrations were required to offer citizens access to their services using their digital IDs.[64] At the end of January 2021, about 17 million digital IDs had been issued through the SPID system.[65]



Netherlands

Country Overview

The Netherlands is renowned for the strength and speed of its digital transformation, scoring amongst the top countries in the world for digital intensity, internet access and IT integration.[66] Its rapid digitalization has moulded a vibrant fintech ecosystem, digital economy and tech-savvy population. The Dutch were one of the first countries to launch mobile and online banking, and a growing digital payments sector promises to drive further innovation and competition. The Netherlands' emphasis on digitalization has also made the small country a global hub for cybersecurity, housing NATO and Interpol cybersecurity operations and The Hague Security Delta (HSD).

The COVID-19 pandemic led to a 3.8% contraction in the 2020 Dutch economy,[67] far less severe than the Eurozone's 6.8% plunge.[68] The Netherlands is forecasted to return to pre-pandemic levels by the start of 2022, with a forecasted growth rate of 2.7% in 2021 and 3.7% in 2022.[69] Its financial stability and digital economy outlook remain fairly strong, especially as the pandemic has sped up and widened the scope of digitalization efforts.

Funds from the EU's Recovery and Resilience Facility could further cement the Netherlands' reputation as a digital haven. It was one of the first countries to make use of the Recovery Assistance for Cohesion and the Territories of Europe (REACT-EU), which will facilitate investments in digital transformation and increase the EU co-financing rate. Meanwhile, a pandemic-driven surge in digital payments—on top of an already well-developed cashless landscape—might attract even more fintech to Amsterdam.

An uptick in cyberattacks amidst a swiftly evolving digital landscape has put cybersecurity front and center of the Netherlands' 2021 digital agenda. Major themes include cross-sectoral and international cooperation, data protection and the adaption of new technologies. Additionally, the Netherlands has been instrumental in supporting the European Central Bank's research into the development of a digital euro.

FINANCIAL REGULATORY AUTHORITIES

Central bank: De Nederlansche Bank is the central bank of the Netherlands.

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens or AP) is the independent, supervisory authority for the processing of personal data.

The Netherlands Authority for the Financial Markets (Autoriteit Financiële Markten or AFM) is the country's financial services regulatory authority.

OTHER REGULATORY AUTHORITIES

The Dutch Authority for Consumers and Markets (Autoriteit Consument & Markt or ACM) ensures fair competition between businesses and protects consumers.

POLICY, LAWS AND REGULATIONS

Cybersecurity Regulation Implementation Act, 18 May 2021

The Dutch State Secretary for Economic Affairs and Climate submitted a bill on the implementation process for the EU's Cybersecurity Regulation, which grants the European Union Agency for Cybersecurity (ENISA) a permanent mandate and introduces an EU-wide cybersecurity certification framework for ICT processes, products and services. The certification system will further integrate the digital internal market. ENISA will provide more support to member states in managing cybersecurity incidents and will bolster operational cooperation at the EU level. The regulation comes amidst a surge in pandemic-driven cyberattacks across the EU, which have demonstrated increasing scope and sophistication. Heightened cooperation and a standardized approach to certification will help in identifying and deterring cyber risks.

Cyber Security Council Advisory Report on Strengthening Dutch Sovereignty in Cybersecurity, 14 May 2021

The Cyber Security Council (CSR) published a report warning that the state has become too reliant on American and Chinese companies for cybersecurity solutions. The report recommends five main guidelines to underpin future national strategy and policy:

1. The use of sovereignty-respecting cloud services, secure digital communications networks, and post-quantum cryptography
2. The institution of an assessment framework regarding digital autonomy in cybersecurity

3. Raising awareness on the importance of autonomy in cybersecurity
4. Strengthening the Dutch innovation landscape
5. Ensuring alignment with EU policy and use of EU funding

The report is unsurprising given the Netherlands' usual status as a global vanguard in all things digital and rights-related. This points towards an increasing tendency for the EU to turn inwards and avoid American and Chinese influences—especially where data protection is involved.

Cyber Security Council Advisory Report on Development of a Long-term Cybersecurity Strategy, 06 April 2021

The Cyber Security Council (CSR) published its report *Integral approach to cyber resilience*, which deems the Netherland's current cybersecurity framework to be insufficient in some areas, especially as organized cybercrime soars. The CSR advises the government to invest EUR 833 million in developing a long-term cybersecurity strategy, alongside a EUR 14 million per year allocation to the Public Prosecution in investigating cybercriminals. The CSR further recommends an integrated approach, by which public and private sectors, including banking and financial services, work together in tackling cybercrime. Information sharing and cross-sectoral cooperation has indeed become a major theme across EU member states in their respective cybersecurity priorities. The report also addresses a major weakness in Dutch cybersecurity amidst an increasing reliance on large foreign market parties, which could leave data and vital networks accessible to outside actors. This echoes the 14 May 2021 warning in the CSR's advisory report on strengthening Dutch sovereignty in cybersecurity.

Dutch Banking Association Publication on Open Finance, 29 March 2021

The Dutch Banking Association published a paper entitled "Towards data-driven digital finance - Choices for an Open Finance framework," which describes how open finance can spur on innovation and deliver benefits to customers. In ensuring customer control over their data, a new legal framework would have to be created that allows for the access and sharing of data. This would have to be launched through a Data Services Regulation. The paper details several recommendations that would underpin a strong open finance system, that both encourages innovation and ensures data protection:

1. "Create a broad horizontal framework for Open Data.
2. Establish the scope of new Open Finance financial services proposals across the entire financial sector.
3. For the establishment of Open Finance, opt for minimum legislation for the scope and access to data, and use maximum market forces for actual organization of data exchange.
4. Create a level playing field between different actors.
5. No deepening of mandatory data sharing for the financial sector, without extension to other sectors.
6. Limit Open Finance to natural persons, in line with the GDPR."

Updated Guidelines on Prevention of Money Laundering and Terrorist Financing and Sanctions Act, 23 March 2021

The central bank issued updated guidelines on the Prevention of Money Laundering and Terrorist Financing (Wwft) and Sanctions Act (Sw). The guidelines outline requirements for the main features of a transaction monitoring system, the main features of a control framework for integrity risks, customer due diligence, the reporting of unusual transactions, training, education and awareness.

The Dutch Banking Association estimated that 16 billion EUR in criminal money is laundered through the Netherlands each year, making it a global hotspot for money laundering.[70] A 2020 Cyber Security Assessment by the National Coordinator for Security and Counterterrorism points to the Netherlands' risk of economic espionage due to its advanced economy.

Dutch National Cyber Security Centre Publishes Annual Plan 2021, 11 February 2021

The National Cyber Security Centre (NCSC) published its annual plan for 2021, which outlines its core legal tasks and major priorities for 2021. The three main priorities include crisis preparation and response to digital incidents, support for vital infrastructure and ensuring the digital security of the central government. Key objectives include strengthening organizations' resilience and future-proofing implementation frameworks and legal powers.

The Dutch public prosecutor's office warned that the frequency of cybercrime cases in 2020 was 127% higher than in 2019.[71]

Dutch Authority for Consumers and Markets Publishes Paper on Supervision of Algorithmic Applications, 09 December 2020

The Dutch Authority for Consumers and Markets published a position paper establishing its outlook on the regulatory supervision of algorithmic applications. Although the paper is vague, it supplies a broad framework for how the ACM might address future opportunities and challenges stemming from algorithm-driven technologies like artificial intelligence. The paper and pilot investigation point to the Netherlands' strength in rapidly investigating and adapting innovative technologies. Indeed, Amsterdam has the highest density of AI start-ups per capita in the EU,[72] and in 2019, the Netherlands launched CLAIRE, the globe's largest network for AI research.

Dutch Central Bank Announces New AML Measures for Crypto Services, 11 November 2020

In a move to crack down on money laundering, the Dutch Central Bank has instituted the first rule of its kind in Europe. Crypto service owners must now monitor incoming and outgoing transactions to ensure clients and ultimate beneficiary owners (UBOs) are not on a Dutch or European sanctions list. In return, crypto exchange users must provide the reason for the transaction, the type of wallet used and picture or cryptographic evidence proving ownership of the address linked to the exchange account. The announcement has caused widespread complaints, with some services and users claiming that the evidence can be easily falsified.

Dutch regulators are currently unsure as to how many cryptocurrency investors are in the Netherlands, despite strict KYC and AML measures.[73] Regulators have issued multiple warnings regarding the inherent volatility and lack of valuation in cryptocurrencies.

Norway

Country Overview

As one of the richest countries in the world[74] and host to a vibrant start-up ecosystem, Norway is on the brink of incredible digital transformation. Demand for digital services and products is already high, with cashless payments and electronic IDs popular amongst the country's tech-savvy population. Social stability and one of the highest global standards of living make it an even more attractive hub for fintech start-ups and financial investment.

The effects of the COVID-19 pandemic have not significantly altered Norway's promising digital trajectory. The Norwegian economy contracted by 2.5% in 2020—its weakest performance in 75 years—though it was not affected as severely as the eurozone, which took a 6.8% plunge in GDP.[75] The IMF projects that the economy could grow 3.2% by the end of 2021, a higher growth rate than its pre-pandemic level.[76] Norway's comparatively unscathed status and quick recovery will cement its reputation for financial stability and boost the development of innovative technologies.

Indeed, Norges Bank, the country's central bank, is exploring the possible introduction of a central bank digital currency (CBDC) and will take the next two years to test technical solutions. Norway has the lowest cash use in the world at less than %4 of transactions,[77] making it well-suited for the launch of a new virtual currency. A CBDC might also counter the growing interest in cryptocurrencies, the volatility of which could threaten to upset banking system stability. In reaction to a 30% one-day drop in bitcoin value, Executive Director for Financial Stability Torbjorn Haegeland said in an interview, "We don't see these swings that we've seen yesterday as major threats to financial stability but if exposures continue to increase, that may pose a threat."[78]

FINANCIAL REGULATORY BODIES

Central Bank: Norges Bank is the central bank of Norway. The bank's primary objective is to promote and maintain economic stability in the country. The bank also manages The Government Pension Fund of Norway, one of the largest sovereign wealth funds in the world.

The Norwegian Data Protection Authority (Datatilsynet) is the national agency responsible for implementing and managing the Personal Data Act 2000 and is the primary data protection authority for the country. The agency independently operates under the Ministry of Government Administration and Reform.

The Financial Supervisory Authority of Norway (Finanstilsynet) is a government agency operating under the Ministry of Finance that supervises financial companies within Norway.

STANDARDS, LAWS AND REGULATIONS

Norges Bank Publishes Financial Infrastructure Report, 20 May 2021

Norges Bank's *Financial Infrastructure Report* points to the Norwegian financial system's marked stability over the past few years, even amidst the COVID-19 pandemic. The report then outlines areas for focus and improvement, including cyber resilience, CBDCs and the regulation of crypto-assets.

Because of the growing sophistication of cybercrime, cyber threats are increasingly posing a danger to national security interests, and Norway is ratcheting up its preparedness. Indeed, in October 2020 and May 2021, two major cyberattacks successfully infiltrated the Norwegian Parliament. Norges Bank and the Financial Supervisory Authority are currently preparing for the launch of the threat intelligence-based ethical red teaming (TIBER-NO) framework, modeled after the TIBER-EU framework published by the European Central Bank in 2018. The TIBER framework lays out testing requirements applying to ICT systems, technical defense mechanisms, processes, skills and contingency plans. The tests simulate real-life cyberattacks and are conducted by an external team, offering companies the opportunity to assess and improve their measures and contingency plans.

Regarding cryptoassets, Norges Bank recognizes that, while risky, decentralized finance can also spur on innovation and improve financial sector efficiency. However, the central bank sees uncertainties, pointing to the unclear regulatory status of decentralized finance market infrastructures under the European Commission's MiCA proposal. "Even if such market infrastructures were to come under the regulation, it is unclear how the regulation would be enforced if such market infrastructures were operated in a decentralised manner. Decentralised finance will amplify some of the challenges associated with market infrastructures for trading in tokenised assets…" Norges Bank will monitor developments in cryptoassets and might even propose regulations of its own.

Risk and Vulnerability Analysis 2021 of Financial Sector, 11 May 2021

The Norwegian Financial Supervisory Authority published its *Risk and Vulnerability Analysis 2021*, which outlines the 2020 threat landscape and evaluates measures employed by obliged entities. Top issues include data protection, internal fraud, operations and emergency preparedness, ID theft and money laundering. Although the COVID-19 pandemic presented uncertainties and new challenges, it did not markedly affect the financial system and regulated companies. Still, the report notes the rise of evolving criminal methods, which might not be adequately addressed by existing measures. For instance, traditional transaction monitoring might not properly identify money laundering risks stemming from new criminal methods.

Norway's overall smooth handling of the COVID-19 pandemic points to the strength of its financial stability, relative insularity from EU turbulence and attractiveness as a growing fintech hotspot.

Finance Ministry Publishes Market Report 2021, 23 April 2021

The Norwegian Ministry of Finance submitted the *Financial Market Report 2021* to the Storting, the Norwegian legislature. The report summarizes key developments ranging from consumer protection to digitalization and includes the central bank's annual report as an appendix. Chapter 4 on "Capital access, digitalisation and regulatory development" is especially significant. The chapter points to the rise of fintech in Norway, and that new market participants and technology—like virtual currencies—might warrant further regulatory guidance.
The Ministry's general outlook on digitalization in finance

is positive, and notes that collaboration between the public sector and the finance industry has the potential to develop cost-saving digital solutions.

A subsequent, brief overview of Norges Bank's research into the possible development of a CBDC points to Norway's low cash use but notes its introduction "is not on the cards at this point in time."

Regarding regulatory development, the Ministry of Finance stresses the importance of Norwegian markets' affiliation with the European Single Market, per its European Economic Area (EEA) membership. In safeguarding its "well-functioning" affiliation, relevant EU provisions must be quickly transposed onto Norwegian law. Due to the increasing scale and complexity of EU regulations, both EU and Norwegian authorities must ensure that regulations do not cause an undue burden on small market participants. Norway must also seek to maintain strong economic relations with the UK, which left the EEA alongside its withdrawal from the EU.

Norges Bank Publishes Third Working Group Report on CBDC, 21 April 2021

Norges Bank's *Central bank digital currencies: third report of working group* outlines the third phase of its research into the possible development of a CBDC. The report reviews a potential CBDC's necessary technical characteristics, including CBDC-cash parity, accessibility to a broad swath of the population, frictions (like volume restrictions) to prevent bank runs, payment immediacy, offline functionality and compliance with EEA law. Regarding its technical architecture, Norges Bank suggests a closed distributed ledger technology (DLT) variant, which would allow the bank control over the currency while still permitting aspects of it to be decentralized. Other solutions include a register-based token and programmable money, though neither appear as likely as a DLT-based architecture. On the user side, a digital wallet is currently the most feasible solution, though this could be accompanied by a physical card. In an overview of the effects a CBDC would have on the Norwegian financial system, the report points to the increased probability of bank runs and the difficulty in gauging demand ahead of a possible CBDC launch. It reiterates the uncertainty involved in the possible introduction of a CBDC due to its relatively new technology and limited real-world trials. The central bank will test possible technical solutions over the next two years, and states that, "Any introduction of a CBDC will still lie sometime in the future. The time spent [researching] reflects Norges Bank's view that there is no immediate need to introduce a CBDC."

Norwegian Financial Supervisory Authority Report on Money Laundering and Financing of Terrorism, 26 March 2021

The Norwegian Financial Supervisory Authority report on money laundering and financing of terrorism, part of its series on reports from the supervised sectors 2020, points to an increase in fraud amidst pandemic-driven uncertainty. The authority notes that obliged entities' compliance with AML legislation has not been significantly impacted by the altered landscape, though there is room for improvement.

Norway has traditionally been proactive in its AML/CFT measures. It recently entered a partnership with seven other Nordic and Baltic states in requesting the IMF to examine the region's ML/TF threat landscape and possible weaknesses. The IMF will deliver its analysis and recommendations in 2022.

Publication of 2020 National Risk Assessment Report, 17 December 2020

The Norwegian Police Directorate published its 2020 national risk assessment report, which outlines the money laundering and terrorist financing threat landscape. The COVID-19 pandemic was instrumental in altering the threat landscape, especially in exacerbating money laundering and fraud. Cryptocurrency and new types of payment services pose an especially high risk of ML. Even registered crypto exchanges are risky, while the anonymity in unregistered exchanges poses a particularly high risk.

The report notes, "Cryptocurrency exchangers are primarily actors with little experience who lack established routines for reporting suspicious relationships. Several of the registered exchanges are small enterprises with limited resources and expertise to perform customer control. It is an inherent vulnerability that virtual currency is a digital and cross-border product, where exchanges go fast. Virtual currencies that are anonymous or partially identifiable and mixed with other currencies makes it difficult to trace the blockchain."

Cryptocurrencies can also facilitate tax fraud, the sale of illegal goods and investment fraud, a type of scam which soared amidst the COVID-19 pandemic. The Norwegian Tax Administration (NTA) warned taxpayers who owned or sold crypto in 2020 to enter it on their tax returns and noted that only about 2% of cryptocurrency holders made declarations for 2019.[79] Given these risks, it is likely that Norway will explore stricter and more comprehensive AML and crypto regulations in cracking down on tax evasion and hard-to-trace transactions.

Poland

Country Overview

The Polish economy, renowned for its diversification and high growth pre-2020, did not face as staggering a plunge as the EU economy at large in 2020. It contracted by 3.5%,[80] its first shrinkage since 1996,[81] but is projected to make a swift comeback with a 2021 growth rate of 3.3%.[82] Poland also enjoys the EU's lowest unemployment rate according to Eurostat data.[83]

This promising outlook could further attract start-ups and investment funds to Poland's fintech ecosystem, which has become a major innovation hub in Central and Eastern Europe. Its particularly robust digital payments sector is becoming increasingly developed as the COVID-19 pandemic drives the swift adoption of contactless and online payments.

Despite its encouraging landscape, Poland still lags behind most of Europe in its overall digitalization indicators per the European Commission's Digital Economy and Society Index (DESI) 2020. Scores in digital integration and the use of internet are particularly low, with 60% of Polish companies having a very low level of digitalization, 15% of citizens not online and about half lacking basic digital skills.[84] Meanwhile, though Poland remained relatively safeguarded from the EU's economic nosedive, the pandemic spurred on increased risks in its banking sector, including an increase in write-downs for expected credit losses, institutional weaknesses and the risk of another credit crunch.[85]

Regulatory initiatives, shifting consumer habits and recovery funds in response to the COVID-19 pandemic could help to prioritize and support digitalization, especially in finance and the economy. The country will receive over 58 billion EUR in grants and loans86 from the EU's Recovery and Resilience Facility, 20% of which is mandated to go towards digital transformation efforts.

Although Poland's 2021 digital agenda is basic, it points to serious intentions in further cultivating the fintech ecosystem. Additionally, the central bank is not currently evaluating the possibility of introducing its own central bank digital currency but is monitoring its peers' progress. Marek Dietl, CEO of the Warsaw Stock Exchange, is adamant in promoting the development of a digital zloty and strengthening Polish competitiveness.[87]

FINANCIAL REGULATORY AUTHORITIES

Central Bank: Narodowy Bank Polskink is the central bank of Poland.

Data Protection Authority: The Polish Data Protection Authority (Urzędu Ochrony Danych Osobowych, UODO), created by the Act of 10 May 2018 on the Protection of Personal Data, regulates data protection in Poland per the GDPR.

The Polish Financial Supervisory Authority (Komisja Nadzoru Finansowego, KNF) is Poland's financial regulatory authority. It oversees and regulates banking, capital markets, insurance, pension schemes and e-money institutions.

POLICY, LAWS AND REGULATIONS

Report on the Development of Financial Innovation, 12 May 2021

The Financial Supervisory Authority published a report addressing the role and actions of the Working Group for Development of Financial Innovation, which was created in 2019. The report outlines barriers to the development of fintech in Poland, actions taken and recommendations on strengthening the fintech ecosystem. Key recommendations include the creation of a regulatory sandbox and clarifications of uncertainties in the regulatory framework. A sandbox could be critical in helping Poland compete with Scandinavian innovation hubs, which typically enjoy robust government support and safety nets in the launch of start-ups. In addressing legal, supervisory and regulatory uncertainties, the report points to the Financial Supervisory Authority's Innovation Hub Program, created in 2018, which connects fintech companies with representatives who can answer questions. An unclear regulatory landscape could deter foreign entities from launching a company or branch in the Polish fintech ecosystem, which has little international influence.[88] Regulatory improvements would attract more foreign direct investment, companies and talent to Poland, which already offers sound cybersecurity, a diversified and stable economy, and the region's largest reserve of IT experts.[10]

Financial Supervisory Annual Report 2020, 12 May 2021

The Financial Supervisory Authority published its annual report addressing its 2020 activities. An overview of the payments sector outlines an increase in the use of cashless payment solutions. The use of card payments and digital wallets, which were popular even before the outbreak of the COVID-19 pandemic, have soared amidst changes brought on by the health crisis. The authority's main activity in this sector was overseeing the compliance of obliged entities and entities' admission to the payment services market through licensing and registration.

The report briefly mentions cryptocurrency in addressing education and training on the emergence of new technologies. The KNF does not have any supervisory powers over cryptocurrencies and issued a January 2021 warning to consumers concerning the risks in crypto investments. The authority pointed to cryptoassets' volatility, complexity, difficulty in converting back to cash and lack of protective regulations.

Act Transposing 5AMLD Provisions Published, 29 April 2021

The Act of 30 March 2021, Amending the Act on Anti-Money Laundering and Counterterrorism and Other Acts was published in the official gazette. The act transposes some of the 5AMLD provisions onto national law. Namely, it:

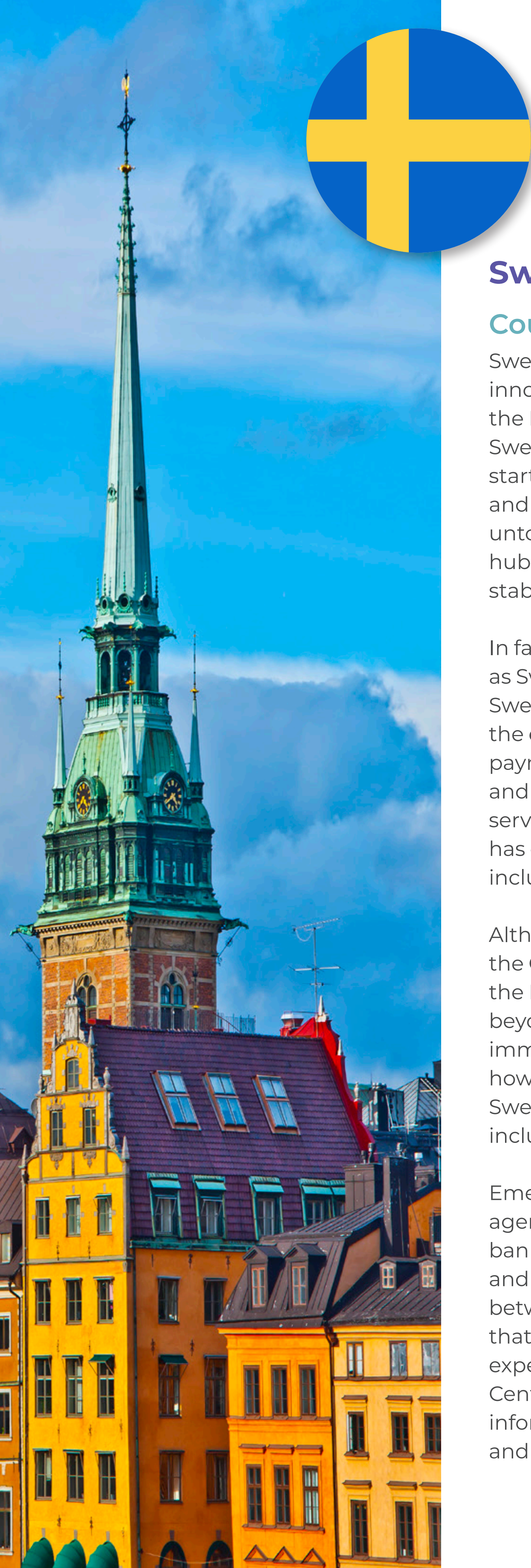
- Imposes new requirements on obliged entities regarding documentation storage and security measures for dealings with high-risk third countries
- Spells out procedures for the verification of identity data in the beneficial owners register
- Requires companies and trusts offering currency exchange services between virtual and fiat currencies, as well as providers of virtual currency accounts, to register with the Ministry of Finance

Resolution on Policy for Artificial Intelligence Development in Poland, 11 January 2021

The resolution on Policy for Artificial Intelligence Development in Poland from 2020, published in the Polish official gazette, outlines opportunities for the development of AI alongside guidelines for its usage. The policy is part of the Polish Strategy Productivity and the Modern State 2030 Strategy and outlines six strategic areas, which include short-term, medium-term and long-term goals. Key strategic areas address the relationships between

AI and society, innovative firms, international cooperation, the public sector, science and education. The goals are broad and ambitious, and if successful, could draw talent currently flocking to Amsterdam, Berlin and Scandinavia. In strengthening society with regard to tech and AI, Poland seeks to become a large beneficiary of the data-based economy and bolster its digital competence, a crucial goal given low digital literacy. The strategic focus on AI and the public sector will additionally help to integrate innovative solutions into the community at large, with support for the rollout of government programs similar to GovTech Polska, initiatives in trusted data spaces, government computing and increased access to data. To support the development of AI firms, Poland aims to create mechanisms in financing their development, establish sandboxes, increase quantity orders and bolster collaboration between start-ups and the government. Support for the Polish scientific and research community in the development of AI solutions will further expand the fintech landscape. In alignment with the EU's rights-based approach to AI, the policy also addresses the support of AI businesses alongside adherence with human dignity and fundamental rights per EU and OECD standards. Indeed, international cooperation and standardization will be key as Europe continues to integrate and Poland strives to become more competitive.

The European Commission's proposed Artificial Intelligence Act, a legal framework to encourage the development of AI solutions while minimizing risk, could supplement or even supersede Poland's resolution. If passed, the Artificial Intelligence Act would harmonize member states' rules on AI solutions to ensure a "well-functioning internal market," which would support Poland's goal in pursuing increased international cooperation and alignment with EU standards. As Poland's policy does not include a well-articulated risk-based approach to the application of AI systems, the EU's Act would be particularly beneficial in helping minimize risk in Polish innovation.



Sweden

Country Overview

Sweden consistently ranks as one of the world's most innovative and digitalized countries, coming in at #2 on the EU's Digital Economy and Survey Index 2020. Indeed, Swedish capital Stockholm has created more billion-dollar start-ups per capita than anywhere outside Silicon Valley,[89] and its fintech scene weathered the pandemic largely untouched.[90] Stockholm's dramatic rise as a global fintech hub is unsurprising given Sweden's wealth, financial stability and receptiveness to change.

In fact, digitalization extends beyond the start-up scene, as Swedes have rapidly adapted to new technologies. Sweden's cash circulation hovers around 1% of the GDP,[91] the electronic identification app BankID and electronic payments app Swish are ubiquitous,[92] and connectivity and internet use rates are high.[93] This amenability to digital services and products, alongside a strong welfare system, has contributed to the country's near 100% financial inclusion rate.[94]

Although Sweden's economy contracted by 2.8% amidst the COVID-19 pandemic, it was relatively insulated from the EU's dire performance and is projected to recover beyond pre-pandemic level in 2021.[95] Sweden was not immune to the pandemic's global surge in cybercrime, however. A December attack—described as the worst in Swedish history—targeted a dozen top businesses, including the Swedish National Space Agency.[96]

Emerging from the pandemic, Sweden's digital agenda includes research into the development of a central bank digital currency (CBDC), a new digital payments system and cybersecurity. Its Project 27 initiative, a joint project between top Nordic banks, aims to create a digital platform that allows real-time, cross-border payments, and is expected to launch in 2022. A National Cyber Security Centre (NCSC) is also in the works. The NCSC will facilitate information exchange and collaboration between public and private sector entities in strengthening defenses against cyberattacks. Although Sweden has already implemented the EU's 5th Anti-Money Laundering Directive (5AMLD), it has not yet transposed the 6AMLD into national law. The deadline for implementation is 03 June 2021.

FINANCIAL REGULATORY AUTHORITIES

Central bank: The **Riksbank** is the Swedish central bank.

Data Protection Authority: The Swedish Authority for Privacy Protection is housed under the Ministry of Justice and protects individuals' privacy.

The Swedish Financial Supervisory Authority (Finansinspektionen, FSA) is the government agency responsible for financial regulation.

POLICY, LAWS AND REGULATIONS

Riksbank Partners with External Entities to Test E-Krona, 28 May 2021

The Riksbank joined a collaboration with consumer bank Handelsbanken and digital services company TietoEVRY in launching the second phase of the e-krona pilot. The second phase of the pilot, which could see results in five years,[97] aims to test the integration of the e-krona's technical platform with the participants' existing internal systems.

In April 2021, the Riksbank published a **report** outlining phase 1 of the e-krona pilot. The technical solution tested in phase 1 was token-based, with e-kronor circulating on a decentralized blockchain platform. This solution, although promising, presents challenges and requires further investigation. Off-line functionality has yet to be tested. Regarding legality, the report notes that there is little to no precedent for the use of a central bank digital currency, and its introduction would probably warrant new regulations. An e-krona would be subject to AML laws and regulations like KYC and transaction tracing.

The launch of the e-krona pilot phase has been driven in part by Sweden's declining cash use and the desire to safeguard against possible future disruptions to the monetary system. However, some Swedish bankers worry that a CBDC could threaten financial stability by spurring on bank runs.[98] The Riksbank is expected to reach a conclusion on the possible e-krona in November 2022.

Publication of National Risk Assessment Money Laundering and Financing of Terrorism in Sweden 2020/2021, 20 April 2021

The national risk assessment of money laundering and financing of terrorism in Sweden 2021/2020, conducted by 16 authorities and the Swedish Bar Association, notes that banks, other financial institutions and unregistered virtual currency exchanges face a high risk of money laundering. Low levels of awareness on money laundering risks play a significant role in heightening the risk of exploitation, and a regular reporting obligation for companies under the purview of country administration boards could aid in bolstering knowledge of such activities. According to a Financial Action Task Force (FATF) publication *Follow-Up Report Sweden 2020*, Sweden has made great strides in strengthening its AML/CFT framework, though the financial industry has still faced notable missteps. In March 2020, the FSA fined Swedbank 4 billion kronor for serious lapses in its AML measures and withholding information from the authority.[99] The assessment comes amidst a wave of Swedish publications on the dangers of money laundering as virtual currency usage and pandemic-driven fraud have risen.

Financial Supervisory Authority Publishes Report on Cryptoassets, 12 February 2021

The Financial Supervisory Authority published its supervision report on *Financial instruments with cryptoassets as underlying asset*, which analyses cryptoassets in the Swedish market and outlines risks in cryptoasset investment. The report stresses the volatility and high-risk status of cryptoassets due to their lack of valuation, and delivers a dire warning, “These instruments are therefore unsuitable for most, if not all, consumers. The absence of a generally accepted credible method of valuation means that investments in financial instruments with underlying crypto-assets are fraught with difficulties for all investors, even those with a good knowledge of the market.” A lack of appropriate consumer protection regulations compounds the inherent risks, although the European Commission’s MiCA proposal could change this. Trading platforms, which are unregulated, pose the risk of market manipulation, such as wash trades. Cryptoassets also facilitate investment scams and money laundering, although the 5AMLD has expanded the regulatory scope in combating crypto-driven ML.

AML Collaboration Between Banks and Swedish Police Authority Becomes Official, 19 January 2021

In June 2020, the top five largest banks in Sweden—Danske Bank, Handelsbanken, Nordea, SEB and Swedbank—-joined the Swedish Policy Authority in the Swedish Anti Money Laundering Intelligence Task Force (SAMLIT) pilot initiative. The pilot collaboration aimed to facilitate cooperation between the banking industry and police in identifying and deterring ML/TF risks. Due to encouraging results, especially regarding information exchange, the pilot collaboration was set to become an official partnership. SAMLIT will further seek to draw in more participant banks and promote regulatory changes to strengthen AML measures. The move points to Sweden's increasingly interdisciplinary approach to fighting crime. Its recently commissioned National Cyber Security Centre (NCSC) is to be established by defense and security agencies, and will be key in facilitating information sharing that could aid in detecting and deterring cyber risks. The government will allocate SEK440 in funds towards its operational costs over 2025-2021. Indeed, the International Monetary Fund (IMF) points to organizational challenges—like the fragmentation between different sectors, such as finance and national security—as a significant obstacle in protection from cyber risks.

Riksbank Report on Payments, 29 October 2020

The Riksbank's report *Payments in Sweden 2020* outlines the evolving and increasingly digitalized Swedish payments sector in 2020, especially in light of the COVID-19 pandemic. Only 9% of the population utilized cash for their last payment, in contrast with 39% in 2010 and 13% in 2018. Cash was primarily utilized for small payments and by older adults. The popularity in digital payments rapidly gained ground in 2012 with the introduction of Swish, the Swedish electronic payments application, and the pandemic increased adoption even further. The swift decline in cash use has presented problems for some demographics, including people living in rural areas and older demographics.

The report notes that the efficiency of international payments must be improved. Card-based, cross-currency payments incur exchange rate markups, and they cannot be used for payments between private individuals and for some types of payments and bills. Account-to-account payments to currencies outside the EU are costly and can often take up to five days. P27, if successfully launched, will be instrumental in revolutionizing the payments industry, making previously inefficient, cross-border and cross-currency transactions convenient and fast.

Riksbank Publishes Commentary on Money and Payments of the Future, 15 October 2020

Riksbank governor Stefan Ingves's economic commentary "Money and payments of the future" outlines measures that must be taken to secure the central bank's functions in the future. Steps include a sufficient cash supply, should the electronic system fail; a national state ID card with e-identification; the introduction of an e-krona; the ability to make cross-currency, cross-border payments at all times; and the ability to make immediate payments in kronor at all times. The measures point to the central bank's ambitious goals and increasing mind towards digitalization and comes on the heels of Sweden's 2017 Digital Strategy, a comprehensive plan to make the country the world's #1 leader in digitalization. The e-krona has already taken center stage of Sweden's 2021 digital agenda, and its cross-border, cross-currency payments system, known as P27, is awaiting permits from EU and national authorities. It has received a clearing license from the Swedish Financial Supervisory Authority.

Assessment on Cyber Risks in the Financial Sector, 31 August 2020

The Swedish Financial Supervisory Authority published its report on *Combatting the Cyber Threat in Sweden: An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector*. The assessment strikes a serious tone, pointing to the high risks—like information security and costs—that cyber threats pose to the international financial system. Alongside the COVID-19 pandemic, the rapidly evolving financial sector—spurred on in large part by the growing dominance of fintech—has contributed to greater vulnerabilities to cyber risk. Fintech companies drive competition and innovation, which bolster financial stability, but can also attract more threats as startups' cyber teams are not as large as those of more traditional entities. Startup companies have also traditionally shown less aversion to risk. As fintech drives an increasingly integrated financial sector, their heightened susceptibility to risk threatens to affect the system at large more readily.

Switzerland

Country Overview

Renowned as an international banking and fintech hub, Switzerland enjoys the second-highest GDP per capita in the world and the 18th-largest economy.[100] Political neutrality, social stability and huge expenditures on R&D[101] have further contributed to the country's status as a global leader in finance and innovation. The World Intellectual Property Organization (WIPO)'s Global Innovation Index 2020 ranks Switzerland #1, for the tenth year in a row.

Although the COVID-19 pandemic drove the Swiss economy to its worst performance in 45 years with a contraction of 2.9%,[102] the Alpine country still fared much better than other developed nations and is forecasted to rebound quickly.[103] The pandemic has also been key in accelerating Switzerland's digital transformation.

A Swiss National Bank (SNB) **Money Market Event** on COVID19- and digitalization points to pandemic-driven increases in cashless payments and automation in big data as primary catalysts in the country's digital transformation. This has expanded opportunities for innovation amidst a more uncertain risk landscape, creating new challenges for the central bank. As it emerges from the pandemic, Switzerland's focuses include the possible development of a central bank digital currency (CBDC), data protection and digital empowerment, strengthening its flagging AML/CFT framework, and competition and innovation in the digital sector.

However, the future of Switzerland's fintech ecosystem might be largely driven by market forces, supported by an accommodating regulatory landscape. Swiss regulators have not taken as proactive an approach to fintech regulations—especially regarding open banking—as the EU has. Indeed, many Swiss banking and fintech community members construe the EU's regulatory approach as heavy-handed and instead tout a market-based one.[104] They have reason to be confident given the past year's immense growth in private sector development of fintech and open banking innovations.

In May 2020, Switzerland's principal stock exchange SIX launched its b.Link platform, which allows financial institutions and third-party providers to securely exchange and access data via APIs. In October 2020, Credit Suisse announced that it would launch a CSX digital portal allowing clients to conduct all banking online. Other leading initiatives include the Open Banking Project and the Swiss Fintech Innovations' (SFTI) Common API. An increase in competition due to the surging presence of neo-banks will likely spur on even further innovation in the Swiss fintech sector.

Still, this increasingly complex, market-powered landscape will result in changes to regulatory frameworks and the creation of new ones. Regulations on data protection, AML and digital inclusion will be crucial in keeping up with rapidly evolving developments in fintech and ensuring transparency, accountability, and security.

FINANCIAL REGULATORY BODIES

Central Bank: The **Swiss National Bank (SNB)** is the central bank of Switzerland. The SNB is responsible for monetary policy, with special attention to price stability.

Data Protection Authority: The **Federal Data Protection and Information Commissioner (FDPIC)** has a supervisory and advisory role in ensuring data protection and transparency in Switzerland.

The Swiss Financial Market Supervisory Authority (FINMA), housed under the Federal Department of Finance, is responsible for financial regulation, including the supervision of banks, securities, stock exchanges and other financial intermediaries.

STANDARDS, LAWS AND REGULATIONS

Swiss-French Cross-Border CBDC Trial, 06 June 2021

The Banque de France, the Swiss National Bank and the Bank for International Settlements (BIS) Innovation Hub announced that they planned on conducting an investigation—named Project Jura—into cross-border settlements using wholesale CBDCs. The banks have partnered with Accenture, Credit Suisse, Natixis, R3, SIX Digital Exchange and UBS in executing the project. The experiment will involve a euro CBDC, a Swiss franc CBDC and a French digital financial instrument on a distributed ledger technology (DLT) platform. The Swiss National Bank clarified in the wake of Project Helvetia—which demonstrated the feasibility of linking tokenized digital assets with central bank money—that the introduction of a CBDC is not a guarantee, though the continuing research points to serious intentions in exploring its development.

FINMA Allows Chip Scanning in Client Onboarding, 05 May 2021

Following a consultation on the revision of the Circular on "Video and online identification," The Swiss Financial Market Supervisory Authority (FINMA) announced it has approved the use of chip scanning in customer due diligence for client onboarding. Financial institutions will be able to scan chips in biometric identity documents—like biometric passports—thus streamlining the identity verification process. FINMA has not approved "automatic video-based identification followed by downstream manual verification by employees"[105] due to security concerns. The authority also announced that geolocation services can be employed to confirm home addresses. The changes will come into effect on 01 June 2021.

Swiss Federal Council Votes to Reform AML Legislation, 19 March 2021

The Swiss Federal Council voted to reform the Anti-Money Laundering Act (AMLA) in anticipation of a 2022 Financial Action Task Force (FATF) audit. Key revisions include enhanced KYC, customer due diligence, transparency and reporting requirements. Financial intermediaries will be obliged to verify customer identity, record the services provided to customers and gather information as to their background and purpose, as well as report suspicions of financial crime to the Money Laundering Reporting Office Switzerland (MLROS). The legislation more closely adheres to international standards, but it does not address areas of concern noted by corruption watchdogs.[106]

Indeed, Switzerland's money laundering landscape is fraught with risk, and the state lags well behind other developed nations in the strength of its AML/CFT framework. A 2020 report by the Basel Institute for Governance on ML/TF risks around the globe has ranked Switzerland #93 of 141 countries on a worst-to-best scale. The score is a composite of information regarding risks related to, amongst other factors, the country's AML/CFT framework. According to the Basel report, Switzerland's mediocre score is partly attributable to a high level of financial secrecy, which diminishes the efficacy of its AML/CFT framework. In a 2020 interview with Swiss newspaper TagesAnzeiger, former head of the MLROS Thelesklaf pointed to a lack of political will in pursuing reforms and outdated technology in processing reports from banks.

CBDC Research: Project Helvetia Demonstrates Viability of Linking Tokenized Digital Assets with Central Bank Money, 03 December 2020

According to the Bank for International Settlements (BIS) report, "Project Helvetia is a joint experiment by the BIS Innovation Hub (BISIH) Swiss Centre, SIX Group AG (SIX) and the Swiss National Bank (SNB), exploring the integration of tokenised assets and central bank money on the SDX platform." The successfully executed experiment demonstrates the legal and functional viability in integrating tokenized digital assets with central bank money, although the Swiss National Bank clarifies that this does not point to a sure launch of a wholesale central bank digital currency (CBDC) and that a retail CBDC is out of the question. Further experimentation is underway and due to be completed by Q3 2021. Despite uncertainties as to an eventual CBDC introduction, the growing popularity of stablecoins in Switzerland might increase pressure on the central bank to develop its equivalent.

In conjunction with Project Helvetia's completion, BISIH announced a plan to establish five new innovation hubs in London, Toronto, Stockholm, Frankfurt and Paris, which will partner with local central banks, Nordic central banks and the Eurosystem. Andréa M. Maechler, governing board member of the SNB, stated in a press conference on Project Helvetia that the expansion of BISIH will allow for an increased focus on strategic priorities, including CBDCs, open finance, cybersecurity, APIs and new financial market infrastructures.[107]

FINMA Publishes 2020 Risk Monitor, 11 November 2020

The Swiss Financial Market Supervisory Authority published its 2020 risk monitor, which outlines the 2020 threat landscape and its evolving supervisory focus. The dominant theme is the COVID-19 pandemic, which put pressure on the financial system in contributing to the emergence of new risks and exacerbating existing ones. A principal threat has been a rise in cyber risks, including increases in the distribution of malware, phishing emails and distributed denial-of-service (DDos) attacks.

Although the overall risk level in money laundering has stayed the same, the landscape has shifted with the advent of new technologies. For the first time, FINMA identifies blockchain technology-based digital assets as a risk to the financial industry. Anonymity and "the speed and cross-border nature of the transactions" can aggravate ML/TF risks. This is especially problematic given the prevalence of crypto use in Switzerland, its lack of a comprehensive regulatory framework on virtual currency and reputation as a money laundering haven.[108]

Parliament Approves Revised Swiss Federal Act on Data Protection, 25 September 2020

The revised Swiss Federal Act on Data Protection (FADP) implements many GDPR provisions while allowing for significant differences. Obliged entities will, for the most part, not undergo major changes in the processing of personal data, although new documentation, auditing and reporting requirements have been established. Companies will be obliged to immediately report serious data breaches to the Federal Data Protection and Information Commissioner (FDPIC); utilize data protection impact assessments (DPIA) in advance of potentially risky data processing; seek approval before using sub-processors; and issue a privacy notice each time data is collected. In contrast with the GDPR, controllers have the option—but not the obligation—to appoint a data protection officer. Should an intentional violation of the revDPA occur, individuals in lieu of the company could face criminal sanctions. The revised act will enter into force in 2022.

Parliament Approves the Swiss DLT Act, 25 September 2020

Parliament adopted the Federal Act on the Adaptation of Federal Law to Developments in the Technology of Distributed Electronic Registers, which clears up legal uncertainty surrounding DLT in securities, creates a new and independent DLT financial infrastructure and imposes requirements on DLT trading facilities. On 01 February 2021, provisions related to the launch of blockchain-based securities came into effect. The remaining provisions will come into force August 2021.

DLT is swiftly becoming a central feature of the Swiss financial system. Cryptocurrency has become so popular that the canton of Zug, as of February 2021, now accepts tax payments in bitcoin and ether, while the municipalities of Zermatt and Chiasso allow bitcoin for smaller tax payments.[109] Following in the footsteps of rivals Goldman Sachs and Morgan Stanley, UBS is considering offering digital currency investments in response to soaring demand.[110]

The flourishing crypto scene has not come without blips, especially in light of regulators' concerns over the increased risk of ML in crypto transactions. Switzerland's leading crypto banker, Bitcoin Suisse, applied for a banking license in mid-2019, but a 17 May 2021 FINMA **press release** reveals that the authority informed the company it is ineligible for approval. FINMA expressed concern regarding weaknesses in Bitcoin Suisse's AML mechanisms.

Publication of Digital Switzerland Strategy, September 2020

The Federal Council's Digital Switzerland Strategy outlines guidelines and specific measures towards implementing the country's digitalization goals across multiple sectors, including the economy. Overall objectives include support for: digital inclusion; security, trust and transparency; individuals' digital empowerment; innovation and competition; and environmental and climate goals. The overall strategy is underpinned by four principles: digital inclusion, digital development, state support to reduce friction amidst structural change and a cross-sectoral approach to digitalization, and each section outlines how it helps in meeting UN sustainable development goals.

The section on digital transformation in the economy addresses ambitious goals alongside existing conditions. Highlights include:

"**4.6.1.** Switzerland is characterized by a high employment rate and good-quality working conditions

4.6.2. Switzerland will provide room for the development of new business models

4.6.3. An innovative, globally networked fintech sector improves the competitiveness of the Swiss finance industry

4.6.4. The cities, municipalities and regions of Switzerland are characterized by a high capacity for innovation

4.6.7. Switzerland will take advantage of its opportunities regarding the virtual international economy"

A section on "Data, digital content and artificial intelligence" addresses the possible development of a Swiss cloud, the importance of individuals' control over their data, the improved access to digital content, the development of open data, a responsible and transparent approach to AI and a "modern, coherent" regulatory framework underpinning rights to and use of data.

Turkey

Country Overview

Turkey has one of the world's fastest growing economies and is poised for incredible digital transformation. Its rapid growth in internet usage and mobile connections,[111] young population and a government keen to modernize have fueled innovations in the banking and payments sectors, and its fintech ecosystem has swiftly developed. Istanbul's strategic location as a nexus between Europe, Asia and the Middle East makes it a particularly attractive hub for international banks and fintech companies.

Despite the emerging market's promising outlook, a recent deceleration in reforms and the COVID-19 pandemic have weakened Turkey's economic and financial sectors. Although Turkey had a 2020 growth rate of 1.8%,[112] one of the few countries in 2020 to have avoided an economic contraction, the health crisis accentuated gender and income inequalities, unemployment skyrocketed, and the value of the lira plummeted. The country's overall economic prospects are expected to improve in 2021, with a projected GDP growth of 5.7%,[113] but the financial sector still faces an uncertain future. The first quarter of 2021 saw a sharp loss in the banking sector's profits[114] [115] and inflation stood at 16.6% in May 2021.[116] Turkish President Recep Tayyip Erdoğan continues to promote interest rate cuts[117] and fired Central Bank President Naci Ağbal in March.

Turkey's post-COVID recovery offers the country a chance to spearhead further digital transformation goals alongside its economic ones. The $15.4 billion Turkey Relance recovery plan, which emphasizes competitiveness and cohesion,[118] mainly provides short-term economic relief, but the government has shown it is eager to revamp digitalization efforts. In June 2021, Technology Minister Mustafa Varank stated that Turkey "aims to become a trend-setting country" in innovative technologies like artificial intelligence.[119] Former Central Bank President Naci Ağbal announced in December 2020 that a conceptual phase on the possible development of a central bank digital currency had been completed, and that the bank aimed to begin pilot tests in the second half of 2021. Other key priorities for 2021 include the regulation of digital currencies and bolstering cybersecurity.

FINANCIAL REGULATORY AUTHORITIES

The Central Bank of the Republic of Turkey (TCMB) is the primary banking authority in the country.

The Personal Data Protection Authority was established under the Law on the Protection of Personal Data to pass and enforce data protection regulations in Turkey.

The Banking Regulation and Supervision Authority (BRSA) is responsible for overseeing and regulating the Turkish banking sector.

POLICY, LAWS AND REGULATIONS

New Reporting Requirement for Digital Currency Exchanges, 06 May 2021

Minister of Treasury and Finance Lütfi Elvan announced that digital currency exchanges are now required to report transactions over TRY 10,000 (approximately USD$1200) to the Financial Crimes Investigation Board (MASAK). On 01 May 2021, a **presidential decree** added crypto platforms to the list of entities obliged to comply with AML regulations. The Central Bank is also reportedly considering the establishment of a central custodian bank for holding digital assets, a capital threshold for digital currency exchanges and a requirement that crypto executives adhere to a certain standard in their understanding of digital currencies. This crackdown on crypto follows the April 2021 arrests of employees at two digital currency exchanges on allegations of massive fraud.

Central Bank Bans Use of Cryptocurrencies and Cryptoassets in Payments, 16 April 2021

The Central Bank published a regulation banning the usage of cryptocurrencies and cryptoassets in the direct or indirect purchase of goods and services. Additionally, no service can be provided that allows for the direct or indirect use of cryptoassets and cryptoassets may not be utilized in the provision of payment services and the issuing of electronic money. Neither can payment service providers develop business models that facilitate the direct or indirect use of cryptoassets in the provision of payment services and the issuing of electronic money, or provide services related to such business models. The Central Bank cites crypto's volatility and its use in illegal activities. The regulation went into effect 30 April 2021. A bill on the regulation and exchange of cryptocurrencies is expected to be introduced in October.

Video Identification in Banks' Digital Onboarding, 05 April 2021

The Regulation on Remote Identification Methods to be Used by Banks and Establishing Contractual Relationships in Electronic Environment was published in the Turkish official gazette. Modeled after BaFin's procedures for video identification in Germany, the regulation aims to facilitate and clarify the use of video identification by banks in digital onboarding. It defines requirements for the verification of the customer's identity document, verification of the customer and authentication of the customer via an SMS one-time passcode (OTP) by video communication. The video communication must be uninterrupted, in real-time and of high image and sound quality. Software solutions must have been manufactured in Turkey, and providers and manufacturers must have R&D centers and response teams located in-country. This emphasis on technological sovereignty is echoed often in Turkish regulation and government rhetoric. The regulation went into effect 01 May 2021 and could be key in heightening financial inclusion for people who live in rural areas, the elderly and others for whom in-person onboarding presents challenges.

Turkey Unveils Cybersecurity Plan, 26 December 2020

Turkey unveiled its three-year National Cyber Security Strategy and Action Plan, which outlines 40 actions and 75 implementation steps in strengthening the country's cybersecurity framework. Overall objectives include protecting the cybersecurity of critical infrastructure, further empowering teams combating cyberthreats, developing technological solutions for operational purposes, increasing awareness in cybersecurity and investing in cybersecurity-related human capital. According to the Transport and Infrastructure Ministry—which formulated the plan in partnership with public and private sectors, NGOs and universities—Turkey successfully thwarted 325,000 cyberattacks since 2018, utilizing Turkish software like Avcı, Azad and Kasırga.[120]

The plan comes amidst a concerted effort to strengthen national cybersecurity and encourage the development of innovative Turkish solutions. In February 2020, Turkey established the National Cybersecurity Intervention Center (USOM) in Ankara, which collaborates with public and private companies in addressing cyberthreats, especially denial-of-service attacks.[121] The center, a subsidiary of the national Information Technologies and Communications Authority, relies on Turkish software.

United Kingdom

Country Overview

Strict and lengthy lockdowns due to the COVID-19 pandemic contributed to the UK's worst economic performance on record, with a 2020 GDP contraction of 9.9%.[122] The Brexit transition and cyberattacks further compounded the rocky landscape. Meanwhile, the pandemic rapidly accelerated digital transformation, with contactless payments making up 88.6% of UK payments in 2020[123] and consumers flocking to e-commerce.

Although Prime Minister Boris Johnson's recovery package does not prioritize digitalization as the EU's does, it is a sweeping plan that emphasizes economic growth—including support for job training and university education—which will dovetail well with digitalization efforts. Despite uncertainties with regard to open banking, digital identity and the payments industry, the UK's attractive fintech landscape and regulations in the works will help to usher in digitalization while fostering innovation and financial inclusion.

Digital identity could prove an important cornerstone in the UK's digital transformation, although it has had a shaky start. In February, the DCMS released a draft of a digital identity trust framework, which will expand upon the government-to-citizen aspects of the Gov.uk Verify system. This is expected to broaden secure digital identities in all industries, aid in AML and anti-fraud measures, attract more fintech entities and onboard previously unbanked individuals. According to a Financial Conduct Authority survey, 1.2 million UK adults are unbanked.[124] Without a workable digital identity system, digitalization could further exacerbate unequal access to financial services.

Digitalization will be instrumental in strengthening the UK's rapidly growing fintech ecosystem. As it stands, the UK fintech sector makes up 10% of the UK's global market share and draws the most venture capital investment in all of Europe.[125] Faced with increasing competition, COVID-19 and Brexit-driven uncertainty, the 2021 Kalifa Review of Fintech warns that the industry could lose its competitive edge without reforms and adaptation.

FINANCIAL REGULATORY BODIES

Central Bank: The **Bank of England (BoE)** is the central bank for the United Kingdom. The bank maintains financial stability for the country, oversees monetary policy and issues currency.

Other Financial Bodies: The **Financial Conduct Authority (FCA)** regulates the financial services industry in the UK. The agency protects consumers and promotes fair competition in the financial services market.

Her Majesty's Treasury (HM Treasury) is the national government's economic and finance ministry. The HM Treasury's primary objective is to develop public economic policy and promote economic growth.

The Department for Digital, Culture, Media & Sport (DCMS) is responsible for the digital economy as well as key aspects of media including the internet, in addition to culture and sport.

STANDARDS, LAWS AND REGULATIONS

HM Treasury Call for Evidence and Consultation on National AML/CTF Framework, 22 July 2021

HM Treasury published a **consultation** on amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The amendments seek to "introduce an ongoing requirement to report discrepancies in beneficial ownership information," expand access to information sharing gateways and implement FATF's "travel rule" with regard to cryptoassets. The consultation was introduced alongside a **call for evidence** seeking feedback on the effectiveness of the national AML/CTF regime. Both the consultation and call for evidence were closed on 14 October 2021. Secondary legislation is expected to be introduced in spring 2022.

Financial Conduct Authority Extends Deadlines for Implementation of SCA Requirements, 20 May and 16 April 2021

On 20 May 2021, The Financial Conduct Authority (FCA) issued a **statement** extending the deadline for the implementation of strong customer authentication (SCA) requirements in e-commerce transactions to 14 March 2022. The six-month extension aims to "ensure minimal disruption to merchants and consumers, and recognizes ongoing challenges facing the industry to be ready by the previous 14 September 2021 deadline."

TOP 3 REGULATORY CONCERNS FOR INTO 2022

56%

Complying with AML requirements for virtual currencies/ cryptocurrencies

52%

Anticipated EU and individual member state artificial intelligence regulations

44%

Anticipated EU Digital Wallet

This follows another FCA deadline extension regarding SCA implementation. On 16 April 2021, the FCA delayed the requirement for card issuers to implement second factor authentication for the purposes of SCA, following data protection concerns over behavioral biometrics. Card issuers have signaled that behavioral biometrics as currently employed could conflict with the GDPR's requirement that individuals provide "explicit consent" for the management of their data. UK Finance is seeking advice from the Information Commissioner's Office on whether a "substantial public interest argument" could negate the need for explicit consent from users.

Although the data protection issue relates only to behavioral biometrics, the FCA postponed the deadline for all forms of second factor authentication. This has not dampened the FCA's enthusiasm for behavioral biometrics, saying that it "encourage[s] all issuers to use this additional time to explore the use of behavioral biometrics over knowledge factors where possible". The deadline was 14 September 2021.

As in the EU, the UK's rollout of SCA requirements has been fraught with uncertainty regarding implementation and enforcement, alongside an oft-shifting timeline. Customers have expressed concerns regarding the requirement to conduct SCA every 90 days, while merchants worry about the effects SCA will have on B2B payments.

Financial Conduct Authority Sends Letter to E-Money Firms Regarding Concerns, 18 May 2021

The Financial Conduct Authority (FCA) sent a letter to UK e-money firms entreating them to clarify to their customers that their accounts are not safeguarded per traditional banking protections. The FCA fears that e-money firms have been misleading in promoting their services, highlighting advantages while minimizing risks. This violates an FCA requirement (BCOBS 2.3.1AR) that communications to e-money customers must include a "fair and prominent indication of any risks." A primary concern of the FCA is that e-money accounts are not protected by the Financial Services Compensation Scheme (FSCS), which protects consumers if a financial firm fails. The warning points to the FCA's increasing concerns about payment and e-money services, especially given the COVID-19 pandemic and the summer 2020 bust of Germany payments service Wirecard. A 2018 FCA **report** found that e-money firms had some weaknesses in their AML/CFT frameworks, a concern that has since been

>60% OF UK BANKS BIGGEST COMPLIANCE CHALLENGE IS SAFEGUARDING SENSITIVE DATA

63%

Safeguarding sensitive data

56%

Keeping pace with changes in consumer privacy laws, industry regulations

48%

Reducing or preventing cyberattacks and fraud

reiterated by an HM treasury **risk assessment** of ML/TF, which found that payment and e-money services were at a medium risk of money laundering.

Publication of Regulatory Initiatives Grid, 07 May 2021

The Financial Services Regulatory Initiatives Forum—composed of the Financial Conduct Authority, Bank of England and other regulators—published the third edition of the Regulatory Initiatives Grid, which outlines plans and initiatives in the works. The authorities outline timeframes for the delivery of several projects related to the payments sector:

- Publication of consultation paper on Confirmation of Payee (CoP), between June and August 2021
- Publication of follow-up paper on the Call for Views on authorized push payment (APP) scam prevention, between July and September 2021
- Publication of follow-up paper mitigating risks associated with launch of New Payments Architecture (NPA), between July and September 2021
- Publication of statement on review of Consumer Protection in Faster Payments, between September and October 2021
- Publication of policy statement following a consultation on updates to the Payment Services and Electronic Money - Our Approach document, Q3 2021
- Publication of Final Strategy on Payment Systems Regulator's desired outcomes over the next five years, between October and December 2021

Competition and Markets Authority Publishes Paper on Digital Regulation Cooperation Forum, 04 May 2021

The Competition and Markets Authority (CMA) published a policy paper on Digital Regulation Cooperation Forum: Embedding coherence and cooperation in the fabric of digital regulators, which addresses barriers to digital cooperation and outlines possible future remedies. The Digital Regulation Cooperation Forum (DRCF), established in July 2020, is a partnership between the Information Commissioner's Office (ICO), the CMA, the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA) to promote coordination amongst the regulators. The paper recommends three major ideas for the government to consider: "supporting appropriate information sharing; embedding coherence and cooperation in the statutory framework for digital services; and providing transparency and accountability."

In promoting a facilitated approach to information sharing, the paper reiterates the importance of ensuring regulators that confidential information shall remain protected by existing legislation. This paper comes on the heels of a 10 March 2021 CMA publication **Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022.** The policy paper stresses the importance of trust in digital technology, alongside competition and innovation that offer benefits to users. The three priority areas for the DRCF over the 2021-2022 timeframe will include a strategic response to industry and technology changes, joint strategic projects that bolster engagement and cooperation, and regulatory coherence.

Law Commission Publishes Call for Evidence on Digital Assets, 30 April 2021

The Law Commission published a call for evidence on digital assets in advance of a consultation paper, which will lay out a proposal for reform. The call recognizes the legal uncertainty underpinning digital assets and seeks to garner information on how they are used. The Law Commission notes that it was asked in March 2020 by the Ministry of Justice (MoJ) and Department for Digital, Culture, Media and Sport (DCMS) to review the law for opportunities on reform with regard to digital assets, including cryptoassets. The deadline for responses was 30 July 2021. The Law Commission anticipates publishing a paper on digital assets by the end of 2021. Some UK banks—like HSBC[126] and retail bank NatWest[127]—have taken a cautious or even completely prohibitive approach to cryptocurrency because of its inherent volatility.

Government to Introduce New Cybersecurity Laws, 21 April 2021

The Department for Digital, Culture, Media & Sport has announced that it plans to unveil new cybersecurity laws ensuring smart devices are better protected from cybercrime. Requirements will include a ban on manufacturers installing a default password, a facilitated system for customers to report security weaknesses and an obligation for customers to be told at sale how long their smart devices will receive security software updates.

Bank of England and HM Treasury Announce Creation of Central Bank Digital Currency Taskforce, 19 April 2021

The Bank of England and HM Treasury have established a joint exploratory taskforce on the development of a central bank digital currency (CBDC). The digital money would complement cash, not replace it. The Bank of England also announced the creation of a CBDC Engagement Forum, which will collect input on the

TOP COMPLIANCE TECHNOLOGIES FOR UK BANKS

48%

Classic biometrics

(e.g., voice, face, fingerprint)

48%

Mobile application shielding

(i.e., techniques that make it harder for hackers to break phone apps)

48%

Behavioral biometrics

(e.g., recognizing user through their digital, physical and cognitive behavior)

non-tech implications of the currency's development, and a CBDC Technology Forum that will gather input on the technological side. In a 13 May **speech**, Sir John Cunliffe, Deputy Governor for Financial Stability, points to some of the advantages in the use of digital money. He notes that "...digital public money and the infrastructure necessary to support it would help ensure the necessary interoperability and common standards between all major payment systems in the future economy. Furthermore, he raises an important concern in that, "... future private money and payments providers may not have the commercial incentives to provide useable services for the unbanked and other parts of the population. Digital public money, appropriately designed, may therefore have an important role to play in ensuring inclusion." The speech draws major themes from the 12 March 2020 Bank of England discussion **paper** *Central Bank Digital Currency: Opportunities, challenges and design*. In a 07 June 2021 discussion **paper** *New forms of digital money*, the bank noted that it had not yet decided whether it will issue a digital pound, but that a future CBDC could promote competition and financial inclusion. The report states that, "Where coupled with innovations such as programmable money and micropayments, a CBDC may increase the utility of central bank money when compared to cash. And it could support a resilient, innovative and competitive payments landscape."

Financial Conduct Authority Publishes Feedback Statement on Open Finance, 31 March 2021

The Financial Conduct Authority's (FCA) feedback statement details its vision for open finance, its potential benefits and the results from its Call for Input regarding its regulatory strategy. The statement emphasizes respondents' concerns that the requirement for customers to apply SCA every 90 days causes friction, and that API availability and performance should be strengthened with a mind towards customer convenience. This parallels concerns in the EU over friction in payments caused by SCA.

Financial Conduct Authority Publishes Policy Statement on Extension of Annual Financial Crime Reporting Obligation, 31 March 2021

Per the policy statement *Extension of Annual Financial Crime Reporting Obligation*, the FCA will require cryptoasset exchange providers, custodian wallet providers, payment institutions (with exceptions) and electronic money institutions to submit an annual

82%

of UK bank execs expect development a Central Bank Digital Currency within two years

financial crime report (a "REP-CRIM"). This will broaden the scope of reporting firms from approximately 2500 to approximately 7000. The requirement will go into effect 30 March 2022.

UK Finance Publishes Report on Blueprint and Transition Plan for Open Banking, 02 March 2021

In light of unmet PSD2 requirements, an HM Treasury Payments Landscape Review and CMA Order standards, UK Finance and Baringa Partners have published a report on how the Open Banking Implementation Entity (OBIE) should evolve in addressing concerns and improving functionality and security. The report outlines plans for a "Future Entity" model that improves upon the current one, while ensuring a smooth transition and compliance with regulatory requirements. The Future Entity, which will center the open data and payments market, is premised on safety, efficiency and reliability. Outcomes in support of this goal include:

1. "Widespread adoption of Open Data and Payments propositions
2. The services provided will be highly secure and reliable
3. The UK remains at the forefront of innovation in Open API propositions
4. Those in vulnerable situations are able to experience equal benefits of Open Data and Payments propositions
5. Poor customer outcomes are prevented"

Open banking has gained in popularity, with over 2.5 million businesses and individual users in the UK,[128] yet this still constitutes only a small percentage of the 68-million-person population.[129]

Publication of the Kalifa Review of Fintech, 26 February 2021

The widely read Kalifa Review, commissioned by HM Treasury, gives recommendations on bolstering fintech amidst tightening competition, COVID-19 and regulatory uncertainty in the face of Brexit. Ron Kalifa, entrepreneur and Chairman of payments company Network International, spells out five points in securing the UK's superior fintech status: policy and regulation, skills, investment, international and national connectivity. "Policy and Regulation" suggests the establishment of a new digital finance package, which would create a regulatory framework to support emerging technology; a "scalebox" that provides extra support to firms focusing on innovative technology; and the development

After collecting comments on its February policy paper, in July, DCMS issued an updated consultation.

Per DCMS, “the consultation seeks views on three key issues:

- The governance system to oversee digital identity and make sure organizations comply with the rules
- How to allow trusted organizations to make digital checks against authoritative government-held data
- Establishing the legal validity of digital identities, so people are confident they are as good as physical documents like passports or bank statements.”

In addition, the UK government plans to play a significant role in the digital identity market, including establishing a regulatory department to oversee members of the trust framework.

of a global trade policy that prioritizes a fintech agenda. Sub-recommendations address a permanent digital sandbox in enhancing cooperation, fintech’s role in supporting financial inclusion, the digitalization of financial services (a CBDC and the regulation of cryptoassets); and the development of a data strategy (creation of a digital ID, the prioritization of Smart Data and a review of regulatory implications of AI). The report is a key indicator of potential future regulations, especially as the UK feels the pressure to maintain its strong lead in fintech. The recommendation on a digital ID will be especially important towards financial inclusion measures and the possible launch of a CBDC.

UK Publishes Policy Paper on Digital Identity, 11 February 2021

The Department for Digital, Culture, Media & Sport has published a policy paper outlining the proposed digital identity and attributes trust framework. The draft paper, geared towards organizations using or seeking to use digital identity applications, lays out the principles and policies underlying broad goals on digital identity. The framework aims to cultivate trust between users and providers of digital identity services, foster cooperation between the government and private sector in addressing fraud and cybercrime, and facilitate interoperability between service providers. Organizations must institute a data management policy that outlines how they “create, obtain, transform, share, protect, document and preserve data”; a privacy compliance framework; a response plan to incidents; and fraud monitoring. User control over their data is heavily emphasized. The proposal suggests ways in which a digital identity service could be developed under the framework, including an application akin to a wallet and an online identity service provider that can disclose appropriate information to a third party. The framework also takes an important step towards boosting digital inclusion. People without access to traditional documents as evidence of identity can rely on a vouching system, wherein a trusted person vouches for someone’s identity. This could prove instrumental in enfranchising people like refugees, asylum-seekers and individuals in high-poverty settings. The paper ends with an outline of next steps, including a call for feedback and a forthcoming second version of the framework.

IN ANTICIPATION OF A CBDC, UK BANKS ARE INVESTING IN:

56%

Technology stacks that can support digital currency

52%

Remote onboarding and digital agreements for account opening

52%

Drafting deposit and transfer rules for digital currency

HM Treasury Releases National Risk Assessment on Money Laundering and Terrorist Financing 2020, 17 December 2020

HM Treasury released its National Risk Assessment on Money Laundering and Terrorist Financing 2020 on a changing threat landscape and responses to it. Although COVID-19 has changed the threat landscape, it has not led to an overall increase in threats. Major changes include the increased use of cryptoassets in money laundering, the exploitation of pandemic-related fears in tailoring messages to install malware, and the increased criminal use of non-cash and mobile payments. This shift in the threat landscape will require both regulators and individuals to adapt.

Even before the March 2020 onslaught of COVID-19 in the UK, the Financial Conduct Authority (FCA) had already signaled a harsher approach to its AML procedures with regard to e-payment services. On 11 February 2020, the FCA froze one million ePayments Systems Limited customer accounts due to the claim that weaknesses had been found in the firm's AML systems and controls. The firm, one of the largest digital payments companies in the UK, received notification from the FCA on 25 February 2021—over a year later—that it could begin processing refunds to customers.[130]

ENDNOTES

1 "Post-Brexit Britain dominates European fintech funding charts." Finextra, 12 July 2021. **https://www.finextra.com/newsarticle/38439/post-brexit-britain-dominates-european-fintech-funding-charts**.

2 Hutchinson, Lorna. "EU unveils new anti-money laundering package." The Parliament Magazine, 21 July 2021. https://www.theparliamentmagazine.eu/news/article/eu-unveils-new-antimoney-laundering-package

3 "MiCA And New AML Regulation Will Interlink, Says EU Commission – ACAMS." VIXIO, 17 July 2021. https://vixio.com/insight/paymentscompliance/mica-and-new-aml-regulation-will-interlink-says-eu-commission-acams

4 Cunningham, Francine. "European eID Regulation aims to facilitate cross border transactions." Lexology, 08 July 2021. https://www.lexology.com/library/detail.aspx?g=a8aa2786-957b-4c37-903a-1ae6ec09376b

5 "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient – Questions and Answers." European Commission, 16 December 2020. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2392

6 Leyden, John. "EU pushes plans for Joint Cyber Unit in fight against increased cyber-attacks." The Daily Swig, 23 June 2021. https://portswigger.net/daily-swig/eu-pushes-plans-for-joint-cyber-unit-in-fight-against-increased-cyber-attacks.

7 "Berlin Declaration on Digital Society and Value-Based Digital Government." EU2020.de, 08 December 2020.

8 "ECB publishes the results of the public consultation on a digital euro." European Central Bank, 14 April 2021. https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html

9 Look, Carolyn. "ECB's Panetta Floats 3,000-Euro Limit on Digital Cash." Bloomberg, 09 February 2021. https://www.bloomberg.com/news/articles/2021-02-09/ecb-s-panetta-floats-3-000-euro-limit-on-digital-cash-spiegel

10 Patel, Mohammed. "Strong Customer Authentication (SCA) ;– Impact Assessment – January 2021." CMSPI, 23 February 2021. https://cmspi.com/eur/resources/sca-january-updates

11 "The Digital Markets Act: ensuring fair and open digital markets." European Commission https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

12 "Proposal for a Regulation of the European Parliament and the Council on European Data Governance (Data Governance Act)." European Commission, 25 November 2020

13 Waterbley, Séverine. "Belgium's Economy in a Nutshell - Economic Outlook of February 2021." Economie, 17 March 2021. https://economie.fgov.be/en/publication/belgiums-economy-nutshell-3

14 "Economic forecast: Some EU countries will recover in 2021, others must wait until 2022." Euronews, 11 February 2021. https://www.euronews.com/2021/02/11/economic-forecast-some-eu-countries-will-recover-in-2021-others-must-wait-until-2022

15 "Phishing in 2020 cost Belgians €34 million, says regulator." The Brussels Times, 24 March 2021. https://www.brusselstimes.com/news/belgium-all-news/161561/phishing-in-2020-cost-belgians-e34-million-says-regulator/

16 Hope, Alan. "Report: Pandemic allowed organised crime to flourish." The Brussels Times, 15 May 2021. https://www.brusselstimes.com/news/belgium-all-news/169676/report-pandemic-allowed-organised-crime-to-flourish-mony -laundering-health-crisis-counterfeit

17 Bischoff, Paul. "Which countries have the worst (and best) cybersecurity?" Comparitech, 24 March 2021. https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country

18 "The economic context of Denmark." Nordea. https://www.nordeatrade.com/se/explore-new-market/denmark/economical-context

19 "The Top 25 Economies in the World." Investopedia, 24 December 2020. https://www.investopedia.com/insights/worlds-top-economies

20 "French tech startups and scaleups to watch in 2021." Sifted. https://sifted.eu/rankings/french-startups-top-rankings

21 "Covid-19 pandemic pushes French economy into deep recession." France24, 29 January 2021. https://www.france24.com/en/europe/20210129-covid-19-pandemic-pushes-french-economy-into-deep-recession

22 Lovell, Tammy. "Emmanuel Macron pledges €1bn for cybersecurity after hospital ransomware attacks." Healthcare IT News, 22 February 2021. https://www.healthcareitnews.com/news/emea/emmanuel-macron-pledges-1bn-cybersecurity-after-hospital-ransomware-attacks

23 Keohane, David and Peggy Hollinger. "Pandemic brought surge in French cyber attacks, warns Thales CEO." Financial Times, 06 April 2021. https://www.ft.com/content/70e1c40d-acc8-4e8e-8ce3-3e0d9901358a.

24 "France Economic Snapshot." Organisation for Economic Co-operation and Development, May 2021. https://www.oecd.org/economy/france-economic-snapshot

25 "France aims to spend €30 billion on decarbonising its economy." Euronews, 07 May 2021. https://www.euronews.com/2021/05/07/france-aims-to-spend-30bn-on-decarbonising-its-economy

26 "Central banks of Singapore, France trial cross border CBDC using JP Morgan tech." edger Insights, 08 July 2020. https://www.ledgerinsights.com/central-bank-singapore-france-cross-border-cbdc-jp-morgan-tech

27 Smith, Tyler. Monetary Authority of Singapore and Banque de France Report Success from CBDC Experimentation." The Fintech Times, 15 July 2021. https://thefintechtimes.com/monetary-authority-of-singapore-and-banque-de-france-report-success-from-cbdc-experimentation

28 "Central banks of France, Tunisia in wholesale cross border CBDC trial." Ledger Insights, 19 July 2021. https://www.ledgerinsights.com/central-bank-of-france-tunisia-in-wholesale-cross-border-cbdc-trial

29 Seibt, Sébastian. "Why is France's finance minister at war with Facebook's cryptocurrency?" France24, 14 September 2019. https://www.france24.com/en/20190914-french-finance-minister-bruno-le-maire-war-with-facebook-cryptocurrency

30 "La polémique sur le paiement des rançons de cyberattaques." Ecole de Guerre Economique, 26 May 2021. https://www.ege.fr/infoguerre/la-polemique-sur-le-paiement-des-rancons-de-cyberattaques

31 Connolly, Kate. "New ID law aims to help reduce 'digital shyness' in Germany." The Guardian, 22 May 2021. https://www.theguardian.com/world/2021/may/22/new-id-law-aims-to-help-reduce-digital-shyness-in-germany

32 Dao, Mai Chi and Aiko Mineshima. "Germany's Post-COVID-19 Recovery in Five Charts." International Monetary Fund, 19 January 2021. https://www.imf.org/en/News/Articles/2021/01/15/na011921-germanys-post-covid19-recovery-in-five-charts

33 "Germany to spend 90% of EU recovery money on green, digital goals." Reuters, 27 April 2021. https://www.reuters.com/article/us-health-coronavirus-germany-recovery-idUSKBN2CE1HY.

34 “Scholz: Clear signal for climate action and digitalization.” Federal Ministry of Finance, 27 April 2021. https://www.bundesfinanzministerium.de/Content/EN/Pressemitteilungen/2021/2021-04-27-german-recovery-and-resilience-plan-adopted.html

35 Hüsch, Moritz et al. “Germany Publishes New Draft Rules for Cookies and Similar Technologies.” Inside Privacy, Covington & Burlington LLP, 27 January 2021. https://www.insideprivacy.com/data-privacy/germany-publishes-new-draft-rules-for-cookies-and-similar-technologies

36 Noyan, Oliver. “Germany adopts new data protection and privacy law.” EURACTIV, 21 May 2021. https://www.euractiv.com/section/digital/news/germany-adopts-new-data-protection-and-privacy-law

37 Hamacher, Adriana. “‘Damn Huge’: Germany Opens Up to Institutional Crypto Funds.” Decrypt, 28 April 2021. https://decrypt.co/69323/damn-huge-germany-opens-up-to-institutional-crypto-funds

38 Michel, Galit. “The Real Impact of PSD2.” Global Banking and Finance Review. https://www.globalbankingandfinance.com/the-real-impact-of-psd2

39 Heinrich, Daniel. “Germany, EU move toward cashless payment during pandemic.” Deutsche Welle, 05 January 2021. https://www.dw.com/en/germany-eu-move-toward-cashless-payment-during-pandemic/a-56138122

40 “German central bank makes case for blockchain settlement in CBDC debate.” Finextra, 25 March 2021. https://www.finextra.com/newsarticle/37745/german-central-bank-makes-case-for-blockchain-settlement-in-cbdc-debate

41 Digital Economy and Society Index (DESI) 2020: Greece. European Commission, 2020.

42 McCarthy, Niall. “The Countries With The Largest Shadow Economies.” Forbes, 9 Feb. 2017, www.forbes.com/sites/niallmccarthy/2017/02/09/where-the-worlds-shadow-economies-are-firmly-established-infographic.

43 Helms, Kevin. “9 Countries Show Huge Growth in Cryptocurrency Interest.” Bitcoin News, Bitcoin, 3 May 2020, https://news.bitcoin.com/countries-growth-cryptocurrency-coinmarketcap

44 “Recovery and Resilience Facility: Germany and Greece submit official recovery and resilience plans.” European Commission, 28 April 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1990.

45 Willis, Richard. “Greece: EIB to help manage EUR 5 billion of investments as part of Greek National Recovery and Resilience Plan: ‘Greece 2.0.’” European Investment Bank, 12 April 2021, https://www.eib.org/en/press/all/2021-120-eib-to-help-manage-eur-5-billion-of-investments -as-part-of-greek-national-recovery-and-resilience-plan-greece-2-0.

46 World Investment Report 2020. United Nations Conference on Trade and Development, 2020.

47 “Italy.” Worldometer, 08 June 2021. https://www.worldometers.info/coronavirus/country/italy/.

48 Orlandi, Giorgia. “Italy’s digital divide: One third of students don’t have access to online lessons.” Euronews, 02 April 2021. https://www.euronews.com/2021/04/01/italy-s-digital-divide-one-third-of-students-don-t-have-access-to-online-lessons.

49 Za, Valentina et al. “Pandemic leaves digital laggard Italy scrambling to catch up.” Reuters, 21 March 2021. https://www.reuters.com/article/us-health-coronavirus-italy-digital-insi/pandemic-leaves-digital-laggard-italy-scrambling-to-catch-up-idUSKBN2BD0AX.

50 “Covid makes cybercrime soar in Italy: + 47% between January and March 2021.” Italy24 News, 06 May 2021. https://www.italy24news.com/News/41216.html.

51 “Italy’s economy seen growing 4.1% this year, business lobby says.” Reuters, 10 April 2021. https://www.reuters.com/article/us-italy-economy-growth-estimates-idUSKBN2BX0AE.

52 Za, Valentina et al. “Pandemic leaves digital laggard Italy scrambling to catch up.” Reuters, 21 March 2021. https://www.reuters.com/article/us-health-coronavirus-italy-digital-insi/pandemic-leaves-digital-laggard-italy-scrambling-to-catch-up-idUSKBN2BD0AX.

53 Fonte, Giuseppe and Gavin Jones. “Draghi says deal reached with EU on Italy’s recovery plan – officials.” Reuters, 25 April 2021. https://www.reuters.com/world/europe/draghi-says-deal-reached-with-eu-italys-recovery-plan-officials-2021-04-25/.

54 “Recovery and Resilience Facility: Belgium, Italy, Austria, and Slovenia submit official recovery and resilience plans.” European Commission, 01 May 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2101.

55 “Central bank backed surety, guarantee blockchain completes pilot, to launch this year.” Ledger Insights, 10 May 2021. https://www.ledgerinsights.com/surety-guarantee-blockchain-completes-pilot-launch-this-year/.

56 Handagama, Sandali. “Around 100 Italian Banks Are Officially on a Blockchain.” Coindesk, 13 October 2020. https://www.coindesk.com/italian-banking-association-100.

57 Nazarro, Sergio. “EXCLUSIVE: Inside Italy’s fight against money laundering and the innovative new methods used to stay ahead of the mafia’s use of technology to hide its dirty money.” AML Intelligence, 25 January 2021. https://www.amlintelligence.com/2021/01/exclusive-inside-italys-fight-against-money-laundering/.

58 “Italian police accuse cryptocurrency exchange boss of huge fraud.” Reuters, 21 December 2020. https://www.reuters.com/article/italy-cyber-cryptocurrency-idINKBN28V1XQ.

59 “2020 E-commerce Payments Trends Report: Italy.” J.P. Morgan. https://www.jpmorgan.com/europe/merchant-services/insights/reports/italy-2020#footnote-1.

60 Za, Valentina et al. “Pandemic leaves digital laggard Italy scrambling to catch up.” Reuters, 21 March 2021. https://www.reuters.com/article/us-health-coronavirus-italy-digital-insi/pandemic-leaves-digital-laggard-italy-scrambling-to-catch-up-idUSKBN2BD0AX.

61 “The Spunta project – blockchain for Italian interbank reconciliation.” European Payments Council, 11 March 2021. https://www.europeanpaymentscouncil.eu/news-insights/insight/spunta-project-blockchain-italian-interbank-reconciliation.

62 Scampuddu, Barbara and Gian Luca Nieddu. International Tax Review, 25 January 2021. https://www.internationaltaxreview.com/article/b1q7cqqtwb2h26/italy-publishes-2021-budget-law.

63 Johnson, Miles. “Vittorio Colao vows to fix Italy’s red tape bureaucracy.” Financial Times, 16 May 2021. https://www.ft.com/content/9bef85c1-38a7-47a3-87ad-5c3b8c683bfe.

64 D’Ambrosio, Annarita. Dal 1° marzo vecchi Pin in soffitta: Spid, Cie e Cns aprono le porte a tutti i siti della Pa. Il Sole 24 Ore, 26 February 2021. https://www.ilsole24ore.com/art/dal-1marzo-vecchi-pin-soffitta-spid-cie-e-cns-aprono-porte-tutti-siti-pa-ADHvEKKB?refresh_ce=1.

65 “SPID on high speed: State of Play on Digital Identity in Italy.” Namirial, 28 January 2021. https://www.namirial.com/en/namirial-spid-digital-identity-electronic-identity-eid-italy-state-of-play-jan-2021/.

66 “The Netherlands Thrives in a World of Digital Connections.” Invest in Holland. https://investinholland.com/news/the-netherlands-thrives-in-a-world-of-digital-connections/.

67 “Economic contraction 0.1 percent in Q4 2020.” Statistics Netherlands, 16 February 2021. https://www.cbs.nl/en-gb/news/2021/07/economic-contraction-0-1-percent-in-q4-2020.

68 Eurozone economy shrank less than feared in 2020 — Eurostat estimate.” Euronews, 02 February 2021. https://www.euronews.com/2021/02/02/eurozone-economy-shrank-less-than-feared-in-2020-eurostat-estimate.

69 “Netherlands Economic Snapshot.” Organisation for Economic Co-operation and Development, May 2021. https://www.oecd.org/economy/netherlands-economic-snapshot/.

70 Meijer, Bart. “Dutch banks join forces in fight against money laundering.” Reuters, 08 July 2020. https://www.reuters.com/article/us-netherlands-banks-money-laundering-idUSKBN2492Q9.

71 Pritchard, Stephen. “The criminal element: Cybercrime cases in the Netherlands more than doubled in 2020.” The Daily Swig, 24 February 2021. https://portswigger.net/daily-swig/the-criminal-element-cybercrime-cases-in-the-netherlands-more-than-doubled-in-2020.

72 “Investments in AI startups, scaleups are increasing worldwide, except in the Netherlands: Techleap.” Silicon Canals, 06 May 2021. https://siliconcanals.com/news/startups/investments-ai-startups-netherlands/.

73 Avan-Nomayo, Osato. “Dutch regulators unsure of number of crypto investors in Netherlands.” Cointelegraph, 20 May 2021. https://cointelegraph.com/news/dutch-regulators-unsure-of-number-of-crypto-investors-in-netherlands.

74 “GDP per capita (current US$).” World Bank Group, 2019. https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

75 “Norway’s economy weakest in 75 years in 2020, but Q4 shines.” Reuters, 12 February 2021.

76 “IMF: Norway has handled the Covid-19 crisis very well.” Regjeringen, 26 April 2021. https://www.regjeringen.no/en/aktuelt/imf-norway-has-handled-the-covid-19-crisis-very-well/id2845979/.

77 Central bank digital currencies: third report of working group. Norges Bank, 2021. https://www.norges-bank.no/contentassets/554ee1f1ac53417d99d43708f5abbe14/norges-bank-papers-1-2021.pdf.

78 Ummelas, Ott. “Crypto Swings May Become a Threat, Norway’s Central Bank Warns.” Bloomberg, 20 May 2021. https://www.bloomberg.com/news/articles/2021-05-20/crypto-swings-may-become-a-threat-norway-s-central-bank-warns.

79 Wright, Turner. “Norwegian authorities urge crypto users to declare earnings on upcoming return.” Coin Telegraph, 21 April 2021. https://cointelegraph.com/news/norwegian-authorities-urge-crypto-users-to-declare-earnings-on-upcoming-return.

80 Bukowski, Paweł and Wojtek Paczos. “Why is Poland’s economy emerging so strongly from the pandemic? A comparison with the UK.” London School of Economics European Politics and Policy, 19 May 2021. https://blogs.lse.ac.uk/europpblog/2021/05/19/why-is-polands-economy-emerging-so-strongly-from-the-pandemic-a-comparison-with-the-uk/.

81 “UPDATE 1-Polish economy shrinks in 2020 first time in years, as forecast.” Reuters, 29 January 2021. https://www.reuters.com/article/poland-economy-gdp-idUSL8N2K42VN.

82 “Polish Economy Returns to Growth Amidst Pandemic-Related Setbacks.” World Bank, 31 March 2021. https://www.worldbank.org/en/news/press-release/2021/03/31/polish-economy-returns-to-growth-amidst-pandemic-related-setbacks.

83 “Unemployment Statistics.” Eurostat. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Unemployment_statistics.

84 “Digital Economy and Society Index (DESI) 2020—Poland.” European Commission. https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020.

85 Kość, Wojciech. “Political deal allows Poland to move on EU recovery fund.” Politico, 27 April 2021. https://www.politico.eu/article/political-deal-allows-poland-to-move-on-eu-recovery-fund/.

86 Adamowski, Jarosław. “Poland Should Introduce CBDC To Protect Its Economy - Stock Exchange CEO.” Cryptonews, 07 May 2021. https://cryptonews.com/news/poland-should-introduce-cbdc-to-protect-its-economy-stock-ex-10224.htm.

87 Kliber, Agata et al. “Triggers and Obstacles to the Development of the FinTech Sector in Poland.” Risks, 01 January 2021.

88 Krajewski, Robert. “Why Poland Should Be The Next Go-To IT Outsourcing For US Startups.” Forbes, 09 June 2021. https://www.forbes.com/sites/forbestechcouncil/2021/06/09/why-poland-should-be-the-next-go-to-it-outsourcing-for-us -startups/?sh=6aa8462074d9.

89 Stockholm Fintech Guide. Invest Stockholm. https://www.investstockholm.com/globalassets/invest/reports/stockholm-fintech-guide.pdf.

90 “What’s Next for Sweden’s Fintech Ecosystem?” FinTech Global, 04 May 2021. https://fintech.global/globalregtechsummit/whats-next-for-swedens-fintech-ecosystem/#:~:text=Sweden’s%20FinTech%20 ecosystem%20has%20gone,millions%20of%20dollars%20last%20year.

91 Sharma, Rakesh. “Sweden Takes Another Step Toward a Digital Currency.” Investopedia, 14 December 2020. https://www.investopedia.com/sweden-takes-another-step-toward-a-digital-currency-5092069.

92 “Sweden—The First Cashless Society?” Swedish Institute, 10 December 2020. https://sweden.se/business/cashless-society/.

93 Digital Economy and Society Index (DESI) 2020. European Commission, 2020.

94 “Sweden.” The World Bank. https://datatopics.worldbank.org/g20fidata/country/sweden.

95 “Swedish Output to Surpass Pre-Pandemic Levels This Year.” Fitch Ratings, 07 May 2021. https://www.fitchratings.com/research/sovereigns/swedish-output-to-surpass-pre-pandemic-levels-this-year-07-05-2021.

96 Sweeney, Oisin. “Sweden Hit by Massive Cyber-Attack.” Euro Weekly News, 22 December 2020. https://www.euroweeklynews.com/2020/12/22/sweden-hit-by-massive-cyber-attack/.

97 Crawley, Jamie. “Sweden’s Central Bank to Test Digital Currency With Handelsbanken.” Coindesk, 28 May 2021. https://www.coindesk.com/riksbank-handelsbanken-cbdc-test.

98 Fulton, Colm. “Swedish bankers face identity crisis over digital currency plans.” Reuters, 05 January 2021. https://www.reuters.com/article/us-sweden-banks-digital-currency-idUSKBN29A1HV.

99 Fulton, Colm et al. “Swedbank hit with record $386 million fine over Baltic money-laundering breaches.” Reuters, 19 March 2020. https://www.reuters.com/article/us-europe-moneylaundering-swedbank-idUSKBN2163LU.

100 Bajpai, Prableen. “World’s 5 Richest Nations By GDP Per Capita.” Nasdaq, 20 May 2021. https://www.nasdaq.com/articles/worlds-5-richest-nations-by-gdp-per-capita-2021-05-20.

101 “Research and development expenditure (% of GDP) – Switzerland.” World Bank. https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=CH&most_recent_value_desc=false.

102 Allen, Matthew. “Swiss economy suffers worst slump in 45 years.” Swissinfo, 26 February 2021. https://www.swissinfo.ch/eng/swiss-economy-suffers-worst-slump-in-45-years/46403548.

103 “Switzerland: Staff Concluding Statement of the 2021 Article IV Mission.” The International Monetary Fund, 07 April 2021. https://www.imf.org/en/News/Articles/2021/04/06/mcs040621-switzerland-staff-concluding-statement-of-the-2021-article-iv-mission.

104 Franklin, Jimmie. “The Swiss Prefer Regulation-Free Open Banking.” VIXIO, 15 September 2020. https://pc.vixio.com/article/63152/insights/swiss-prefer-regulation-free-open-banking.

105 “FINMA allows chip scanning in online identification process.” FINMA, 17 May 2021. https://www.finma.ch/en/news/2021/05/20210517-mm-rs-16-07-online-identifizierung/.

106 “Swiss lawmakers have agreed to revise the money laundering law but have rejected new rules for lawyers, notaries and other consultants.” Swissinfo, 10 March 2021. https://www.swissinfo.ch/eng/parliament-agrees-modest-tightening-of-anti-money-laundering-law/46435970.

107 Franklin, Jimmie. “Swiss Shy Away From Retail CBDC.” VIXIO, 03 December 2020. https://pc.vixio.com/article/64094/insights/swiss-shy-away-retail-cbdc.

108 “Swiss lawmakers have agreed to revise the money laundering law but have rejected new rules for lawyers, notaries and other consultants.” Swissinfo, 10 March 2021. https://www.swissinfo.ch/eng/parliament-agrees-modest-tightening-of-anti-money-laundering-law/46435970.

109 Khatri, Yogita. “Swiss canton Zug now accepts bitcoin and ether for tax payments.” The Block, 18 February 2021. https://www.theblockcrypto.com/linked/95270/swiss-canton-zug-now-accepts-bitcoin-ether-tax-payments.

110 Choudhury, Ambereen et al. “UBS Explores Offering Crypto Investments to Rich Clients.” Bloomberg, 10 May 2021. https://www.bloomberg.com/news/articles/2021-05-10/ubs-exploring-ways-to-offer-crypto-investments-to-rich-clients.

111 Kemp, Simon. “Digital 2021: Turkey.” DataReportal, 11 February 2021. https://datareportal.com/reports/digital-2021-turkey.

112 Kucukgocmen, Ali. “Turkey emerges from COVID-19-hit 2020 with 1.8% economic growth.” Reuters, 01 March 2021. https://www.reuters.com/article/us-turkey-economy-gdp-idUSKCN2AT1UE.

113 “Turkey Economic Snapshot—Economic Forecast Summary (May 2021).” OECD, May 2021. https://www.oecd.org/economy/turkey-economic-snapshot/.

114 Petrova, Aleksia. “Turkish banks’ net profit down 39% y/y at end-Feb.” SeeNews, 29 March 2021. https://seenews.com/news/turkish-banks-net-profit-down-39-yy-at-end-feb-736190.

115 “Turkish state-run banks may need taxpayer funds to meet losses – academic.” Ahval, 10 June 2021. https://ahvalnews.com/turkey-banking/turkish-state-run-banks-may-need-taxpayer-funds-meet-losses-academic.

116 “Turkish inflation falls unexpectedly to nearly 16.6% in May.” Daily Sabah, 03 June 2021. https://www.dailysabah.com/business/economy/turkish-inflation-falls-unexpectedly-to-nearly-166-in-may.

117 “Turkish lira crashes to record low on Erdogan’s call for rate cut.” Al Jazeera, 02 June 2021. https://www.aljazeera.com/economy/2021/6/2/turkish-lira-crashes-to-record-low-on-erdogans-call-for-rate-cut.

118 “Turkey—Government and institution measures in response to COVID-19.” KPMG, 28 October 2020. https://home.kpmg/xx/en/home/insights/2020/04/turkey-government-and-institution-measures-in-response-to-covid.html.

119 “New ‘Turcorns’ on the way: Minister.” Hurriyet Daily News, 10 June 2021. https://www.hurriyetdailynews.com/new-turcorns-on-the-way-minister-165412.

120 Şimşek, Barış. “Turkey launches 3-year cybersecurity action plan.” Daily Sabah, 29 December 2020. https://www.dailysabah.com/politics/turkey-launches-3-year-cybersecurity-action-plan/news.

121 “Turkey’s new center set to beef up nationwide cybersecurity.” Daily Sabah, 10 February 2020. https://www.dailysabah.com/turkey/2020/02/10/turkeys-new-center-set-to-beef-up-nationwide-cybersecurity.

122 McAuley, Niamh. “GDP first quarterly estimate, UK: October to December 2020.” Office for National Statistics, 12 February 2021. https://www.ons.gov.uk/economy/grossdomesticproductgdp/bulletins/gdpfirstquarterlyestimateuk/octobertodecember2020.

123 “Insights: COVID-19 and the rise of the contactless consumer.” Barclay’s, 05 February 2021. https://home.barclays/news/2021/02/Insights--COVID-19-and-the-rise-of-the-contactless-consumer/.

124 Financial Lives 2020 survey: the impact of coronavirus. Financial Conduct Authority, 11 February 2021. https://www.fca.org.uk/publication/research/financial-lives-survey-2020.pdf.

125 Kalifa Review of UK Fintech. 26 February 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978396/KalifaReviewofUKFintech01.pdf.

126 Wilson, Tom. “HSBC bans customers from buying bitcoin-backer MicroStrategy shares.” Nasdaq, 12 April 2021. https://www.nasdaq.com/articles/hsbc-bans-customers-from-buying-bitcoin-backer-microstrategy-shares-2021-04-12-0.

127 Makortoff, Kayleena. “NatWest will refuse to serve business customers who accept cryptocurrencies.” The Guardian, 21 April 2021. https://www.theguardian.com/technology/2021/apr/21/natwest-will-refuse-to-serve-business-customers-who-accept-cryptocurrencies.

128 “Three years since PSD2 marked the start of Open Banking, the UK has built a world-leading ecosystem.” Open Banking, 13 January 2021. https://www.openbanking.org.uk/about-us/latest-news/three-years-since-psd2-marked-the-start-of-open-banking-the-uk-has-built-a-world-leading-ecosystem/#:~:text=More%20than%202.5%20million%20UK,access%20credit%20and%20make%20payments.

129 “Total population, both sexes combined (thousands).” UN Data, 2021. https://data.un.org/Data.aspx?q=united+kingdom+population+2021&d=PopDiv&f=variableID%3a12%3bcrID%3a826%3btimeID%3a87.

130 Wilkes, Guy. “Does the FCA’s new hardline approach to AML failure treat customers fairly?” Lexology, 17 May 2021. https://www.lexology.com/library/detail.aspx?g=a30a9066-eb70-4528-8400-d02c978ed666.

Middle East

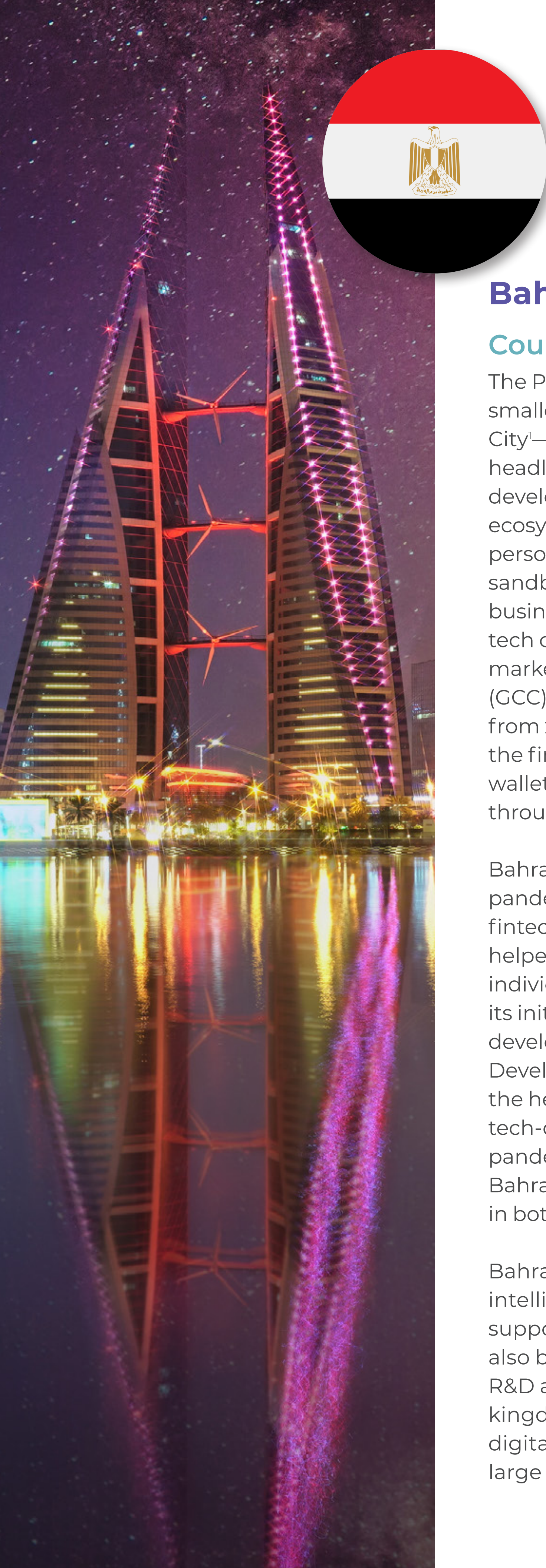
The Middle East is undergoing exciting developments in fintech as states seek to diversify oil-reliant economies and recover from the pandemic. The wealthy and ambitious Gulf Cooperation Council (GCC) states—including Bahrain, the Kingdom of Saudi Arabia, Qatar and the United Arab Emirates—are eager to provide regulatory and financial support to fintechs, develop artificial intelligence and explore central bank digital currencies (CBDCs). The Kingdom of Saudi Arabia and the United Arab Emirates have the most established fintech hubs in the GCC, but fintech-friendly Bahrain will be a market to watch in 2022.

Rapid digital transformation and a surge in fintech investment could help these states to compete with digital powerhouses like Singapore and Taiwan.

Israel, nicknamed the “Startup Nation,” similarly continues to cultivate its robust fintech ecosystem and promote digitalization. The central bank has completed a digital shekel pilot, the Ministry of Finance has called for the establishment of a fintech regulatory sandbox and a national artificial intelligence program is in the works. As Israeli innovation is quick to develop, regulators must ensure they institute stronger cybersecurity and data protection standards to accommodate disruptive technologies like AI, distributed ledger technology (DLT) and big data.

Meanwhile, developing countries across the Middle East have enormous growth potential in fintech. Egypt is a key state to watch as it undergoes socioeconomic transformation. Its regulators have made some progress in providing greater regulatory clarity for fintech, digital payments are gaining in popularity and 2020 saw the first Egyptian fintech reach unicorn status. Barriers to the development of fintech persist, however, as cash use still dominates, regulatory uncertainty remains and national cybersecurity is weak.

Digitalization will be especially crucial in broadening public access to financial services, promoting economic diversification and encouraging pandemic recovery in conflict-affected states such as Iraq and Libya. Going forward, governments, the private sector and international organizations must first partner to strengthen digital infrastructure. As internet and mobile phone penetration rates increase, innovation in payments will have an opportunity to expand and drive financial inclusion. Both Iraq and Libya, devastated by the legacies of war, have high percentages of adults who are unbanked.



Bahrain

Country Overview

The Persian Gulf island country of Bahrain is one of the smallest states in the world—about the size of New York City[1]—but its wealth and innovation have made international headlines. **The Global Fintech Ecosystem Report 2020**, developed by Startup Genome, notes that Bahrain's fintech ecosystem is one to watch. Bahrain's 0% corporate and personal tax rates, wage subsidies, fintech regulatory sandbox, low capital startup requirements for certain businesses and a USD$100 million fund towards "unquoted tech companies" have made the kingdom an attractive market for fintech companies. The Gulf Cooperation Council (GCC) state is now home to over 90 fintechs, a 35% increase from 2018.[2] Over 53 million virtual payments were made in the first half of 2021, and in 2020, Bahrain's national digital wallet—BenefitPay—saw a 785% increase in remittances through its Fawri+ online payment service.[3]

Bahrain's economic resilience amidst the COVID-19 pandemic has also contributed to its emerging status as a fintech-friendly hub. A USD$11.4 billion stimulus package helped to alleviate economic stress on businesses and individuals,[4] and a June 2021 royal decree extended many of its initiatives, with an extra USD$1.2 billion.[5] Economic development agency OCO Global ranked Bahrain's Economic Development Board (EDB) #6 in the world for its response to the health crisis, and #2 in the technology sub-index for its tech-driven initiatives to promote investment.[6] Although the pandemic and a dip in oil prices drove a 5.4% contraction in Bahrain's 2020 GDP,[7] the economy is forecast to grow by 3.1% in both 2021 and 2022.[8]

Bahrain's 2021 digital agenda focuses on eKYC, artificial intelligence, a cross-border digital currency pilot and support for fintech and digitalization. The private sector has also been spearheading ambitious initiatives to promote R&D and education in artificial intelligence.[9] As the kingdom rapidly evolves, regulators must harness digitalization in supporting financial inclusion for Bahrain's large population of migrant workers.

Financial Regulatory Authorities

The **Central Bank of Bahrain (CBB)** is the country's central bank and primary monetary authority.

Other Authorities

The **Bahrain Economic Development Board (EDB)** is a government agency that seeks to promote economic growth through investment.

The **Ministry of Justice, Islamic Affairs and Endowments** serves as the Personal Data Protection Authority per the Personal Data Protection Law (PDPL).

Policy, Laws and Regulations

Cross-Border Payment Solution, 14 May 2021

The central bank partnered with the Arab Banking Corporation (Bank ABC) and JP Morgan to trial the transfer of funds in and out of Bahrain, with the use of digital dollars. The project, which will utilize JP Morgan's blockchain platform Onyx, seeks to speed up payments and settlements and address other inefficiencies in cross-border transfers. The central bank might look towards an eventual central bank digital currency (CBDC) trial.[10]

Bahrain Supernova Fintech Challenge, April 2021

The central bank announced the Bahrain Supernova Fintech Challenge, which will give fintech startups access to the bank's digital lab to develop proofs of concept. Within the digital lab, fintechs will have access to an API sandbox, along with 330 APIs and simulated data sets from participating banks. Top themes include autonomous finance, user experience, artificial intelligence and regtech.[11] The central bank has been eager to promote fintech and innovative technologies, and its Fintech and Innovation Unit launched a fintech regulatory sandbox in June 2017.

Launch of eKYC, 30 January 2021

The central bank announced the successful launch of the national eKYC platform. According to the bank's press release, "The platform provides a national digital identity database for financial institutions to securely verify the identities of their customers, validate their information and share data digitally before providing products and services. This includes retrieval of customer data from governmental entities including the eGovernment Authority. BENEFIT has also developed the Application Programming Interface ('API') for the platform, which allows for seamless integration with financial institutions' core systems, digital channels and mobile apps. With the introduction of Open Banking in Bahrain, this also provides an opportunity for fintech companies to verify customers' identities through their online and mobile applications."[12]

Egypt

Country Overview

Ten years after the Arab Spring protests toppled governments across the Middle East and North Africa, Egypt's economy shows remarkable growth potential and resilience. The most populous country in the Arab world and Africa's second-largest economy, Egypt was one of the few emerging markets to have avoided an economic contraction in 2020. Although weaker than its 2019 performance, GDP grew by 3.6%[13] and the economy remained stable. Recent macroeconomic structural reforms and a strong policy response have in part contributed to economic resilience, and the International Monetary Fund (IMF) forecasts a strong comeback, at 2.8% for the 2020-2021 fiscal year and 5.2% for the 2021-2022 fiscal year.[14] *The Economist* ranks Egypt #4 of 50 on its "global normalcy index," which tracks large economies' return to pre-pandemic life.

Despite structural reforms and a promising economic outlook, Egypt continues to face obstacles. Unemployment is high,[15] the non-oil private sector has grown slowly,[16] political tension is rampant and poverty remains widespread. Amidst this challenging landscape, digitalization offers the state an opportunity to tap into its full growth potential by diversifying the economy, creating new jobs and strengthening the middle class. Fortunately, Egypt's digital transformation was well underway even before the onset of the COVID-19 pandemic.[17] Vision 2030, launched in 2016, seeks to achieve sustainable development goals, and includes commitments towards financial inclusion, digital transformation, a culture of entrepreneurship, knowledge-based economic growth and resilience and competitiveness of the economy.[18] In line with Vision 2030, the Ministry of Information and Communications Technology (MICT) launched the Digital Egypt strategy, which seeks to promote overall digitalization, digital jobs and skills, and innovation.

During the health crisis, digital transformation accelerated as the public and private sectors moved operations online and consumer preferences shifted. Egypt's leading digital payments platform, Fawry, saw a surge in growth,[19] and the government estimates that the ICT sector will contribute 8% to the GDP by 2024.[20] A spate of recent regulations—including the Non-Cash Payment Law and a fintech regulatory sandbox—will be instrumental in attracting new entrants and investment funds to the state's fintech ecosystem.[21] Although cash still dominates and the number of unbanked individuals remains high, this burgeoning fintech sector could promote financial inclusion, contribute to economic recovery and help the state to compete with more established digital economies like the United Arab Emirates and Saudi Arabia.

Egypt's 2021 digital agenda focuses on digital banking and financial inclusion. Regulators are especially keen to develop and adopt AI solutions and other innovative technologies, and they are looking to implement finger-vein recognition for identity verification in the national ID system.[22] In 2019, the central bank announced interest in exploring the potential development of a central bank digital currency (CBDC), but it has not issued any updates. As Egypt looks towards the future, regulators must ensure that structural reforms and digitalization initiatives are applied evenly, support a young and fast-growing population and are accompanied by adequate cybersecurity standards.

Financial Regulatory Authorities

The **Central Bank of Egypt (CBE)** is the country's central bank.

The **Egyptian Financial Supervisory Authority (EFSA)** regulates the non-banking financial markets sector.

The **Financial Regulatory Authority (FRA)** regulates Egypt's financial services sector.

The **Personal Data Protection Centre (the "Centre")** oversees and enforces compliance with the Data Protection Law.

Policy, Laws and Regulations

New Banking Law, 16 September 2021

Law 194/2020 (the "New Banking Law" or the "CBE Law"), published 15 September 2020, establishes a new regulatory framework for the payments sector, which was previously regulated only indirectly. Per the regulation, Payment System Operators (PSOs) and Payment Service Providers (PSPs) must obtain a banking license from the central bank, and are subject to audit and inspection. Regulated entities must keep all electronic records related to accounts and payment orders, which will be considered valid as evidence if stored according to central bank requirements.[23] The central bank has the authority to issue warnings and fines, freeze activities and revoke licenses. Fintech and regtech startups may be exempted from licensing requirements, with approval by the central bank. The CBE Law also prohibits entities from conducting activities with cryptocurrency, unless licensed by the central bank.[24] Regulated entities must have been in compliance by 16 September 2021. The law will be instrumental in attracting foreign direct investment (FDI) to Egypt's fintech sector, modernizing the economy and making the banking sector more competitive.

Simplified Procedures for Opening Accounts, 24 March 2021

The central bank, in partnership with the Money Laundering and Terrorist Financing Combating Unit, issued a circular to banks regarding the application of simplified procedures for account opening. In the case that data on identity documents differs from data provided on the account opening form, alternate documentation may be supplied for proof of work or address. These documents are acceptable as evidence of work: membership card, professional license, tax card, document from the General Authority for Insurance and document from the Labor Office. A utility bill or lease contract may be utilized as evidence of address. If a small business does not have a commercial register or license, it may open an account with an ownership contract. The move comes as part of Egypt's efforts to support financial inclusion.[25]

Data Protection Law, 16 October 2020

The Data Protection Law, published 15 July 2020, imposes new requirements on processors and controllers of personal data, and codifies the rights of data subjects. In order for the processing of personal data to be considered legitimate and legal, processors must obtain the data subject's consent; and the processing must be necessary for the execution of a contractual obligation, legal action, an action in support of the data subject's legal rights or the execution of an agreement to benefit the data subject. Data controllers and processors must obtain a license from the Personal Data Protection Centre, appoint a data protection officer and maintain records of processing activities. A fee of up to LE

2,000,000 (approximately USD$127,000) is required for the acquisition of a license. Cross-border transfers of personal data are prohibited unless permission is granted from the Personal Data Protection Centre, and personal data may not be sent to a jurisdiction with personal data protection standards of a lesser level than the Egyptian Data Protection Law. Data subjects have the rights to knowledge, access, withdrawal, objection, erasure and modification, and they may limit the scope of the processing and refuse or withdraw consent to electronic marketing. In the case of a data breach, controllers and processors must notify the Personal Data Protection Centre within 72 hours of being made aware, and data subjects have a right to be notified. The Law, influenced by the EU's General Data Protection Regulation (GDPR), went into effect 16 October 2020. It will not be fully enforced until 2022.[26]

Iraq

Country Overview

Decades of conflict have ravaged oil-rich Iraq, which has struggled to diversify its economy, develop the banking sector and respond to crises. In 2020, the COVID-19 pandemic and a decline in global oil demand drove a 10.4% contraction in the Iraqi economy[27] and brought the poverty rate to an estimated 30% of the population.[28] Inflation and unemployment are high, and the International Monetary Fund (IMF) predicts growth of a mere 1.1% in 2021.[29] Meanwhile, security concerns related to ISIS, tensions with Iran and political instability remain a challenge to this emerging market.

As Iraq seeks to recover in the wake of the pandemic, war and other conflict, regulators must ground economic initiatives in digital transformation. Expansions in digital infrastructure, the adoption of innovative technologies like AI and big data, and digital banking will be particularly important areas to watch. Iraq's partnership with Gulf Cooperation Council (GCC) states like Saudi Arabia, the United Arab Emirates and Kuwait could be its solution to securing the funds and other support it needs to pursue ambitious structural reforms. GCC states have already contributed to Iraqi reconstruction efforts,[30] and Iraq stands to benefit further from their wealth, stability and intense digital momentum.

Although Iraq's fintech ecosystem is in its infancy, with only fourteen fintechs in the country,[31] there is reason for optimism. Iraq relies mostly on the 3G network[32] and internet speed is slow,[33] but internet penetration is relatively high at 75%.[34] Demand for mobile and electronic payment services is rising,[35] and recent successes in the sector could pave the way for followers. In August 2020, an Iraqi company—in partnership with a Lebanese fintech and Visa—introduced the country's first digital-only payment card,[36] and the country's first fully digital bank went live in September 2021.[37] A more robust fintech ecosystem would help Iraq in diversifying and growing its economy, bolstering financial inclusion and expanding employment opportunities.

This year, Iraq has focused on digitalization in payments, overall digitalization and financial inclusion. The state has sought to adopt new biometric voter cards for its 2021 election, but the rollout of the cards has been delayed, amidst other problems.[38] As Iraq digitalizes, regulators must institute a national data protection framework, beef up cybersecurity and ensure that vulnerable communities like displaced people are not further excluded.

Financial Regulatory Authorities

The **Central Bank of Iraq (CBI)** is the country's central bank.

The **Iraqi Securities Commission (ISC)** regulates the capital market and seeks to protect investors.

Policy, Laws and Regulations

Digital Landscape Assessment, 03 August 2021

Iraq is receiving the help of the United Nations Development Programme (UNDP) and the e-Governance Academy in devising a digital landscape assessment (DLA), which will evaluate the state's digital progress and supply recommendations towards boosting digitalization. According to the UNDP's press release, "Building on the assessment upon its completion, a Public Sector Digital Transformation Roadmap is planned to be developed to establish the baseline for Iraq's digital governance, identify the strategic priorities for digital transformation in the public sector and outline the main building blocks of a digital society while tackling challenges and bottlenecks– e.g. secure data exchange, digital identity and digital signature for citizens and businesses, data security and capacity development– along with proposals for the institutional, financial and legal framework of e-Governance."[39]

Iraqi-Egyptian Digitalization Partnership, 18 June 2021

Iraqi Minister of Communications Arkan Shahab and Egyptian Minister of Communications and Information Technology Amr Talaat signed a memorandum of understanding in an effort to facilitate the exchange of information related to IT and communications. Key areas of cooperation include cybersecurity, research and development, telecom infrastructure, digitalization, legislation and regulations, technology parks, innovation, entrepreneurship, satellites and digital Arabic content. The two ministers plan to launch a joint committee to develop short-term, medium-term and long-term plans for the digitalization of Iraq.[40]

Digitalization in Payments, 19 April 2021

The central bank has partnered with Mastercard to promote cashless payments and financial inclusion in Iraq. The collaboration will initially focus its efforts on building a digital payments ecosystem for the education sector, with plans to expand into other sectors. According to Mastercard's press release, "The Mastercard partnership with CBI is a starting point that will allow for the development of a full digital ecosystem in Iraq, which will cover key pillars including the use of Public Policy and Regulation to curb the shadow economy, a wholesale modernization of the payment ecosystem, and the digitization of key value chains. Those include government collections and disbursement and peer-to-peer and consumer spending, as well as business purchases and salary payments."[41]

Israel

Country Overview

Nicknamed the “Startup Nation,” innovative and wealthy Israel is home to a well-developed and exciting fintech ecosystem. The small Middle Eastern country has the world’s most startups per capita,[42] the second-highest research and development expenditure per GDP[43] and over a dozen fintech unicorns.[44] Tech giants—Amazon, Apple, Facebook, Google, Intel, and Microsoft—have flocked to Israel in order to tap local expertise and expand R&D. A friendly regulatory environment, strong cybersecurity and economic resilience have contributed to the country’s status as a global tech leader.

Although Israel’s economy contracted by 2.4% in 2020,[45] the finance sector remained stable, and the International Monetary Fund projects a 2021 growth rate of 5%.[46] Still, the changing nature of the COVID-19 pandemic lends a measure of uncertainty to Israel’s economic growth and overall future. The state has been widely praised for its speedy vaccine rollout, but August 2021 brought another surge of infections as vaccine efficacy dwindled and restrictions eased. Political turmoil—both domestic and international—has compounded this uncertain landscape.

Despite the health crisis—and in some cases, because of it—Israel’s robust fintech ecosystem is poised for even further expansion. The COVID-19 pandemic has accelerated digital transformation, and governments, businesses and individuals worldwide have rushed to adopt and invest in Israeli digital solutions. The Israeli fintech sector brought in USD$2.3 billion in venture capital investments in the first half of 2021, a 260% increase from the first half of 2020.[47] In March 2021, Israel’s first digital bank was launched in pilot mode. Slated for a public launch in early 2022, First Digital Bank will harness innovative technologies like AI[48] to offer 24/7 remote onboarding and other services.[49] The first half of 2021 also saw the Israeli cybersecurity sector raise a record USD$3.4 billion, and seven Israeli cybersecurity companies became unicorns.[50]

This year's ambitious digital agenda focuses on central bank digital currency (CBDC), fintech, artificial intelligence and cybersecurity. As Israel continues to pursue groundbreaking initiatives, regulators must ensure that digitalization drives financial inclusion and that the digital gap does not widen. Digitalization in banking, alongside improvements to digital infrastructure, could be instrumental in providing Arab Israelis, the elderly and other vulnerable communities expanded access to financial services. Regulators must also ensure that further digital transformation dovetails with adequate data protection, as the role of digital technology in response to the pandemic has aggravated Israelis' fears over surveillance and privacy.[51]

Financial Regulatory Authorities

The **Bank of Israel** is the central bank of Israel.

The **Capital Markets, Insurance and Savings Authority** regulates non-banking financial entities.

The **Israel Securities Authority (ISA)** seeks to facilitate fairness and transparency in the capital market.

The **Privacy Protection Authority (PPA)**, housed in the Ministry of Justice, enforces the Protection of Privacy Law (PPL).

Policy, Laws and Regulations

Big Data Database, August 2021

The central bank announced a plan that will require commercial banks and credit companies to transfer certain customer data from the past five years, towards the establishment of a big data database. Analysis of the database will reportedly be utilized in strengthening the efficiency of the financial sector and facilitating decision-making on cash use, payments and communication. The bank has yet to comment on the protection of customer data and cybersecurity controls and procedures.[52]

Memorandum on Fintech Regulatory Sandbox, July 2021

The Ministry of Finance published a Memorandum of Law, which calls for the establishment of a fintech regulatory sandbox. The proposed sandbox will be headed by a committee of officials from the Bank of Israel, the Capital Markets Savings and Insurance Authority, the Israel Securities Authority, and the Anti-Money Laundering Authority. The committee will select the participant fintechs. The sandbox will last for two years, with the possibility of extension. Companies that require a license to operate will participate in the licensing track, and all others will participate in the guidance track. The Memorandum was open for public feedback until 19 July 2021.[53]

Digital Shekel Pilot, 21 June 2021

Bank of Israel Deputy Governor Andrew Abir stated at a conference that the central bank had conducted an Ethereum-based pilot test on a CBDC, but he remained skeptical that a digital shekel would ever be launched. The announcement came on the heels of a May central bank working paper addressing a potential CBDC. The working paper proposed a draft model wherein the central bank issues the CBDC, which is then distributed by payment service providers.[54]

As of June 2021, the Palestine Monetary Authority (PMA)—the emerging central bank of Palestine—has been considering the launch of its own CBDC. Palestine does not have its own currency, and instead relies on the Israeli shekel, the Jordanian dinar and the US dollar, and the introduction of a Palestinian digital currency would signal a semblance of monetary authority. The PMA is currently conducting two studies on cryptocurrencies, however, it is unlikely that a Palestinian digital currency will come to fruition. The Palestinian economy and central bank are weak and hindered by Israeli control.[55]

Request for Information on Biometric Verification in KYC, 12 April 2021

The Identity & Biometric Applications Unit of Israel's National Cyber Directorate published a Request for Information (RFI) seeking feedback from Israeli and international providers of biometric verification-based know-your-customer (KYC) technologies. The RFI sought information on document scanning and authentication, biometric verification, presentation attack detection (PAD) and other details related to fraud detection, data security tests, product performance and privacy enhancement. The deadline for replies was 14 June 2021. The move comes as the Israeli government seeks to establish onboarding and authentication processes in the access to online government services.[56]

Draft Bill on Cyber Defense and the National Cyber Directorate, 04 March 2021

The Israeli government published an updated draft bill on *Cyber Defense and the National Cyber Directorate*, which authorizes the National Cyber Directorate (NCD) to direct certain organizations in strengthening cybersecurity. An organization must be engaged in essential activities and have a critical weakness in its cybersecurity, such that a cyberattack against the organization would endanger public interest. The updated bill requires the NCD to confer with an organization and allow it to independently address weaknesses in its cybersecurity before the agency takes action. The NCD may then obtain a court order allowing it to instruct an organization in improving its computer systems.[57]

Advance Ruling Paper on Cryptocurrency, 21 December 2020

The Israeli Securities Authority issued an advance ruling paper in response to a request by Kirobo Ltd., a blockchain company. The advance ruling paper deemed that cryptocurrency is a security, subject to the Israeli Securities Law, and not a utility token. The regulator also added that the definition of a security must be interpreted broadly, in order to protect cryptocurrency investors.[58]

National Artificial Intelligence Program, December 2020

A committee headed by AI expert Dr. Orna Berry developed a national artificial intelligence program, which calls for the allocation of NIS 5.26 billion (approximately USD$1.6 billion) towards the development and adoption of AI over a five-year span. The program will unfurl in stages. The first stage, approved in April 2021, allocates NIS 550 million (approximately USD$170 million) towards several initiatives, including the establishment of a High Performance Computing (HPC) supercomputer, bolstering human capital, developing a friendlier regulatory environment and providing support for R&D in neuro-linguistic programming (NLP). In investing in NLP, the program seeks to expand computers' ability to understand both Hebrew and Arabic. Said Dr. Berry, "Our goal is to develop artificial intelligence to the level of a national forte, but it won't be just an academic issue. We want to bring about a change in the uses of AI, which will lead to increased labor productivity, contribute to economic growth and improve the quality of services to the public."

The program will be spearheaded by Telem, the National Infrastructure Forum for Research and Development. Telem is currently searching for a director of the program, who will be housed under the Innovation Authority and report to a steering committee.[59]

Kingdom of Saudi Arabia

Country Overview

The ambitious and wealthy Kingdom of Saudi Arabia, home to the largest economy in the Arab world, is poised to become a regional fintech hotspot as it emerges from the COVID-19 pandemic. Although the health crisis and a decline in oil prices drove a 4.1% shrinkage in the Saudi economy in 2020,[60] GDP is forecasted to expand by 2.4% in 2021.[61] The Kingdom has enforced strict vaccination rules amidst the rise of the Delta variant,[62] and the economy is expected to return to pre-pandemic levels by mid-2022.[63] As the Gulf state recovers, regulators are keen to continue efforts to diversify the economy, digitalize the financial sector[64] and become a global leader in the development of innovative technologies.

Vision 2030, a national strategy launched by Crown Prince Mohammad bin Salman in 2016, aims to reduce Saudi dependence on oil and foster a modern, vibrant economy. Accelerated digitalization—spurred on by the pandemic—will be instrumental in achieving its fintech-heavy goals and helping the Kingdom to compete with innovation powerhouses like the United Arab Emirates. In 2020, digital payments soared by 75%[65] and e-commerce rose by 74% between March and April.[66] The fintech sector is raking in venture capital investments, and even big tech has flocked to the Kingdom, with Google set to open a cloud region there.[67] Sophisticated 5G technology,[68] strong cybersecurity and a friendly regulatory environment[69] have especially made the Kingdom an attractive choice for fintech startups. The Global Cybersecurity Index 2020, developed by the United Nations' International Telecommunication Union, ranks Saudi Arabia #2 in the world.

This year, Saudi Arabia's digital agenda focuses on cybersecurity, open banking, data protection, instant payments, a digital identity project, the digitalization of government services and the development of innovative technologies like big data and artificial intelligence. In 2020, the central bank spearheaded numerous blockchain-based experiments, including a cross-border digital currency pilot with the United Arab Emirates. The National Information Center (NIC), part of the Saudi Ministry of Interior, is planning to institute iris recognition for the identification of travelers at all air, land and sea borders.[70] As the Kingdom increasingly pursues sustainability and other green initiatives, it will have even more impetus to develop and implement groundbreaking technologies.[71] Alongside this rapid digitalization, however, regulators must look towards adopting data protection and privacy standards, as the Kingdom does not have a national data protection framework.

Financial Regulatory Authorities

The **Saudi Central Bank (SAMA)** is the Central Bank of the Kingdom of Saudi Arabia.

The **Capital Market Authority (CMA)** is Saudi Arabia's financial regulatory authority governing capital markets in the country.

Other Regulatory Authorities

The **Communications and Information Technology Commission (CITC)** is Saudi Arabia's communications authority, and seeks to ensure competitiveness and fairness in the market.

The **Saudi Data and Artificial Intelligence Authority (SDAIA)** sets the national data and artificial intelligence agenda.

Policy, Laws and Regulations

Digital Government Framework, 01 August 2021

The board of directors of the Digital Government Authority (DGA) announced the body's first draft regulatory framework for a digital government. The DGA was established 11 March 2021 to lead the digitalization of government services, a key goal of Vision 2030. The framework hinges on eight principles, including "Digital by Design" and "Mobile First," alongside a five-pronged e-government policy. As part of the "Whole of Government as Platforms Policy," the DGA seeks to support government agencies in digitalization efforts through resources, data and tools. In a move to promote citizen participation in the implementation of the framework per the "Beneficiary-Centric Policy," the DGA will continuously issue surveys and public consultations.[72] The draft regulatory framework was open for comments until 14 August 2021.

Cybersecurity Regulatory Framework, 29 May 2021

The Communications and Information Technology Commission (CITC) announced the launch of a cybersecurity regulatory framework for service providers in communications, information technology and postal services. The framework includes cybersecurity requirements and controls, as well as a risk management methodology.

The Kingdom has been aggressive in strengthening cybersecurity and digital literacy. In August 2021, the Saudi Federation for Cyber Security, Programming and Drones (SAFCSP) announced a USD$1.2 billion spate of initiatives to bolster the digital skills of 100,000 young Saudis by 2030.[73] The Global Cybersecurity Index 2020 noted that Saudi Arabia, ranked #1 in the region and #2 in the world, is strong in its legal, organizational and cooperative measures, alongside capacity development. Between January and March 2021, over 7 million cyberattacks were deterred in Saudi Arabia.[74]

Saudi Payments Adopts Instant Payments, 21 April 2021

Saudi Payments, a major payment system established by the central bank, announced the introduction of its instant payments system "sarie." Sarie allows customers to make real-time transactions of up to SAR 20,000 (approximately USD$5,333) and quick transfer services of up to SAR 2,500 (approximately USD$666) through the use of a mobile number, email address or IBAN number.[75] The system, launched in collaboration with IBM and Mastercard, will be key in achieving Vision 2030's goal of 70% cashless transactions by 2030.

Digital Identity Project, 24 March 2021

The Ministry of Interior, in partnership with the Saudi Data and Artificial Intelligence Authority (SDAIA), introduced a national digital identity on the Tawakkalna application. The app, launched in May 2020 as part of efforts to combat the COVID-19 pandemic, now provides a national digital identity for Saudi citizens, as well as a resident identity for non-citizens in the Kingdom. The digital identity can be utilized to access certain government services,[76] which aligns with Vision 2030's aim of digitalizing government and creating a seamless experience for users.

Open Banking Policy, January 2021

The central bank issued its brief Open Banking Policy, which aims to promote competition, innovation, financial inclusion and efficiency in the banking system. The central bank is currently assessing the potential impacts of open banking, and how best to adopt it in the Kingdom. The launch of open banking will occur over three phases: design, implementation and go-live. According to the central bank's policy document, "The implementation phase will cover the development of the defined frameworks, technology building blocks and rollout activities including testing with financial market participants, and enhancement of customer awareness."[77] The central bank plans to go live in the first half of 2022.

Cross-Border Central Bank Digital Currency Pilot, 29 November 2020

The central banks of Saudi Arabia and the United Arab Emirates successfully completed a cross-border central bank digital currency (CBDC) pilot, called Project Aber. The experiment utilized distributed ledger technology (DLT) to facilitate cross-border payments between the two countries, with a dual-issued digital currency. Three use cases were tested: payment between central banks, domestic payments between commercial banks and cross-border payments between commercial banks. The report notes that its distributed payment system is a "significant improvement over centralized payment systems in terms of architectural resilience."

National Strategy for Data and Artificial Intelligence, 21 October 2020

The Saudi Data and Artificial Intelligence Authority (SDAIA) launched the National Strategy for Data and Artificial Intelligence (NSDAI), which aims to invest USD$20 billion in AI and train 2,000 data and AI specialists over a ten-year period.[78] Speaking at a G20 media briefing, head of SDAIA Abdullah al-Ghamdi stated, "We aspire to have artificial intelligence as a component of an alternative economy through startups and innovation companies..."[79]

Libya

Country Overview

Libya has been devastated by the COVID-19 pandemic, the presence of ISIS, an ongoing humanitarian crisis and a long and brutal civil war. The Second Libyan Civil War officially ended in October 2020, and a provisional government established in March 2021, but sporadic violence amongst mercenary forces continues. Poverty and inflation rates are high, and Libyans lack access to basic needs such as food, water and healthcare. A mere 1.8% of the population has been vaccinated against the COVID-19 disease,[80] and already-weak health infrastructure has been further strained. The economy plunged by 31.3% in 2020, and although the World Bank predicts a possible comeback of 67% in 2021,[81] this will not provide Libya the structural reforms and aid it desperately needs.

As Libyan regulators, the private sector and international organizations seek to rebuild the North African country, initiatives must be grounded in digital transformation. Digital transformation will be critical in diversifying Libya's oil-reliant economy, rebuilding in the wake of war and making progress towards the achievement of sustainable development goals. Although Libya's fintech ecosystem is only just emerging, innovation in payments could bolster financial inclusion, especially for vulnerable groups like women, the elderly and displaced people. Cryptocurrency investment is popular in Libya, as in other fragile and conflict-affected states.[82]

This year, Libyan regulators are focused on forging international connections in support of digital transformation, AML/CTF and a biometric ID system. As Libya digitalizes, regulators must bolster national cybersecurity, as cyberattacks and hacking were used in the civil war to leak secret documents and spread misinformation.[83] Strong partnerships between the public and private sectors will also be key in boosting digitalization, especially as private companies forge connections with foreign governments. In June 2021, chairman of the Libyan Telecoms Holding Company Faisal Ahmed Qarqab met with Egyptian Minister of Communications and Information Technology (ICT) Amr Talaat to establish a joint working team aimed at developing the Libyan telecom and ICT sector. The joint working team will spearhead projects related to digital transformation, digital infrastructure, digital skills and education, capacity building and the sector's legal framework.[84] Internet penetration has been steadily increasing since 2021, but still stood at a mere 21.76% in 2017.[85]

Financial Regulatory Authorities

The **Central Bank of Libya** is Libya's central bank and primary monetary authority.

The **Libyan Capital Market Authority** regulates and supervises the financial markets and non-banking financial instruments.

The **National Authority for Information Security and Safety** is Libya's data protection authority.

Policy, Laws and Regulations

Meeting on Anti-Money Laundering and Counter-Terrorist Financing, 22 August 2021

The European Union Border Assistance Mission in Libya (EUBAM) had a meeting with the Libyan Ministry of Interior's Department for Combating Financial Crime to discuss improvements to the ministry's anti-money laundering and counter-terrorist financing investigation techniques. Information exchange and data protection were also addressed.[86]

Libyan-British Cooperation in Cybersecurity, August 2021

Chairman of the Libyan Post Telecommunications and Information Technology Company (LPTIC) Faisal Gurgab met with British Ambassador to Libya Nicholas Hopton to discuss cooperation in cybersecurity, communications and technology. Libya hopes to benefit from British cybersecurity technologies and promote opportunities for British development and investment, alongside a return of British IT and communications companies to the country.[87]

Qatar

Country Overview

Wealthy and ambitious Qatar is undergoing rapid digital transformation, which will be instrumental in helping the state to diversify its economy, compete with other Gulf Cooperation Council (GCC) countries and recover from the COVID-19 pandemic. The Qatari economy contracted by 3.7% amidst the pandemic and a decline in global oil demand,[88] but it is expected to have a strong comeback. The World Bank predicts growth rates of 3% in 2021 and 4.1% in 2022, due in part to business environment reforms, stabilized demand for natural gas and the 2022 FIFA World Cup.[89] In early 2021, Qatar restored diplomatic relations with Bahrain, Egypt, Saudi Arabia and the United Arab Emirates, another positive step towards further economic growth and regional integration.

Qatar's burgeoning fintech sector will be an especially important driver of economic growth, and it will help the state in achieving development goals set out in its National Vision 2030. The central bank has been keen to partner with the private sector in implementing digital payments initiatives, and the government has launched numerous national strategies aimed at promoting digital transformation, innovation and financial inclusion. CEO of Doha Bank Raghavan Seetharaman estimates that venture capital investments in Qatari fintech startups rose 180% in the first half of 2021.[90] By 2023, the state's digital spending could skyrocket to USD$3.2 billion.[91]

This year, Qatari regulators are focused on anti-money laundering and counter-terrorist financing, artificial intelligence and financial inclusion. The central bank plans to launch a fintech regulatory sandbox sometime in 2021. A key challenge will be ensuring that migrant workers are financially and digitally included. Qatar has the world's highest ratio of citizens to migrants, who make up 95% of the state's workforce.[92] Digitalization in the payments sector will be especially key in making remittances cheaper and faster. Regulators must also strengthen national cybersecurity, as digitalization and the pandemic have driven a global rise in the frequency and sophistication of cyberattacks. According to IBM's 2021 *Cost of a Data Breach Report*, the Middle East had the world's second-most expensive data breaches, at USD$6.93 million per incident.[93]

Financial Regulatory Authorities

The **Qatar Central Bank** is the country's central bank.

The **Qatar Financial Markets Authority (QFMA)** regulates and supervises the financial markets.

Other Regulatory Authorities

The **Ministry of Transport and Communications (MoTC)** oversees compliance with the Qatari Personal Data Protection Law.

Policy, Laws and Regulations

Artificial Intelligence Committee, 07 March 2021

Qatar's Cabinet approved a draft decision to establish the Artificial Intelligence Committee, to be housed under the Ministry of Transport and Communications (MoTC). The three-person committee will be tasked with implementing the country's 2019 National Artificial Intelligence Strategy, which aims to secure Qatar's status as a global AI hub. Key responsibilities will include support for startups working in AI and the development of plans and programs for boosting digital skills in the area of AI.[94]

Anti-Money Laundering and Counter-Terrorist Financing Assessment, February 2021

The Qatar Financial Markets Authority (QFMA), in partnership with the Chartered Institute for Securities & Investment (CISI), has launched a national anti-money laundering and counter-terrorist financing (AML/CTF) digital assessment tool. Obliged entities can access the tool, available in both Arabic and English, on laptops and mobile phones. The tool assesses knowledge of AML/CFT requirements, and reports results to the QFMA in a move to bolster compliance.[95]

Personal Data Protection Law Regulatory Guidelines, November 2020

The Compliance and Data Protection Department (CDP) of the Ministry of Transport and Communications (MoTC) released guidelines on the Data Protection Law. The fourteen guidelines, many of which are influenced by the EU's General Data Protection Regulation (GDPR), clarify requirements and introduce new ones. Data controllers must keep a Record of Processing Activities (ROPA); a Data Privacy Impact Assessments (DIPA) must be conducted before new processing activities are begun; and authorization from the CDP must be obtained before the processing of "special nature" personal data, including data pertaining to health, children, religion and criminal convictions. Obliged entities must institute a Personal Data Management System (PDMS) to help in data management and the reporting of violations; send data breach notifications to the CDP and relevant data subjects within 72 hours; obtain explicit consent for direct marketing communications; facilitate data subjects' ability to exercise their rights; and in the case that processing is contracted to a third party, conduct due diligence on the third party processor. Privacy controls must inform processing activities and business practices. Violations could incur fines up to QAR 5,000,000 (approximately USD$1,373,600).[96]

The United Arab Emirates

Country Overview

The wealthy and innovative United Arab Emirates (UAE) is the region's #1 fintech hotspot, and Dubai in particular is poised to compete with global digital hubs like Berlin, London and Singapore.[97] The World Economic Forum's *Global Competitiveness Report 2020* ranks the UAE top ten in the world for its information and communications technology (ICT) adoption and digital legal framework, and strong cybersecurity has helped to cement its fintech-friendly status. The UAE ranked #5 in the world on the Global Cybersecurity Index 2020, developed by the United Nations' International Telecommunication Union.

Although the COVID-19 pandemic drove a 6.1% contraction in the Emirati economy in 2020,[98] which could potentially stall progress and allow for regional competitors like Saudi Arabia to gain ground, the future of the UAE's digital economy is promising. Digitalization continues at breakneck speed and regulators are ambitious and venture capital funds are pouring in. The Emirati banking sector has remained strong amidst the health crisis,[99] and the International Monetary Fund (IMF) predicts a 2021 GDP growth rate of 3.1%.[100]

As the UAE emerges from the COVID-19 pandemic, it plans to revamp its economy by tapping into innovative technologies like digital currency, blockchain, artificial intelligence and big data. The UAE already ranks #1 in the Arab world, and #34 in the world, for innovation in the economy, per the Global Innovation Index (GII) 2020, developed by Cornell University, INSEAD and the World Intellectual Property Organization (WIPO).

This year, the UAE is focused on central bank digital currency (CBDC), a licensing regime for providers of cryptoassets, AML/CFT, data protection in Abu Dhabi and a Dubai-based innovation hub. As the state digitalizes, regulators have an opportunity to support financial inclusion, especially amongst non-Emirati residents. The UAE is the globe's second-largest sender of remittances,[101] and its high number of migrant workers would benefit from cheaper and more accessible payment systems.

Financial Regulatory Authorities

The **Central Bank of the United Arab Emirates (UAECB)** is the primary monetary authority governing all financial institutions operating in the country that don't fall within the financial free zones, the geographic economic centers that develop and enforce their own regulations and laws.

The **Abu Dhabi Global Market (ADGM) Office of Data Protection (ODP)** is the primary data authority for the ADGM financial free zone.

The **ADGM Financial Services Regulatory Authority (FSRA)** seeks to ensure a fair, stable and robust financial services sector in the ADGM financial free zone.

The **Dubai Financial Services Authority (DFSA)** regulates the financial services sector in the Dubai International Financial Centre (DIFC) financial free zone.

The **Securities and Commodities Authority (SCA)** regulates and oversees the UAE's financial markets.

Laws, Policy and Regulations

Biometric Verification System, August 2021

The UAE's Ministry of the Interior partnered with the Abu Dhabi Islamic Bank (ADIB) to launch a biometric identity verification-based onboarding system. Users wishing to open a new account with the ADIB can submit a selfie through the bank's mobile app, and the selfie is then verified with facial recognition technology and biometric matching through the Ministry of the Interior's Facial Recognition database. Users must also tap their Emirates ID card to their mobile phones during the onboarding process to facilitate the retrieval of data from the chip.[102]

The Emirati government has shown increasing interest in supporting the use of biometric identification to access services. In April 2021, the UAE enabled a capability that allows residents to connect their faces with their UAE Pass digital IDs. Residents can now access online government services through facial recognition.[103]

2023-2026 Strategy, 12 July 2021

The central bank launched its 2023-2036 Strategy, which seeks to secure the UAECB's status as one of the top ten central banks in the world and promote digital transformation in the financial sector. Major plans include the development of a central bank digital currency and a digital identity system, as well as to further harness the power of innovative technologies like artificial intelligence and big data. The strategy also aims to promote green initiatives in the economy and strengthen financial inclusion.

Dubai International Financial Centre Innovation Hub, 25 May 2021

The Dubai International Financial Centre (DIFC) Innovation Hub was inaugurated by Deputy Ruler of Dubai and President of the DIFC Sheikh Maktoum. The Innovation Hub seeks to bring together startups, tech unicorns and big tech to cultivate Dubai's fintech ecosystem. Startups will receive financial support from the DIFC FinTech Hive's accelerator program and the USD$100 million FinTech Fund. DIFC Governor Essa Kazim stated, "With a strong focus on promoting promising startups and innovative ventures, DIFC is accelerating the strategic and sustainable development of the economy to be future-ready. The DIFC Innovation Hub is the region's dedicated zone for innovators and investors to leverage the extraordinary potential of new generation technology."[104]

Anti-Money Laundering and Countering the Financing of Terrorism Office, 24 February 2021

The UAE Cabinet approved the creation of the Executive Office of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), which will implement the National AML/CFT Strategy and National Action Plan (NAP). Towards this end, the Executive Office seeks to strengthen national and international cooperation; collaborate with the Gulf Cooperation Council (GCC), Working Group on AML-CFT, G20 and the Financial Action Task Force (FATF); bolster information sharing between sectors; support legislative initiatives to strengthen the national AML/CFT framework; and coordinate with the Ministry of Foreign Affairs and International Cooperation (MOFAIC) in communicating progress to the Higher Committee on AML/CFT.[105]

On 13 April 2021, the National Committee for Combating Money Laundering and Financing of Terrorism and Illegal Organisations (NAMLCFTC) adopted AML/CFT guidelines for financial institutions and designated non-financial businesses and professions. The guidelines seek to raise awareness on adherence to AML/CFT regulations, as well as risks and penalties for non-compliance.

Multiple Central Bank Digital Currency Bridge Project, 23 February 2021

A joint statement announced the addition of the Central Bank of the United Arab Emirates and the Digital Currency Institute of the People's Bank of China to the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project, spearheaded by the Hong Kong Monetary Authority and the Bank of Thailand. The project, supported by the Bank for International Settlements (BIS) Innovation Hub, explores the use of a CBDC and distributed ledger technology (DLT) in instantaneous cross-border payments, and investigates scalability, interoperability, privacy and governance. It aims to simplify cross-border fund transfers by lowering costs, reducing inefficiencies and easing the burden of complicated regulatory compliance.

Abu Dhabi Global Market Data Protection Regulations, 11 February 2021

The ADGM issued new data protection regulations, modeled on the EU's General Data Protection Regulation (GDPR), which expand data subjects' rights and impose new obligations on data processors and controllers. The regulations apply to processors and controllers of data in the ADGM, even if the processing of data occurs outside the ADGM. Data subjects have the rights to erasure, access, rectification, portability and the right to object. The regulations established a new Office of Data Protection (ODP), a data breach notification system, requirements for record-keeping, requirements for data security and more severe non-compliance penalties. Violators may face fines of up to USD$28 million. Businesses may be required to appoint a data protection officer in some scenarios. International transfers of data may occur if the receiving entity or jurisdiction adheres to an adequate standard of data protection. Businesses established after 14 February 2021 had until 14 August 2021 to comply with the new regulations, and businesses established before 14 February 2021 have until 14 February 2022 to comply with them. Until the end of the transitional period, the preexisting data protection regulations will still be in effect.

Regulation on the Licensing of Cryptoassets, 01 December 2020

The SCA's decision The Authority's Chairman of the Board of Directors Decision No. (21/R.M) of 2020 Concerning the Regulation of Crypto Assets, published 01 November 2020 in the official gazette, has gone into effect. The law details a licensing regime for entities seeking to offer services involving cryptoassets, including exchanges, marketplaces, custodian services and crowdfunding platforms. Entities must be incorporated onshore either in the UAE or one of its financial free zones, and they must be licensed by the SCA prior to offering services involving cryptoassets. In order to obtain a license, entities must demonstrate compliance with UAE regulations on cybersecurity, data protection, anti-money laundering and counter-terrorist financing. Computer systems must be kept onshore. In the case that licensees rely on third-party contractors, entities will assume all legal liability for breaches to the Decision. The Decision also created a classification of customers to whom cryptoassets may be offered: Qualified Investors and those who do not meet the definition of Qualified Investor. Licensees must seek prior approval from the SCA before offering cryptoassets to a non-Qualified Investor, and licensees must file documents with the SCA before offering cryptoassets to a Qualified Investor. In conducting due diligence, licensees must consider all customers as “high risk.” The SCA reserves the authority to monitor transactions, audit licensees, impose fines, publish names of violators and withdraw licensees’ rights.[106]

Cross-Border Central Bank Digital Currency Pilot, 29 November 2020

The central banks of Saudi Arabia and the United Arab Emirates successfully completed a cross-border central bank digital currency (CBDC) pilot, called Project Aber. The experiment utilized DLT to facilitate cross-border payments between the two countries, with a dual-issued digital currency. Three use cases were tested: payment between central banks, domestic payments between commercial banks and cross-border payments between commercial banks.

ENDNOTES

1 “Bahrain.” WorldData. https://www.worlddata.info/asia/bahrain/index.php.

2 “The Global Fintech Ecosystem Report 2020.” Startup Genome, 24 November 2020. https://startupgenome.com/reports/global-fintech-ecosystem-report-2020.

3 Faridi, Omar. “Cashless Transactions Increase to $3.62B in Bahrain During H1 2021: Report.” Crowdfund Insider, 13 September 2021. https://www.crowdfundinsider.com/2021/09/180243-cashless-transactions-increase-to-3-62b-in-bahrain-during-h1-2021-report/.

4 “Bahrain Coronavirus Updates.” Economic Development Board Bahrain. https://www.bahrainedb.com/key-updates-on-covid-19/.

5 “Bahrain unveils $1.2bn stimulus package for Covid-hit sectors.” Trade Arabia, 15 June 2021. http://www.tradearabia.com/news/IND_383545.html.

6 “Bahrain EDB recognised globally for its resilience in navigating the pandemic.” Bahrain News Agency, 14 July 2021. https://www.bna.bh/en/news?cms=q8FmFJgiscL2fwIzON1%2BDrxuF42WsvZ8vX2vV0B9u08%3D.

7 “Kingdom of Bahrain.” International Monetary Fund, April 2021. https://www.imf.org/en/Countries/BHR.

8 Abu Omar, Abeer. “Bahrain’s Economy Set to Grow 3.1% This Year And Next.” Bloomberg, 04 July 2021. https://www.bloomberg.com/news/articles/2021-07-04/bahrain-s-economy-set-to-grow-3-1-this-year-and-next.

9 “Deal signed in Bahrain to boost research and development in AI.” ZAWYA, 15 September 2021. https://www.zawya.com/mena/en/business/story/Deal_signed_in_Bahrain_to_boost_research_and_development_in_AI-SNG_243216635/.

10 “Central Bank of Bahrain taps JPMorgan Onyx for digital currency trials.” Finextra, 14 May 2021.

11 “Bahrain Launches Fintech Innovation Challenge: The Bahrain Supernova.” The Fintech Times, 01 May 2021. https://thefintechtimes.com/bahrain-launches-fintech-innovation-challenge-supernova/.

12 “CBB announces launch of eKYC as part of digital transformation strategy.” Central Bank of Bahrain, 30 January 2021. https://www.cbb.gov.bh/media-center/cbb-announces-launch-of-ekyc-as-part-of-digital-transformation-strategy/.

13 “Egypt Economic Outlook.” African Development Bank Group. https://www.afdb.org/en/countries/north-africa/egypt/egypt-economic-outlook.

14 “Egypt: Overcoming the COVID Shock and Maintaining Growth.” International Monetary Fund, 14 July 2021. https://www.imf.org/en/News/Articles/2021/07/14/na070621-egypt-overcoming-the-covid-shock-and-maintaining-growth.

15 “Unemployment, total (% of total labor force) (modeled ILO estimate) - Egypt, Arab Rep.” The World Bank, 15 June 2021. https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS?locations=EG.

16 Böwer, Uwe. “Making Egypt’s Post-COVID Growth Path More Sustainable.” European Commission, May 2021. https://ec.europa.eu/info/sites/default/files/economy-finance/eb066_en.pdf.

17 “Video: How is Egypt enhancing its digital transformation agenda?” Oxford Business Group, 28 April 2021. https://oxfordbusinessgroup.com/news/video-how-egypt-enhancing-its-digital-transformation-agenda.

18 “Egypt’s Vision 2030.” Ministry of Planning and Economic Development. https://mped.gov.eg/EgyptVision?lang=en.

19 Faridi, Omar. “Egyptian Digital Payments Provider, Fawry, Experiences Record Growth Following COVID-19 Outbreak.” Crowdfund Insider, 10 September 2020. https://www.crowdfundinsider.com/2020/09/166569-egyptian-digital-payments-provider-fawry-experiences-record-growth-following-covid-19-outbreak/.

20 Ghoneim, Dr. Abdel Wahab. “Egypt Digitalization In Alignment with Egypt vision 2030 for SDGS.” Egyptian Cabinet: Information and Decision Support Center, 03 May 2021. https://idsc.gov.eg/Upload/DocumentLibrary/Attachment_A/4798/3%20-%20EGYPT%20DIGITALIZATION.pdf.

21 Werr, Patrick. “Egypt eyes surge in fintech investment after new laws.” Reuters, 22 June 2021. https://www.reuters.com/business/egypt-eyes-surge-fintech-investment-after-new-laws-2021-06-22/.

22 Dawood, Ayub. “Egypt to unlock futuristic ID verification with finger-vein recognition tech.” Mashable, February 2021. https://me.mashable.com/tech/12805/egypt-to-unlock-futuristic-id-verification-with-finger-vein-recognition-tech.

23 Youssef, Lamiaa. “Egypt’s New Banking Law Payments Fintech Electronic Evidence.” Sharkawy & Sarhan, 06 October 2020. https://www.sharkawylaw.com/egypts-new-banking-law-payments-fintech-electronic-evidence/.

24 Bälz, Kilian and Hussam Mujally. “Client Alert: The New Egyptian Central Bank Law - A Step Towards a Cashless Economy.” Lexology, 08 December 2020. https://www.lexology.com/library/detail.aspx?g=fe521813-1f32-4caf-a04e-3c162c8397a2.

25 Mounir, Houssam. “Central Bank of Egypt directs for simplified bank account opening procedures.” Daily News Egypt, 25 March 2021. https://dailynewsegypt.com/2021/03/25/central-bank-of-egypt-directs-for-simplified-bank-account-opening-procedures/.

26 “Egypt’s Data Protection Law enters into force.” Clyde & Co, 19 October 2020. https://www.clydeco.com/en/insights/2020/10/egypt-s-data-protection-law-enters-into-force.

27 “Iraq’s Economic Update — April 2021.” The World Bank, 02 April 2021. https://www.worldbank.org/en/country/iraq/publication/economic-update-april-2021.

28 Fordham, Alice. “In Iraq’s ‘Dire’ Economy, Poverty Is Rising — And So Are Fears Of Instability.” NPR, 03 February 2021. https://www.npr.org/2021/02/03/961149079/in-iraqs-dire-economy-poverty-is-rising-and-so-are-fears-of-instability?t=1631116345397.

29 “Iraq.” International Monetary Fund. https://www.imf.org/en/Countries/IRQ.

30 “The GCC can strengthen Iraq.” The National News, 01 February 2021. https://www.thenationalnews.com/opinion/editorial/the-gcc-can-strengthen-iraq-1.1158370.

31 “FinTech Startups in Iraq.” Tracxn, 05 September 2021. https://tracxn.com/explore/FinTech-Startups-in-Iraq.

32 Blaubach, Thomas. “The 5G divide in the Middle East: Further disparity between the Gulf and its neighbors.” Middle East Institute, 20 May 2021. https://www.mei.edu/publications/5g-divide-middle-east-further-disparity-between-gulf-and-its-neighbors.

33 “Iraq’s Mobile and Fixed Broadband Internet Speeds.” Speedtest, July 2021. https://www.speedtest.net/global-index/iraq.

34 Kemp, Simon. "Digital Iraq: 2021." DataReportal, 11 February 2021. https://datareportal.com/reports/digital-2021-iraq.

35 Lewis, Sharon. "The Ultimate Snapshot of Fintech in 10 Arab Countries." Fintech News, 08 August 2021. https://fintechnews.ae/9479/fintech/fintech-in-arab-countries/.

36 "IRAQ-BORN FINTECH COMPANY INC LAUNCHES COUNTRY'S FIRST DIGITAL PAYMENT CARD 'NEO'." Startup Scene, 31 August 2020. https://thestartupscene.me/INVESTMENTS/Iraq-born-Fintech-Company-INC-Launches-Country-s-First-Digital-Payment-Card-Ne.

37 "First Iraqi Bank goes live on ICS BANKS Digital Banking solution from ICSFS." IBS Intelligence, 06 September 2021. https://ibsintelligence.com/ibsi-news/first-iraqi-bank-goes-live-on-ics-banks-digital-banking-solution-from-icsfs/.

38 Hersey, Frank. "Biometric card delays 'exclude millions' from Iraq elections." Biometric Update, 30 June 2021. https://www.biometricupdate.com/202106/biometric-card-delays-exclude-millions-from-iraq-elections.

39 "Innovation first: new initiative by UNDP digitalizes Iraq's public sector." United Nations Development Programme in the Arab States, 03 August 2021. https://www.arabstates.undp.org/content/rbas/en/home/presscenter/articles/2021/innovation-first--new-initiative-by-undp-digitalizes-iraqs-publi.html.

40 "Egypt to help Iraq implement digital transformation and govt service automation projects." Ecofin Agency, 23 June 2021. https://www.ecofinagency.com/telecom/2306-42774-egypt-to-help-iraq-implement-digital-transformation-and-govt-service-automation-projects.

41 "Mastercard Enters into Strategic Partnership with Central Bank of Iraq to Advance Digital Payments in the Country." Mastercard, 19 April 2021. https://newsroom.mastercard.com/mea/press-releases/mastercard-enters-into-strategic-partnership-with-central-bank-of-iraq-to-advance-digital-payments-in-the-country/.

42 Santosdlaz, Richie. "In Focus With Fintech and Israel's Fintech-Aviv." The Fintech Times, 24 April 2021. https://thefintechtimes.com/in-focus-with-fintech-and-israels-fintech-aviv/.

43 "Leading countries by research and development (R&D) expenditure as share of gross domestic product (GDP) worldwide in 2021." Statista, February 2021. https://www.statista.com/statistics/732269/worldwide-research-and-development-share-of-gdp-top-countries/.

44 Levanon, Adi. "Israel's maturing fintech ecosystem may soon create global disruptors." TechCrunch, 26 August 2021. https://techcrunch.com/2021/08/26/israels-maturing-fintech-ecosystem-may-soon-create-global-disruptors/.

45 Scheer, Steven. "Israeli economy dips 2.4% in 2020, but COVID hit less than in OECD." Reuters, 16 February 2021. https://www.reuters.com/article/us-israel-economy-gdp-idUSKBN2AG14I.

46 "Israel." International Monetary Fund, April 2021. https://www.imf.org/en/Countries/ISR.

47 Farber-Ball, Daniel. "Israeli Fintech companies raise $2.3 billion in the first half of 2021." CTech, 26 July 2021. https://www.calcalistech.com/ctech/articles/0,7340,L-3913298,00.html.

48 Rochvarger, Michael. "Israel's First Digital Bank Begins Operations, Heralding 'Artificial Intelligence Revolution'." Haaretz, 15 March 2021.

https://www.haaretz.com/israel-news/tech-news/.premium-israel-s-first-digital-bank-begins-operations-heralding-ai-revolution-1.9619382.

49 "Israel's First Digital Bank to offer full digital banking services to US citizens." CTech, 15 July 2021. https://www.calcalistech.com/ctech/articles/0,7340,L-3912540,00.html.

50 Solomon, Shoshanna. "Israel cybersecurity firms raise record $3.4b, 41% of global sector investment." The Times of Israel, 01 July 2021. https://www.timesofisrael.com/israel-cybersecurity-firms-raise-record-3-4b-41-of-global-sector-investment/.

51 Keshet, Yael. "Fear of panoptic surveillance: using digital technology to control the COVID-19 epidemic." Israel Journal of Health Policy Research, 25 November 2020. https://ijhpr.biomedcentral.com/articles/10.1186/s13584-020-00429-7.

52 Zwick, Gilad. "Bank of Israel demands customer data from banks, credit firms." Israel Hayom, 29 August 2021. https://www.israelhayom.com/2021/08/29/bank-of-israel-demands-customer-data-from-banks-credit-firms/.

53 Scharf, Amir and Ricky Brenner. "CAPITAL MARKETS | ISRAEL CONSIDERS REGULATORY SANDBOX PROGRAM FOR FINTECH." Tadmor Levy, 07 July 2021. https://tadmor.com/media-item/capital-markets-israel-considers-regulatory-sandbox-program-for-fintech/.

54 "Bank of Israel to explore digital shekel CBDC." Ledger Insights, 11 May 2021. https://www.ledgerinsights.com/bank-of-israel-digital-shekel-cbdc-central-bank-digital-currency/.

55 Cranny, Manus and Gwen Ackerman. "Palestinian Monetary Authority Eyes Digital currency Launch." Bloomberg, 25 June 2021. https://www.bloomberg.com/news/articles/2021-06-24/palestinian-monetary-authority-mulls-digital-currency-launch.

56 Burt, Chris. "Israel posts RFI for biometric KYC systems to be used in government services." Biometric Update, 19 April 2021. https://www.biometricupdate.com/202104/israel-posts-rfi-for-biometric-kyc-systems-to-be-used-in-government-services.

57 Ravia, Haim and Dotan Hammer. "Israeli Gov't Revises Draft Bill Granting Powers to the National Cyber Directorate." Lexology, 31 March 2021. https://www.lexology.com/library/detail.aspx?g=358a4226-f487-41c4-992b-e5b2a53e08d2.

58 Ravia, Haim et al. "Israel: Israeli Regulator Says Cryptocurrency Is A Security Subject To The Israeli Securities Law." Mondaq, 02 February 2021. https://www.mondaq.com/fin-tech/1031864/israeli-regulator-says-cryptocurrency-is-a-security-subject-to-the-israeli-securities-law.

59 Ziv, Amitai. "Israel Is Lagging on AI. It Will Now Invest Billions to Bridge the Gap." Haaretz, 12 April 2021. https://www.haaretz.com/israel-news/tech-news/.premium-the-ai-nation-israel-to-appoint-artificial-intelligence-czar-1.9703391.

60 Azhar, Saeed. "Saudi Arabia's economy grew 1.5% in Q2, first expansion since pandemic." Nasdaq, 09 August 2021. https://www.nasdaq.com/articles/saudi-arabias-economy-grew-1.5-in-q2-first-expansion-since-pandemic-2021-08-09.

61 "GCC Countries Back on Path to Economic Growth after Contraction Due to the Pandemic." The World Bank, 04 August 2021. https://www.worldbank.org/en/news/press-release/2021/08/03/gcc-countries-back-on-path-to-economic-growth-after-contraction-due-to-the-pandemic.

62 Nereim, Vivian. "Saudi Arabia Now Has The World's Toughest Vaccine Rules." Bloomberg, 01 September 2021. https://www.bloomberg.com/news/articles/2021-09-01/saudi-arabia-now-has-the-world-s-toughest-vaccine-rules.

63 "Forecasting Saudi Arabia's economy amid a global pandemic." The Economist, 25 June 2021. https://www.eiu.com/n/forecasting-saudi-arabias-economy-amid-a-global-pandemic/.

64 “Saudi Arabia ‘holds 10 times more fintech companies than planned.’” Arab News, 13 July 2021. https://www.arabnews.com/node/1893086/business-economy.

65 Hafiz, Talat Zaki. “Fintech is driving Saudi Arabia toward a cashless society.” Arab News, 16 August 2021. https://www.arabnews.com/node/1912256.

66 “Saudi e-commerce posts record growth of 70% in two months.” Saudi Gazette, 13 July 2020. https://saudigazette.com.sa/article/595437.

67 “Fintech firms dominate Saudi startup scene, attracting venture capitalists.” Arab News, 11 August 2021. https://www.arabnews.com/node/1908861/business-economy.

68 “Saudi Arabia is biggest 5G adopter in the Gulf, report shows.” Arab News, 20 April 2021. https://www.arabnews.com/node/1845696/business-economy.

69 Hamid, Triska and Nesma Abdel Azim. “Can Saudi Arabia become the region’s fintech frontrunner?” Wamda, 10 June 2021. https://www.wamda.com/2021/06/saudi-arabia-regions-fintech-frontrunner.

70 “Saudi Arabia to Deploy Iris Biometrics at its Borders.” Find Biometrics, 12 November 2020. https://findbiometrics.com/saudi-arabia-deploy-iris-biometrics-borders-111208/.

71 Hossain, Mohammad Raafi. “A Rising Crypto Capital: Why All Eyes Are Turning to MENA for Blockchain and Digital Asset Innovation.” Nasdaq, 30 August 2021. https://www.nasdaq.com/articles/a-rising-crypto-capital%3A-why-all-eyes-are-turning-to-mena-for-blockchain-and-digital-asset.

72 Ihab, Nada and Hussein Abdul-Enein. “Access Alert: Introducing Saudi Arabia’s E-Government Regulatory Framework.” Access Partnership, 03 August 2021. https://www.accesspartnership.com/access-alert-introducing-saudi-arabias-e-government-regulatory-framework/.

73 Bhat, Divsha. “Saudi announces $1.2bn tech initiatives, including all-new LEAP and @Hack events.” Gulf Business, 25 August 2021. https://gulfbusiness.com/saudi-announces-1-2bn-tech-initiatives-including-all-new-leap-and-hack-events/.

74 Nasrallah, Tawfiq. “Saudi Arabia: Over 7 million cyber attacks foiled in 3 months.” Gulf News, 27 March 2021. https://gulfnews.com/world/gulf/saudi/saudi-arabia-over-7-million-cyber-attacks-foiled-in-3-months-1.78142613.

75 “Saudi Payments switches on instant payment system.” Finextra, 21 April 2021. https://www.finextra.com/pressarticle/87227/saudi-payments-switches-on-instant-payment-system.

76 Krimly, Reem. “Saudi Arabia launches digital ID project on ‘Tawakkalna’ app.” Alarabiya News, 25 March 2021. https://english.alarabiya.net/News/gulf/2021/03/25/Saudi-Arabia-launches-digital-ID-project-on-Tawakkalna-app.

77 “Open Banking Policy.” Saudi Central Bank. https://www.sama.gov.sa/en-US/Documents/Open_Banking_Policy-EN.pdf.

78 “Saudis launch national artificial intelligence strategy.” Reuters, 21 October 2021. https://www.reuters.com/article/us-saudi-economy-ai-idUSKBN2761LZ.

79 “Saudi Arabia to invest $20 billion in Artificial Intelligence by 2030.” The Economic Times, 19 November 2020. https://economictimes.indiatimes.com/news/international/saudi-arabia/saudi-arabia-to-invest-20-billion-in-artificial-intelligence-by-2030/articleshow/79305307.cms?from=mdr.

80 “Coronavirus (COVID-19) Vaccinations.” Our World in Data, 14 September 2021. https://ourworldindata.org/covid-vaccinations?country=OWID_WRL.

81 “Libya’s Economic Update — April 2021.” The World Bank, 02 April 2021. https://www.worldbank.org/en/country/libya/publication/economic-update-april-2021.

82 Harrison, Polly Jean. “Research Finds Cuba, Libya and Syria Comprise Top 10 Crypto-Loving Countries.” The Fintech Times, 15 February 2021. https://thefintechtimes.com/research-finds-cuba-libya-and-syria-comprise-top-10-crypto-loving-countries/.

83 Herbert, Matt. “Libya’s war becomes a tech battleground.” Institute for Security Studies, 08 October 2019. https://issafrica.org/iss-today/libyas-war-becomes-a-tech-battleground.

84 Burkitt-Gray, Alan. “Egypt offers to help Libya to rebuild telecoms services.” Capacity Media, 23 June 2021. https://www.capacitymedia.com/articles/3828908/egypt-offers-to-help-libya-to-rebuild-telecoms-services.

85 “Individuals using the Internet (% of population) – Libya.” The World Bank. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=LY.

86 Zaptia, Sami. “EUBAM and Interior Ministry discuss money-laundering and financing terrorism.” Libya Herald, 23 August 2021. https://www.libyaherald.com/2021/08/23/eubam-and-interior-ministry-discuss-money-laundering-and-financing-terrorism/.

87 “Libyan, British officials discuss cooperation in cybersecurity technology.” The Libya Update, 29 August 2021. https://libyaupdate.com/libyan-british-officials-discuss-cooperation-in-cybersecurity-technology/.

88 “Qatar economy emerges from COVID-19 in a position of strength.” PwC, 25 July 2021. https://www.pwc.com/m1/en/media-centre/2021/qatar-economy-emerges-from-covid19-in-position-of-strength.html.

89 “Qatar.” The World Bank, 21 April 2021. https://thedocs.worldbank.org/en/doc/6853dd5c93a231b05c90c7a1fd7ac5b4-0280012021/original/14-mpo-sm21-qatar-qat-kcm4.pdf.

90 John, Deepak. “Fintech to transform digital banking in Qatar.” The Peninsula, 25 August 2021. https://thepeninsulaqatar.com/article/25/08/2021/Fintech-to-transform-digital-banking-in-Qatar.

91 “Qatar poised to reap rewards of digital transformation.” The Peninsula, 10 September 2021. https://www.thepeninsulaqatar.com/article/10/09/2021/Qatar-poised-to-reap-rewards-of-digital-transformation.

92 Zayadin, Hiba. “Migrant Workers and the Qatar World Cup.” Human Rights Watch, 02 August 2021. https://www.hrw.org/news/2021/08/02/migrant-workers-and-qatar-world-cup.

93 “IBM Report: Cost of a Data Breach Hits Record High During Pandemic.” IBM, 28 July 2021. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.

94 “Cabinet okays decision to set up Artificial Intelligence Committee.” Qatar Tribune, 04 March 2021. https://www.qatar-tribune.com/news-details/id/208649/cabinet-okays-decision-to-set-up-artificial-intelligence-committee.

95 Flinders, Karl. “Qatar regulator launches platform to monitor human understanding of financial crime.” Computer Weekly, 16 February 2021. https://www.computerweekly.com/news/252496385/Qatar-regulator-launches-platform-to-monitor-human-understanding-of-financial-crime.

96 Higham, Emma et al. “New regulatory guidelines on the Qatar Personal Data Protection Law.” Clyde & Co, 15 March 2021. https://www.clydeco.com/en/insights/2021/03/new-regulatory-guidelines-on-the-qatar-persona-1.

97 Rahal, Nabila. “Why Dubai is set to become a ‘flourishing’ fintech hub.” Arabian Business, 30 August 2021. https://www.arabianbusiness.com/startup/467776-why-dubai-is-set-to-become-flourishing-fintech-hub.

98 “UAE economy shrank 6.1% last year amid COVID-19 crisis -preliminary data.” Reuters, 02 May 2021. https://www.reuters.com/article/us-emirates-gdp-idUSKBN2CJ09C.

99 Das Augustine, Babu. “UAE Central Bank finds banking sector resilient in its 2020 Financial Stability Report.” Gulf News, 17 June 2021. https://gulfnews.com/business/banking/uae-central-bank-finds-banking-sector-resilient-in-its-2020-financial-stability-report-1.1623936888881#.

100 “United Arab Emirates.” International Monetary Fund. https://www.imf.org/en/Countries/ARE.

101 Essaid, Salim. “UPDATE 1-Cryptocurrency promise for UAE’s unbanked migrants - but not yet.” Reuters, 03 August 2021. https://www.reuters.com/article/emirates-tech-migrants-idUSL8N2PA7UG.

102 “Government Database Access Allows Abu Dhabi Islamic Bank to Enable Biometric Onboarding.” Mobile ID World, 30 August 2021. https://mobileidworld.com/abu-dhabi-islamic-bank-biometric-onboarding-808301/.

103 “UAE Uses Face Biometrics to Provide Access to Government Services.” Find Biometrics, 09 April 2021. https://findbiometrics.com/uae-uses-face-biometrics-provide-access-government-services-040905/.

104 Godinho, Varun. “New DIFC Innovation Hub to spur fintech ecosystem in Dubai.” Gulf Business, 26 May 2021. https://gulfbusiness.com/new-difc-innovation-hub-to-spur-fintech-ecosystem-in-dubai/.

105 “UAE Establishes Executive Office to Combat Money Laundering and Terrorist Financing.” United Arab Emirates Ministry of Foreign Affairs & International Cooperation, 24 February 2021. https://www.mofaic.gov.ae/en/mediahub/news/2021/2/24/24-02-2021-uae-office#.

106 Shivji, Khaled. “UAE announces new regulations for licensing crypto assets.” Keystone Law, 12 November 2020. https://www.keystonelaw.com/me/keynotes/uae-announces-new-regulations-for-licensing-crypto-assets/.

Africa

In 2020, Africa faced its first recession in 25 years in reaction to the COVID-19 pandemic, which aggravated longstanding challenges like poverty and inequality across the continent. Africa has a chance to recover from the pandemic stronger than ever, however, if governments can harness digitalization in tackling structural reforms. Recovery will be uneven, though, and poor economic performances by Angola, Nigeria and South Africa—which contribute to a third of Sub-Saharan Africa's GDP—could affect strong showings by Côte d'Ivoire and Ghana.[1]

Africa's rapidly growing fintech sector will be invaluable in supporting recovery, spearheading sustainable development goals and promoting much-needed economic diversification. Kenya, Nigeria and South Africa have already become major fintech hubs on the continent, while fintech ecosystems in Côte d'Ivoire and Ghana show incredible promise. Africa is home to about 70% of global mobile money transactions,[2] and mobile money and banking solutions like Orange Bank Africa have expanded public access to financial services. This eager adoption of innovative payments will continue to grow as governments invest in stronger digital infrastructure and internet and mobile phone penetration rates increase. Still, fintech faces barriers to growth, as startups struggle with complex bureaucratic processes and a lack of regulatory clarity. More opportunities for partnerships with large tech companies and traditional banks would also promote the development of fintech.

Going into 2022, African states are focused on central bank digital currency (CBDC), the regulation of cryptoassets, improvements to digital infrastructure and support for fintech. CBDCs will be an especially exciting area to watch in the coming years. On 25 October, Nigeria introduced the eNaira, a CBDC intended to drive financial inclusion, facilitate remittances and encourage economic growth. South Africa is participating in an international cross-border CBDC project, Ghana is conducting a retail CBDC trial, and Côte d'Ivoire and Kenya have also shown an interest in developing a CBDC.

Amidst rapid digital transformation, regulators must enhance data protection and privacy standards, strengthen cybersecurity and ensure that digitalization initiatives do not widen digital divides. The uneven application of digital progress can further exclude traditionally marginalized people based on geography, gender and income status.

Algeria

Country Overview

Algeria—Africa's largest country and its fourth-largest economy[3]—has been hit hard by the COVID-19 pandemic, which exposed vulnerabilities in the state's economic resilience, healthcare infrastructure and political stability. Following a five-year slowdown, the Algerian economy plunged by 5.5% in 2020 amidst containment measures and a drop in hydrocarbon production.[4] Summer 2021 brought another wave of infections, with case numbers surging from 500 to 1,500 a day, and the health system was close to buckling under the strain.[5] Political instability, societal unrest, corruption and a wildfire crisis have lent further uncertainty to the emerging market's future.

Digitalization will be key in helping Algeria to reach development goals, drive economic diversification, promote financial inclusion and modernize the banking and financial sector. Fifty-seven percent of Algerian adults—and 71% of women—do not have access to a transaction account, and a mere 16% of adults, and 11% of women, use digital payments.[6] The banking and financial sector relies on dated technological infrastructure,[7] and fintech innovation could revolutionize its services—making them faster, cheaper, more accessible and easier to use.

Although Algeria's fintech ecosystem is in its early stages of growth, there is reason for optimism. The **Digital Intelligence Index (DII)**, developed by Mastercard and Tufts University's Fletcher School, ranks Algeria relatively high for digital evolution momentum. The new presidential administration has been particularly progressive in its digital transformation efforts. President Abdelmadjid Tebboune took office in December 2019, and in January 2020, Yacine El-Mahdi Oualid was appointed as the country's first Minister of Startups. In October 2020, the government launched the country's first Fund for Startups; the 2020 Finance Law introduced tax incentives for startups in innovative and emerging technologies; and a September 2020 executive decree established a national committee for the classification of startups, innovative projects and incubators.[8] Recent improvements to national digital infrastructure and a government push to promote digital skills in education will be especially crucial in spearheading innovation.

This year's digital agenda focuses on an artificial intelligence strategy and a fintech regulatory sandbox. Regulators must also ensure that its national data protection framework, signed into law June 2018, is fully enacted and enforced. The National Authority for the Protection of Personal Data has not yet been established.[9] Meanwhile, cybersecurity remains a key challenge. A 2021 **study** by Comparitech ranked Algeria the world's fifth-least cybersecure state.

Financial Regulatory Authorities

The **Bank of Algeria** is the central bank of Algeria.

The **Securities and Investments Organization and Monitoring Commission (COSOB)** regulates and oversees the securities market.

Policy, Laws and Regulations

Fintech Regulatory Sandbox, 30 September 2021

The Securities and Investments Organization and Monitoring Commission launched Algeria's first fintech regulatory sandbox, dubbed the "GIE-Algeria FinLab." The Minister of Startups, Yacine El-Mahdi Oualid, stated that the sandbox aims to "enable start-ups and project leaders in the fintech sector to develop their solutions to modernize banking and insurance services, while moving towards financial inclusion."[10] Oualid is particularly keen to spur on developments in blockchain and artificial intelligence.

Artificial Intelligence Strategy, 18 January 2021

Algeria launched a National Strategy on Research and Innovation in Artificial Intelligence 2020-2030, which aims to harness AI in socioeconomic development and bolster digital skills in AI. Minister of Higher Education and Scientific Research Abdelbaki Benziane stated that the strategy aims to strengthen the knowledge economy by empowering students, and that universities and businesses should more readily partner in promoting innovation and education.[11]

Angola

Country Overview

Although Angola has made development progress since the end of its civil war in 2002, it has been mired in recession since 2016.[12] In 2020, the oil-dependent economy contracted by a further 2% amidst the COVID-19 pandemic,[13] which led to a global drop in oil demand and deepened poverty in the state. Inflation hit a four-year high in May 2021.[14] The International Monetary Fund predicts a gradual economic recovery due to good fiscal performance and debt management,[15] but the ever-changing pandemic could cause unforeseen setbacks. On 01 October 2021, the government reinstituted restrictions as deaths from COVID-19 outstripped the malaria death rate.[16]

As Angola emerges from the health crisis, digital transformation must underpin efforts to revamp and diversify the economy, promote financial inclusion and make progress in poverty reduction. Approximately 70% of the adult population lacks access to banking services,[17] and fintech will be key in making financial services more widely available, cheaper, faster and easier to use. The central bank's national plan for financial inclusion aims for 50% of the population to have access to basic financial services by the end of 2022, and mobile money solutions like Safaricom's M-Pesa could accelerate progress towards this goal.[18]

Although Angola's fintech ecosystem is in its infancy, startups have begun to emerge across the country, and they have encouraged job creation, investment and participation in the formal economy.[19] The government has also taken small steps towards cultivating a more attractive regulatory environment for fintech. In September 2020, the central bank and Beta-i, an innovation consultancy, partnered to launch a fintech regulatory sandbox. The sandbox will run four eight-month programs, with ten selected projects per program.[20] Still, Angola's business environment is riddled with corruption, which will be a major obstacle in the cultivation of the fintech ecosystem.

This year, regulators are focused on central bank digital currency (CBDC). The central bank is also expected to introduce a mobile instant payments system, in partnership with telecommunications operator Unitel.[21] A biometric electronic passport is slated to launch in late 2021, in an attempt to crack down on fraud and forgery.[22] Regulators must look to implement a national cybersecurity framework, as there are currently no cybersecurity regulations in the country. On the **Global Cybersecurity Index (GCI) 2020**, developed by the United Nations' International Telecommunication Union (ITU), Angola is ranked #151 out of 194 states.

Financial Regulatory Authorities

The **National Bank of Angola** is the central bank of Angola.

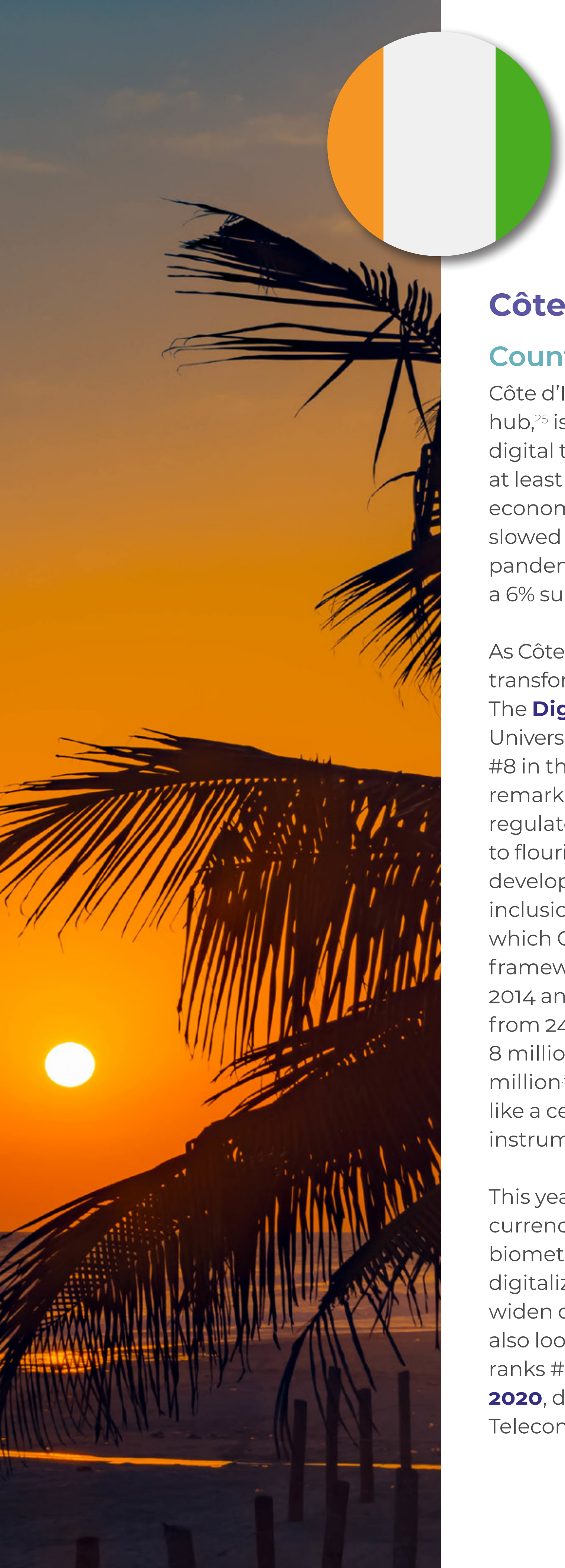
The **Agência de Protecção de Dados (ADP)** is the primary data protection authority in Angola.

The **Capital Markets Commission** regulates the capital markets in Angola.

Policy, Laws and Regulations

Central Bank Digital Currency, 09 June 2021

The central bank announced that it was in the midst of an ongoing study on the role of digital currencies—particularly CBDC—in promoting financial inclusion.[23] In October 2020, central bank governor José de Lima Massano stated that the central bank was in the early stage of assessing the use of blockchain in payment systems.[24]



Côte d’Ivoire

Country Overview

Côte d’Ivoire, francophone West Africa’s major economic hub,[25] is on the brink of incredible economic expansion and digital transformation. From 2011 to 2019, the GDP soared by at least 7% per year, making it Africa’s second fastest-growing economy for that period.[26] Although economic growth slowed to 1.8% in 2020 in reaction to the COVID-19 pandemic,[27] the International Monetary Fund (IMF) estimates a 6% surge in 2021.[28]

As Côte d’Ivoire recovers from the pandemic, digital transformation will go hand in hand with economic progress. The **Digital Intelligence Index (DII)**, developed by Tufts University’s Fletcher School and Mastercard, ranks Côte d’Ivoire #8 in the world for digital evolution momentum. Between remarkable developments to the ICT sector[29] and a friendly regulatory environment, the Ivorian fintech ecosystem is set to flourish. Innovation in payments has already contributed to development progress, particularly in promoting financial inclusion. In 2015, the Central Bank of West African States, of which Côte d’Ivoire is a member, introduced a regulatory framework for the issuance of nonbank e-money. Between 2014 and 2017, mobile money account ownership increased from 24% to 34% of the adult Ivorian population.[30] About 8 million adult Ivorians—in a country of just over 27 million[31]—are still unbanked,[32] and emerging technologies like a central bank digital currency (CBDC) would be instrumental in expanding access to financial services.

This year, regulators are focused on central bank digital currency (CBDC). The state is also looking to roll out national biometric ID cards. A key challenge will be ensuring that digitalization initiatives are applied equitably and do not widen disparities, such as the digital divide. Regulators must also look to strengthen national cybersecurity. Côte d’Ivoire ranks #11 in Africa on the **Global Cybersecurity Index (GCI) 2020**, developed by the United Nations’ International Telecommunication Union (ITU).

Financial Regulatory Authorities

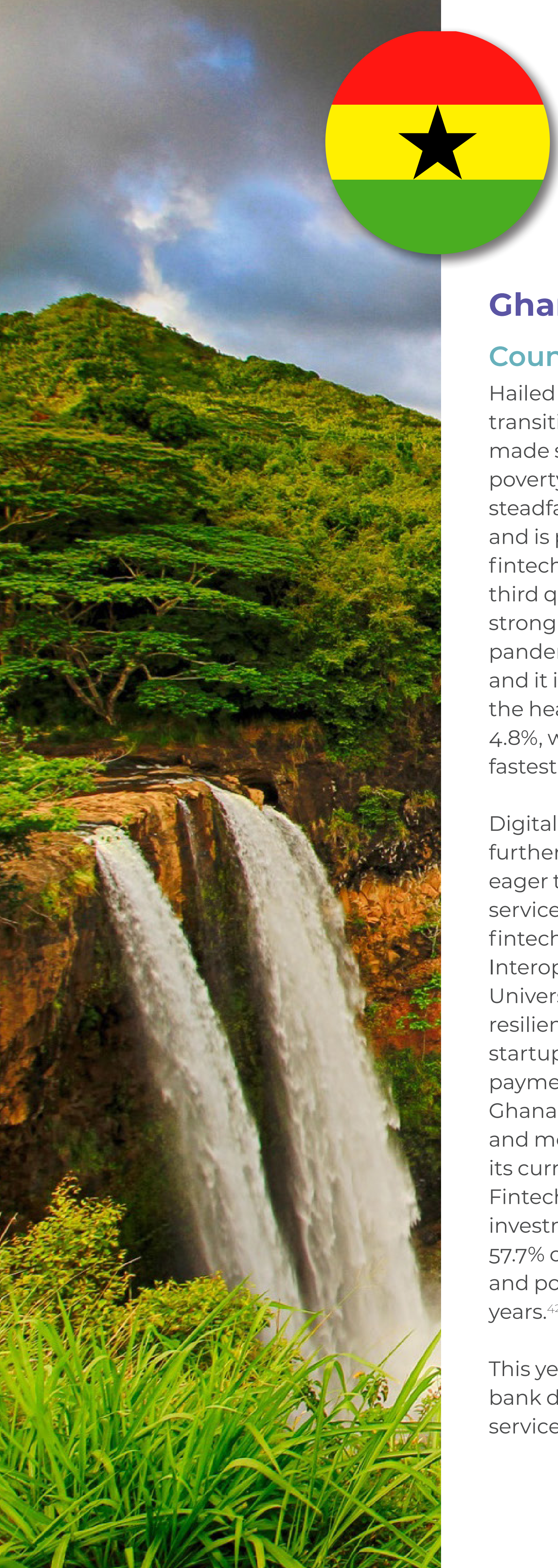
The **Central Bank of West African States (BCEAO)** is the central bank for the eight states that constitute the West African Economic and Monetary Union (UEMOA), including Côte d'Ivoire, Benin, Burkina Faso, Guinea-Bissau, Mali, Niger, Senegal and Togo.

The **Telecommunications/ICT Regulatory Authority of Côte d'Ivoire (ARTCI)** is the data protection authority of Côte d'Ivoire.

Policy, Laws and Regulations

Central Bank Digital Currency, February 2021

The Central Bank of West African States (BCEAO) has shown interest in exploring a CBDC, which would strengthen financial inclusion, simplify cross-border payments and promote greater regional integration. In February, the central bank and the International Islamic Trade Finance Corporation (ITFC) held a virtual workshop on CBDC. The workshop sought to examine international trends in CBDC, the adoption of CBDC by the BCEAO, the role of CBDC in interregional and international trade, and security, policy, legal and regulatory concerns.[33]



Ghana

Country Overview

Hailed as one of West Africa's most stable states since its 1992 transition to a multi-party democratic system,[34] Ghana has made significant strides in economic development and poverty reduction. The West African state has also been steadfast in its digital transformation over the past four years, and is poised for incredible economic growth and a boom in fintech. Although the economy contracted in the second and third quarters of 2020, it grew by 1.1% overall thanks to a strong performance before the onset of the COVID-19 pandemic.[35] In 2019, the economy grew at a breakneck 6.5%,[36] and it is set to resume this rapid growth as it emerges from the health crisis. Fitch Ratings predicts a 2021 growth rate of 4.8%, which would make the state Sub-Saharan Africa's fastest-growing economy.[37]

Digitalization will likely be a major cornerstone of Ghana's further socioeconomic development, as regulators have been eager to adopt innovative technologies, digitalize public services and foster a favorable regulatory environment for fintechs. Government initiatives like the Mobile Money Interoperability System, **Digital Financial Services Policy**, Universal QR Code and Ghana Card are driving economic resilience, progress and financial inclusion.[38] Meanwhile, startups are increasingly being established, and the payments and remittances sector will be one to watch.[39] Ghana is now Africa's fastest-growing mobile money market, and mobile payments revenue is estimated to increase from its current USD$3.5 billion to USD$14-20 billion in 2025.[40] Fintech will prove invaluable in attracting foreign direct investment and expanding access to financial services. Only 57.7% of the Ghanaian adult population has a bank account,[41] and poverty reduction efforts have stalled over the past nine years.[42]

This year, regulators are spearheading initiatives in central bank digital currency (CBDC), the digitalization of public services, anti-money laundering, cybersecurity and a fintech regulatory sandbox pilot. A Startup Bill is also in the works, and it would facilitate the establishment of innovative companies and offer tax breaks. As digital transformation progresses, regulators must ensure that they continue to collaborate with the private sector and develop a fintech-friendly environment. Partnerships between regulators, fintech startups and international companies like Mastercard and Visa will streamline Ghana's efforts to achieve sustainable development goals and nurture its digital economy.

Financial Regulatory Authorities

The **Bank of Ghana (BoG)** is the central bank of Ghana.

The **Data Protection Commission** is the national data protection authority of Ghana.

The **Securities and Exchange Commission (SEC)** regulates the equity capital markets in Ghana.

Policy, Laws and Regulations

Retail Central Bank Digital Currency Trial, 11 August 2021

The central bank announced that it had partnered with German firm Giesecke+Devrient (G+D) to trial a retail CBDC. According to the joint press release, "The project is part of the 'Digital Ghana Agenda', which involves the digitization of the country of 30 million people and its government services. The digital Cedi, or 'e-Cedi', is intended to complement and serve as a digital alternative to physical cash, thus driving the Ghanaian cashlite agenda through promotion of diverse digital payments, while ensuring a secure and robust payment infrastructure in Ghana. It also aims to facilitate payments without a bank account, contract, or smartphone, by so doing boosting the use of digital services and financial inclusion amongst all demographic groups."[43] The experiment will be conducted in three phases: design, implantation and pilot. Beyond the technical infrastructure, the project will focus on IT security, legal implications and a CBDC's impact on monetary policy and the national payment system.

Ghana.gov Account, 14 July 2021

Vice President Dr. Mahamudu Bawumia launched the Ghana.gov platform, which allows citizens to access and make payments for online government services. According to Dr. Bawumia, "It is estimated that about 10 to 15% of government collections are lost through inefficiencies, theft and other accounting schemes. Going digital means that we can improve our revenue collections by an estimated three billion Cedis [approximately USD $501,510,000] annually...This government's aim of making Ghana a globally competitive market is anchored in the belief that increasing access to public services through technology will have a strong positive impact in the general ease of doing business within Ghana. In the process, this will boost our ranking among other nations and thereby help grow our foreign direct investments."[44]

Regulatory and Innovation Sandbox Pilot, 25 February 2021

The central bank launched a regulatory and innovation sandbox pilot, available to banks, specialized deposit-taking institutions and payment service providers, including dedicated electronic money issuers and unregulated entities. According to the bank's press release, "the Bank of Ghana would give preference to products and services leveraging blockchain technology, remittance products, crowdfunding products and services, e-KYC (electronic know your customer) platforms, RegTech (regulatory technology), SupTech (supervisory technology), digital banking, products and services targeting women financial inclusion and innovative merchant payment solutions for micro, small and medium size enterprises (MSMEs)."[45] Besides facilitating the development of innovative ideas and effective regulations, the sandbox aims to promote financial inclusion, reduce time-to-market and lower the cost of innovation.

New Anti-Money Laundering Law, 29 December 2020

A new Anti-Money Laundering Act, 2020 (Act 1044) was enacted. The new Act aims to improve upon the Anti-Money Laundering Act, 2008 (Act 749), bring Ghana's AML/CTF framework in line with international standards and consolidate all AML/CTF regulations into one. It expands the authority of Ghana's anti-money laundering authority, the Financial Intelligence Centre (FIC); widens the scope of illegal activities; introduces modifications in response to the emergence of innovative technologies; and imposes harsher penalties for violations. The FIC is expected to collaborate with relevant national agencies in enforcing the Act, and is authorized to share information with international counterpart agencies and issue notices and directives.[46] Persons who aid in the execution of illegal activities—including but not limited to fraud, bribery, insider trading, currency counterfeit and corruption—are now included under the scope of the Act. In light of the increasing popularity of cryptocurrencies and their role in illegal activities, the Act defines virtual asset service providers (VASPs) and imposes requirements on them. In the case of violations of the Act, guilty persons are subject to a fine no less than 100% and no greater than 500% of the proceeds of the crime. Guilty corporate entities face a fine of no less than 300% of the proceeds of the crime."[47] In summer 2021, Ghana was removed from the Financial Action Task Force's "grey list."[48]

The Cybersecurity Act, December 2020

The Cybersecurity Act, 2020 (Act 1038) was passed. The Act aims to strengthen the detection and deterrence of cybersecurity threats, promote collaboration with international agencies and raise awareness on cybersecurity. The newly-created Cyber Security Authority is authorized to issue licenses for cybersecurity services, set certification standards for cybersecurity products, advise the government on cybersecurity, protect children online and provide technical support to law enforcement and security agencies in the prosecution of violators.[49] The Act also established a Cybersecurity Fund, to provide financial assistance in strengthening national cybersecurity; and a National Computer Emergency Response Team, that is responsible for responding to and coordinating responses to cybersecurity incidents affecting public institutions, private institutions and international bodies. In addition, the Act imposes requirements for incident reporting and the licensing of cybersecurity service providers. Ghana ranks #3 in Africa on the **Global Cybersecurity Index (GCI) 2020**, developed by the United Nations' International Telecommunication Union (ITU). The index notes that Ghana's areas of relative strength are legal and technical measures.

Kenya

Country Overview

One of East Africa's largest economies, Kenya is poised to become a global leader in fintech innovation.

Structural reforms have driven incredible economic growth and social development, and between 2015 and 2019, Kenya was one of Sub-Saharan Africa's fastest-growing economies at an average annual growth rate of 5.7%.[50] The Kenyan economy grew at a sluggish 0.6% in 2020 amidst the COVID-19 pandemic,[51] but the International Monetary Fund (IMF) predicts a 2021 surge of 7.6%,[52] its most rapid growth in a decade. Still, poverty and inequality persist,[53] and the health crisis has reversed development progress and plunged 2 million more Kenyans into poverty.[54]

As Kenya recovers from the pandemic, digitalization will be key in driving financial inclusion, achieving sustainable development goals and pursuing **Vision 2030** initiatives. Launched in 2008, the vision aims for Kenya to reach middle-income status by 2030. Innovations in fintech have already paved the way: companies like Safaricom and Equitel have promoted financial inclusion throughout Kenya, and 83% of the population now has access to some type of financial service.[55] Safaricom's M-Pesa mobile banking service gained a million new subscribers in 2020, bringing the total to 25 million users,[56] and new entrants to the digital banking scene are sure to come. Kenya has 93 fintechs in operation, 16.1% of Africa's total, and fintech funding has soared 209% over the past two years.[57] The mobile payments sector is particularly strong, with mobile transactions at 87% of the GDP, a rate second only to China's.[58] As the Kenyan fintech ecosystem matures, regtech, insurtech and blockchain will be areas to watch.[59]

Kenya's 2021 digital agenda focuses on strengthening the national payments system, a possible central bank digital currency (CBDC) and the expansion of its regulatory sandbox. The central bank is also expected to release a digital finance policy. As Kenya continues to digitalize, regulators must look to strengthen the national cybersecurity framework. In the central bank's **Banking Sector Innovation Survey 2020**, banking institutions identified cybersecurity as one of the top three challenges faced in product innovation, and over a third of banking institutions deemed cyber-risk their key risk in this area. The surveyed institutions also identified a lack of clarity in several regulatory requirements, including requirements on cloud computing, distributed ledger technology (DLT) and turnaround time for approval of new products. Money laundering is another primary challenge to the financial sector and its regulators. According to an International Narcotics Control Strategy report, Kenya remains a major hotspot for money laundering, terrorist financing and fraud.[60]

Financial Regulatory Authorities

The **Central Bank of Kenya** is the country's central bank and the primary regulatory authority for the financial sector.

The **Capital Markets Authority of Kenya** regulates and supervises the capital markets in Kenya.

The **Office of the Data Protection Commissioner (DPC)** enforces the Data Protection Act (DPA).

Policy, Laws and Regulations

Biometric Identification Requirement in Insurance Coverage, 11 July 2021

The National Hospital Insurance Fund (NHIF), Kenya's national insurance agency, replaced its insurance cards with a fingerprint recognition system. Members must register their biometric data in order to file claims and receive insurance, and may register at participating hospitals or NHIF service centers. The move aims to tamp down on fraud and manual claims processing. The Kenyan government has also sought to introduce a national biometric identification system, but the project has stalled.[61]

Central Bank Digital Currency, June 2021

In an interview, Central Bank of Kenya Governor Dr. Patrick Njoroge stated that, "We are already having discussions with other global players, in various ways, around the introduction of Central Bank Digital Currencies. The push comes as a result of mushrooming of private cryptocurrencies and we are already feeling left out and need to create our own space."[62] Njoroge also mentioned the need to address cryptocurrency's role in illicit activities such as money laundering.

Regulatory Sandbox: Cryptoassets, Artificial Intelligence and Machine Learning, April 2021

The Capital Markets Soundness Report (CMSR) Volume XVIII, Quarter 1 2021 outlines national, regional and international capital markets developments. Per the report, the CMA now welcomes fintech firms with artificial intelligence and machine learning applications to apply for participation in the authority's regulatory sandbox. The CMA is also reviewing a plan to allow fintech firms with crypto applications (except cryptocurrencies) to participate in the sandbox. In response to the rising popularity of crypto investment in Kenya, the CMA expresses the desire to forge a "common stance and joint-messaging" with the central bank. The CMA would also like to establish a joint Financial Sector Regulatory Sandbox with other financial sector regulators, so that "joint expertise from the various subsectors may be leveraged to test various forms of crypto-assets and other FinTechs to inform future oversight of the same."[63] The number of cryptocurrency investors in Kenya is estimated to be around 4.5 million, 8.5% of the population,[64] and Kenya ranks #1 in the globe for P2P crypto trade.[65]

Kenya National Payments System Vision and Strategy 2021-2025, December 2020

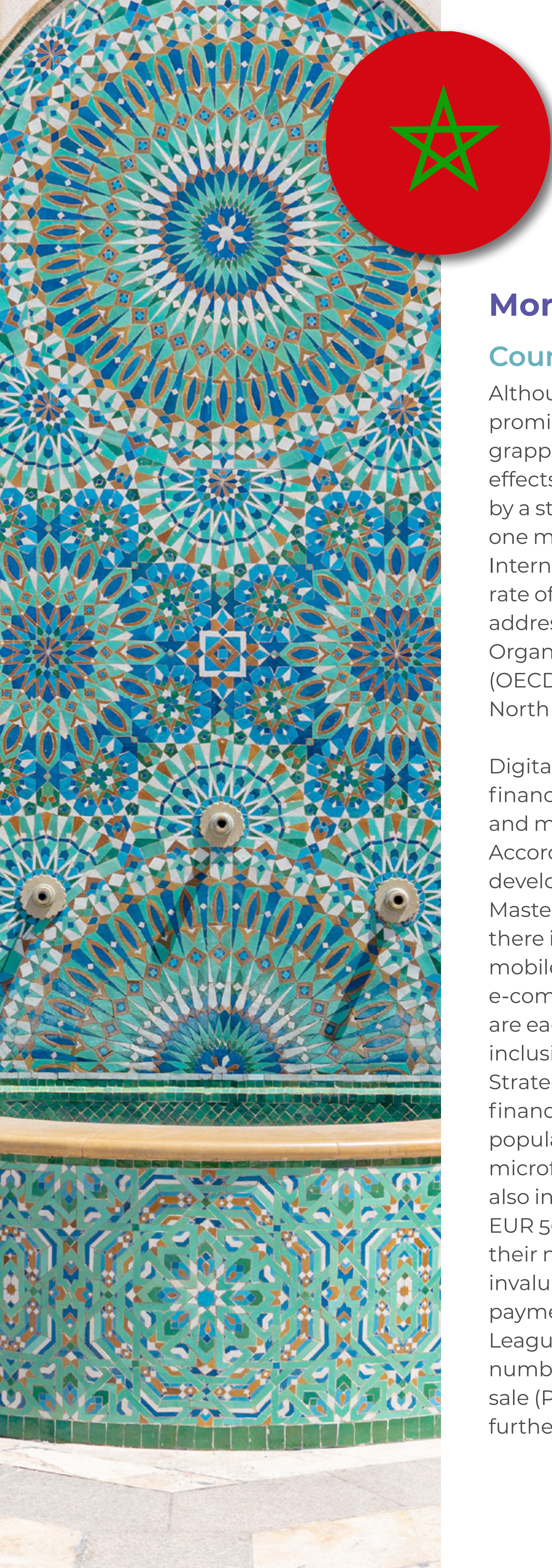
The central bank issued the draft *Kenya National Payments System Vision and Strategy 2021-2025*, which aims to drive digital payments and promote innovation, choice and security. The four main objectives of the vision and strategy are:

1. "To facilitate payments systems that meet the diverse needs of users and supports the country's development agenda.
2. To ensure payments systems are secure through influencing industry and global standards, and adopting safe technologies.
3. To power an ecosystem based on collaboration leading to launch of premier and globally competitive innovations.
4. To implement a supportive policy, legal and regulatory framework that is firmly enforced across all existing and emerging players."[66]

Towards these objectives, the central bank seeks to promote the development of a financial data protection framework; promote the adoption of digital identity in verification, including e-KYC; strengthen security data analytics and security reporting; promote efficient and effective clearing infrastructure for payment systems; spearhead initiatives to facilitate cross-border payments; and boost accessibility to payment instruments amongst vulnerable communities.

First Data Protection Commissioner, 16 November 2020

Immaculate Kassait was sworn in as Kenya's first data protection commissioner (DPC). The DPC enforces and oversees implementation of the 2019 Data Protection Act, and is authorized to conduct investigations, impose fines for non-compliance and facilitate negotiation in the case of a dispute. Kassait has vowed to hold big tech companies accountable.[67]



Morocco

Country Overview

Although Morocco's digital transformation progress shows promise, the cash-reliant Maghrebi state continues to grapple with structural challenges and the devastating effects of the COVID-19 pandemic. In 2020, the GDP plunged by a staggering 7.1%,[68] unemployment and poverty rose, and one million people became vulnerable to poverty.[69] The International Monetary Fund (IMF) predicts a 2021 growth rate of 5.7%,[70] but the government will have an uphill battle in addressing drastic income inequality. According to the Organisation for Economic Co-operation and Development (OECD), Morocco has the highest income inequality rate in North Africa.[71]

Digitalization will be crucial in expanding public access to financial services, bringing people into the formal economy and making progress towards other development goals. According to the 2020 **Digital Intelligence Index (DII)**, developed by Tufts University's Fletcher School and Mastercard, digital evolution in Morocco is sluggish. Still, there is reason for optimism. Morocco has relatively strong mobile coverage and mobile phone penetration, e-commerce surged amidst the pandemic, and regulators are eager to promote mobile payments and financial inclusion. In 2019, the government launched the National Strategy for Financial Inclusion, which seeks to raise the financial inclusion rate from 34% to 47% of the adult population by 2024 through the development of microfinance and mobile financial services. Regulators have also introduced remote onboarding for accounts capped at EUR 500 and requested payment institutions to strengthen their networks of access points.[72] Fintech will be particularly invaluable in promoting financial inclusion and making payments faster, cheaper and more accessible. Of the 22 Arab League member states, Morocco is home to the third-highest number of fintechs, and payment, remittance and point-of-sale (POS) sectors will be ones to watch.[73] Barriers to the further development of fintech persist, however, as Morocco lacks a fintech regulatory framework.

This year, Morocco is exploring central bank digital currency (CBDC) and a Memorandum of Understanding (MoU) with Luxembourg. Partnerships with wealthy countries and international agencies will be especially crucial in driving recovery and strengthening the digital economy. In June, the World Bank approved a USD$450 million loan to help Morocco spearhead reforms aimed at expanding access to digital and financial services.[74] Morocco's Digital Development Agency (DDA) is also keen to spearhead e-government initiatives. In 2020, it launched the Digital Morocco strategy, which aims to have 50% of Moroccan administrative procedures online, reduce the digital divide by 50% and connect 20% of Moroccan SMEs.[75] Going forward, regulators must seek to strengthen national digital infrastructure and ensure that digitalization initiatives do not widen socioeconomic disparities.

Financial Regulatory Authorities

The **Bank Al-Maghrib (BAM)** is the central bank of Morocco.

The **National Commission for the Protection of Personal Data Protection (CNDP)** is Morocco's data protection authority.

The **Moroccan Capital Markets Authority (AMMC)** regulates the financial markets in Morocco.

Policy, Laws and Regulations

Central Bank Digital Currency, February 2021

The central bank confirmed that it was in the early stages of exploring a CBDC. It established a committee to "identify and analyze the contributions, the benefits as well as the risks of a CBDC for the national economy. In addition, this committee will thoroughly review all consequences of a CBDC on monetary policy, the structure of banking intermediation, financial stability and legal framework."[76] The bank noted that it was "premature to consider the issuance of a digital currency in the short term."[77] The introduction of a CBDC could be revolutionary in promoting digital payments and financial inclusion in Morocco.

Memorandum of Understanding on Digitalization, January 2021

Morocco and Luxembourg signed a Memorandum of Understanding (MoU) in a move to collaborate on digitalization initiatives, with a focus on e-government, digital inclusion and digital infrastructure. In 2020, Luxembourg opened a Trade and Investment Office in Casablanca, which seeks to offer Moroccan investors and companies an inroad to Luxembourg, while pinpointing opportunities for Luxembourger companies in Morocco.[78] Morocco and Israel have also been strengthening ties since their March normalization of relations, and the states are expected to further cooperate in fintech.[79] Investment funds from the wealthy and innovative Israel could provide Morocco with much-needed capital as it seeks to recover from the pandemic.

Nigeria

Country Overview

Nigeria—Africa's largest economy and its most populous state—is poised for incredible growth in fintech, but it continues to face serious structural challenges. Forty percent of Nigeria's population lives in poverty—and 25% are vulnerable—due to inequality, a lack of job opportunities and social and political turmoil. Amidst the COVID-19 pandemic and rapid population growth, approximately seven million more Nigerians were estimated to have fallen into poverty in 2020.[80] Meanwhile, Nigeria's oil-dependent economy contracted by 1.8% in 2020 in response to the health crisis, capital outflows, heightened risk aversion, a slowdown in remittances and a global drop in oil prices.[81] The International Monetary Fund (IMF) predicts growth rates of 2.5% and 2.6% in 2021 and 2022, respectively.[82]

Nigeria's rapidly growing fintech ecosystem could be key in promoting economic diversification, financial inclusion and other development goals. The West African state is home to about 200 fintech startups,[83] which raised approximately USD$330.5 million in the first half of 2021—over double the sector's earnings in 2020.[84] Companies like Opay and Palmpay have made international headlines,[85] and digital money is estimated to contribute USD$3.7 trillion to Nigeria's GDP by 2025.[86] Despite fintech's optimistic outlook, overall digitalization in Nigeria has lagged. According to the **Digital Intelligence Index (DII)**, developed by Mastercard and Tufts University's Fletcher School, Nigeria ranks last of 90 economies in digital evolution momentum.

This year, regulators are focused on central bank digital currency (CBDC), open banking, a national digital ID, a cryptocurrency ban and a fintech regulatory sandbox. To enable further digitalization, regulators must strengthen national data protection standards and digital infrastructure. Cheaper, faster and more accessible digital infrastructure will help to ensure that the digital divide does not widen. Less than 50% of the Nigerian population has access to the internet,[87] although smartphone penetration is steadily increasing.[88] Cybersecurity remains another key challenge, as less than 25% of Nigerian businesses have an IT security provider or staff member.[89]

Financial Regulatory Authorities

The **Central Bank of Nigeria** is the central bank of Nigeria.

The **National Information Technology Development Agency (NITDA)** enforces the Nigerian Data Protection Regulation (NDPR).

The **Securities and Exchange Commission (SEC)** regulates the Nigerian capital market.

Policy, Laws and Regulations

National Digital ID, 31 October 2021

Nigeria's quest to institute a national digital ID, which began seven years ago, has been fraught with controversy. By 31 October 2021, Nigerians were required to have linked their national identity numbers (NINs) with their mobile numbers, a move that has been met with outcry over data protection and privacy concerns. The 11-digit NIN, the bedrock of the national digital ID system, aims to tamp down on insurgency and other crimes. Per an August 2021 statement by the National Identity Management Commission, only about 60 million citizens and legal residents—in a country of 200 million—have enrolled for an NIN.[90] In February 2021, the Minister of Communications and Digital Economy communicated a plan to replace the bank verification number (BVN) with the NIN, as the BVN can only be used by people with bank accounts.[91]

Central Bank Digital Currency, 25 October 2021

The central bank launched its CBDC, the eNaira, making Nigeria one of the first countries in the world to introduce a digital currency. The eNaira, which supplements cash and coins, aims to bolster financial inclusion and make remittances cheaper and faster. The project was announced in February, after the central bank banned banks and other financial institutions from handling and facilitating cryptocurrency transactions.[92] Still, Nigerians continue to gravitate towards cryptocurrencies as inflation climbs. Cryptocurrencies also offer Nigerians an easier way to make cross-border transactions, as US dollars can be difficult to obtain in the state.[93]

Approved Standard Operating Guidelines for BVN Matching System Version 2.0, 29 March 2021

The Nigeria Inter-Bank Settlement System (NIBSS) issued the Approved Standard Operating Guidelines for BVN Matching System Version 2.0 (the "BVN Guideline"), non-bank entities would no longer be able to utilize the bank verification number (BVN) system for the identity verification of new customers.[94] The move has had a negative effect on Nigerian fintechs, who were previously allowed to use the system. It is unclear why the NIBSS, which is owned by the central bank, issued the new rule, but there is speculation that it intends to attract more participants to the national identity number (NIN) system.[95]

Regulatory Framework for Open Banking, 17 February 2021

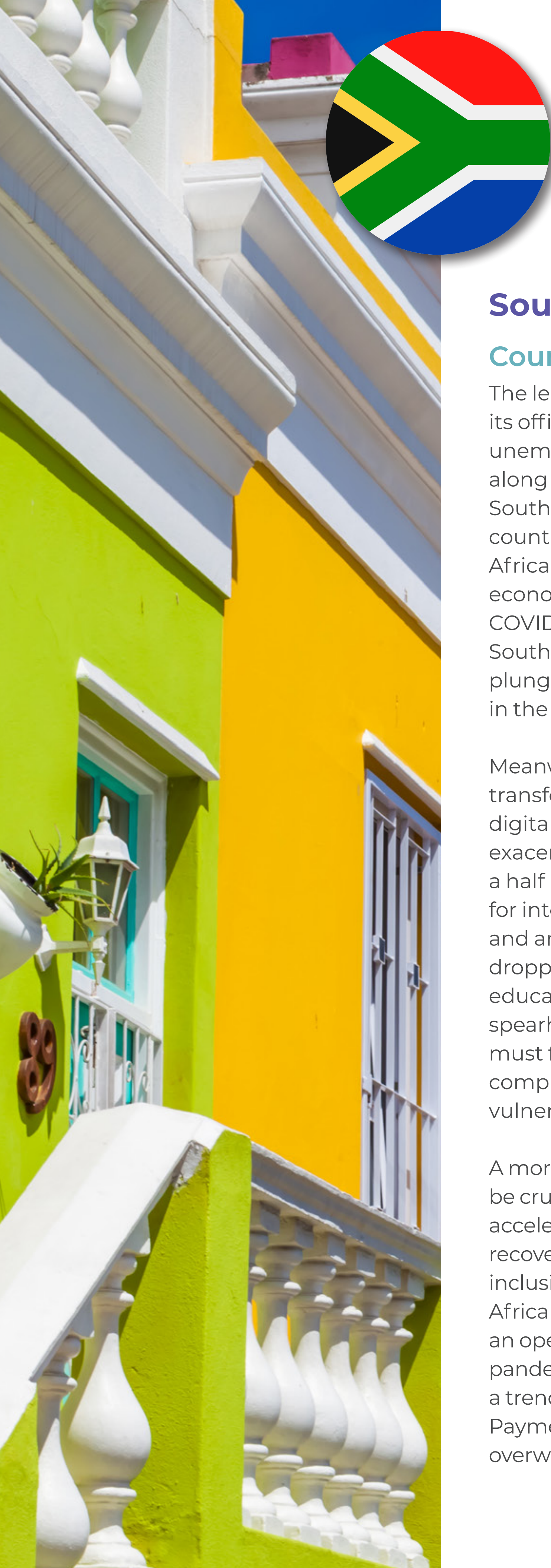
The central bank issued the Regulatory Framework for Open Banking. According to the circular, "The framework establishes principles for data sharing across the banking and payments ecosystem, which will promote innovation, broaden the range of financial products and services, and deepen financial inclusion. The regulatory framework stipulates, amongst others, data and Application Programming Interface (API) access requirements, principles for API, data, technical design and information security specifications. Operational guidelines related to the framework will be communicated in due course."[96] An open banking regime will be instrumental in driving down costs, encouraging innovation and offering consumers more choice, which will expand access to financial services amongst Nigeria's unbanked population.

Cryptocurrency Ban, 05 February 2021

The central bank issued a circular banning banks and other financial institutions from dealing in and facilitating cryptocurrency transactions. The bank claimed that violations would incur "severe regulatory sanctions."[97] Lamido Yuguda, the director-general of the Nigerian Securities and Exchange Commission, stated that the ban has caused market disruptions, and that the SEC and central bank were developing a regulatory framework for cryptocurrencies. The ban has not stopped cryptocurrency transactions in Nigeria, however, as investors have flocked in rising numbers to peer-to-peer channels.[98]

Fintech Regulatory Sandbox, 13 January 2021

The central bank approved a framework for regulatory sandbox operations, which seeks to promote competition, foster the development and adoption of innovative technologies, strengthen confidence in the financial system and bolster financial inclusion. The sandbox is open to fintechs operating in payments.



South Africa

Country Overview

The legacy of South African apartheid has endured long after its official end in 1994, and high inequality, poverty, unemployment and food insecurity rates persist—generally along racial and gender lines. In 2019, the World Bank named South Africa the most unequal country in the world, with the country's top 1% owning 70.9% of its wealth.[99] Although South Africa has instituted some structural reforms, social and economic development stalled even before the onset of the COVID-19 pandemic. The pandemic drove a 7% contraction in South Africa's 2020 economy, 2 million people have been plunged into poverty[100] and unemployment soared to 32.6% in the first quarter of 2021.[101]

Meanwhile, South Africa has made strides in its digital transformation, but progress has been applied unevenly. The digital divide has thus widened,[102] and the pandemic further exacerbated inequality in access to digital services. Seven and a half million low-income South Africans pay 80 times more for internet access than do middle- and high-income people, and amidst the pandemic, 750,000 South African children dropped out of school because they lacked access to remote education.[103] Internet penetration is at a mere 56%.[104] In spearheading further digitalization initiatives, regulators must first and foremost invest in high-quality and comprehensive digital infrastructure, especially in vulnerable communities.

A more strategic and inclusive approach to digitalization will be crucial in expanding access to financial services, accelerating development and driving the post-pandemic recovery. Fintech in particular could pave the way for financial inclusion and attract the foreign direct investment that South Africa desperately needs. South Africans have already shown an openness to innovative technologies. In reaction to the pandemic, they have increasingly flocked to digital payments, a trend that is expected to continue. The Mastercard New Payment Index revealed that South Africans are overwhelmingly open to innovative payment methods that involve QR codes, biometric identity verification and contactless.[105]

This year, South African regulators are focused on a cross-border central bank digital currency (CBDC) trial under a retail CBDC model; cybersecurity; a cryptoassets regulatory framework; and the enforcement of the data protection framework. The Automated Biometric Identification System (ABIS), a national digital ID project launched in 2017, is still underway, but continues to face setbacks.[106]

Financial Regulatory Authorities

The **South African Reserve Bank (SARB)** is the central bank of South Africa.

The **Financial Sector Conduct Authority (FSCA)** supervises and regulates financial institutions' market conduct.

The **Information Regulator** oversees compliance with the Protection of Personal Information Act (POPIA).

The **Prudential Authority**, housed within the South African Reserve Bank, regulates banks, insurers, co-operative financial institutions, financial conglomerates and certain market infrastructures.

Policy, Laws and Regulations

Cross-Border CBDC Trial, 02 September 2021

The Bank for International Settlements Innovation Hub has partnered with the central banks of South Africa, Australia, Malaysia and Singapore to trial the use of CBDCs in cross-border transactions. According to the Bank for International Settlements' press release, "Led by the Innovation Hub's Singapore Centre, Project Dunbar aims to develop prototype shared platforms for cross-border transactions using multiple CBDCs. These multi-CBDC platforms will allow financial institutions to transact directly with each other in the digital currencies issued by participating central banks, eliminating the need for intermediaries and cutting the time and cost of transactions. The project will work with multiple partners to develop technical prototypes on different distributed ledger technology platforms. It will also explore various governance and operating designs that would enable central banks to share CBDC infrastructures, benefitting from the collaboration between public and private sector experts in different jurisdictions and areas of operation."[107] The results are slated for an early 2022 publication date. A cross-border CBDC would be crucial in making remittances faster and cheaper. South Africa is the continent's largest remittance send-market, at a volume of USD$921 million in 2020. Approximately 50% of its remittances are sent via informal channels.[108]

Enforcement of Protection of Personal Information Act, 01 July 2021

Enforcement of the Protection of Personal Information Act (POPIA) 2013 went into effect. Certain provisions pertaining to oversight of access to information went into effect 30 June 2021. POPIA, signed into law in 2013, has only been partially enforced until now. The Act applies to all organizations that process personal information in South Africa, and codifies data protection rights for individuals, companies and trusts. It imposes reporting obligations in the case of data breaches and requirements on the cross-border transfer of personal data.[109] Cross-border transfers of personal data are prohibited unless the recipient is subject to equal data protection standards; the data subject has provided consent; the transfer must be performed in executing a contract to which the data subject is a party; or the transfer benefits the data subject and consent is likely to be given.[110] Organizations in non-compliance could face fines of up to ZAR 10 million (approximately USD$580,000).[111]

Position Paper on Cryptoassets, 06 June 2021

Following a spate of crypto scams—including South Africa's largest Ponzi scheme in history, which saw the disappearance of USD$3.6 billion in Bitcoin—financial regulators are eager to regulate cryptoassets. The Crypto Assets Regulatory Working Group (CAR WG), part of the Intergovernmental Fintech Working Group (IFWG), published the *Position Paper on Crypto Assets*, which outlines recommendations towards a national cryptoassets regulatory framework. The three primary recommendations include the application of the AML/CFT framework to cryptoasset service providers (CASPs), the development of a framework for monitoring cross-border financial flows and the application of financial sector laws to CASPs.

Per the paper, "This would require CASPs to become licenced intermediaries and provide for the rendering of advice by such entities. This allows for regulatory oversight and will assist in addressing the immediate exploitation of consumers by unscrupulous entities."[112] Regulators hope to solidify a timeline for the implementation of the framework within three to six months. Kuben Naidoo, chief executive officer of the Prudential Authority, stated, "Now we are defining this as a financial product and if there are scams where the public is being duped, given incorrect or false information, it is certainly a market conduct issue that should be taken seriously."[113] Crypto investment has become wildly popular in South Africa, with daily trading values topping USD$145 million in January 2021.[114]

Cybercrimes and Cybersecurity Act, 26 May 2021

President Cyril Ramaphosa signed the Cybercrimes and Cybersecurity Act into law. The Act requires electronic communications service providers and financial institutions to report cybersecurity breaches to the SA Police Service, within 72 hours of becoming aware. The Act also criminalizes cyber fraud, extortion, forgery, the sending of harmful data messages and the unauthorized access of personal data, a data storage medium or computer system. Perpetrators face fines and prison sentences of up to 15 years.[115]

Tanzania

Country Overview

Although macroeconomic stability contributed to Tanzania's move from "low-income" to "lower-middle-income" country status in July 2020,[116] political turmoil and the COVID-19 pandemic have chipped away at progress and bred uncertainty. In 2020, Tanzania's GDP grew by 2%, a major downgrade from its 2019 growth of 5.8%,[117] and 600,000 Tanzanians were plunged into poverty.[118]

Digitalization will be instrumental in helping Tanzania to make progress in economic and social development, particularly with regard to financial inclusion and economic diversification. According to 2019 statistics, around 28% of Tanzanians lack access to a bank account—with a 9% gender gap in the financial inclusion rate—and 44% of excluded people are farmers or fishermen.[119] Economic diversification will prove especially crucial as climate change threatens to destabilize the agriculture-based economy.

Tanzania's digitalization journey is in its early growth stage, with an internet penetration rate of 25%.[120] The East African state has about 33 fintech startups, and faces several challenges in further developing its nascent ecosystem. According to a **report** by the United Nations Capital Development Fund, primary obstacles include a lack of funding, "limited availability of affordable and skilled local talent," few partnerships between fintech startups and large businesses, and a lack of engagement between fintech startups and regulators.[121]

There is reason for optimism, however, as national regulators and international organizations look to accelerate digital transformation in Tanzania. This year's digital agenda focuses on the adoption of innovative technologies, such as digital currency and blockchain, and the development of a real-time, digital payment system. President Samia Suluhu Hassan has requested the central bank to investigate the possible role of digital currency in the Tanzanian economy.[122] The government is also developing a national digital economy blueprint, with a major focus on bolstering the state's IT and connectivity capabilities.[123] In May 2021, the World Bank approved USD$150 million towards the Digital Tanzania Project (DTP), which aims to boost access to high-quality broadband internet services.[124] Alongside digitalization efforts, regulators must look to implement data protection and cybersecurity standards. Tanzania currently has no national data protection framework.

Financial Regulatory Authorities

The **Bank of Tanzania** is the central bank of Tanzania.

The **Capital Markets and Securities Authority (CMSA)** regulates and oversees the financial services sector.

Policy, Laws and Regulations

Amendments to the Regulations for Electronic Transactions Levy for 2021, 31 August 2021

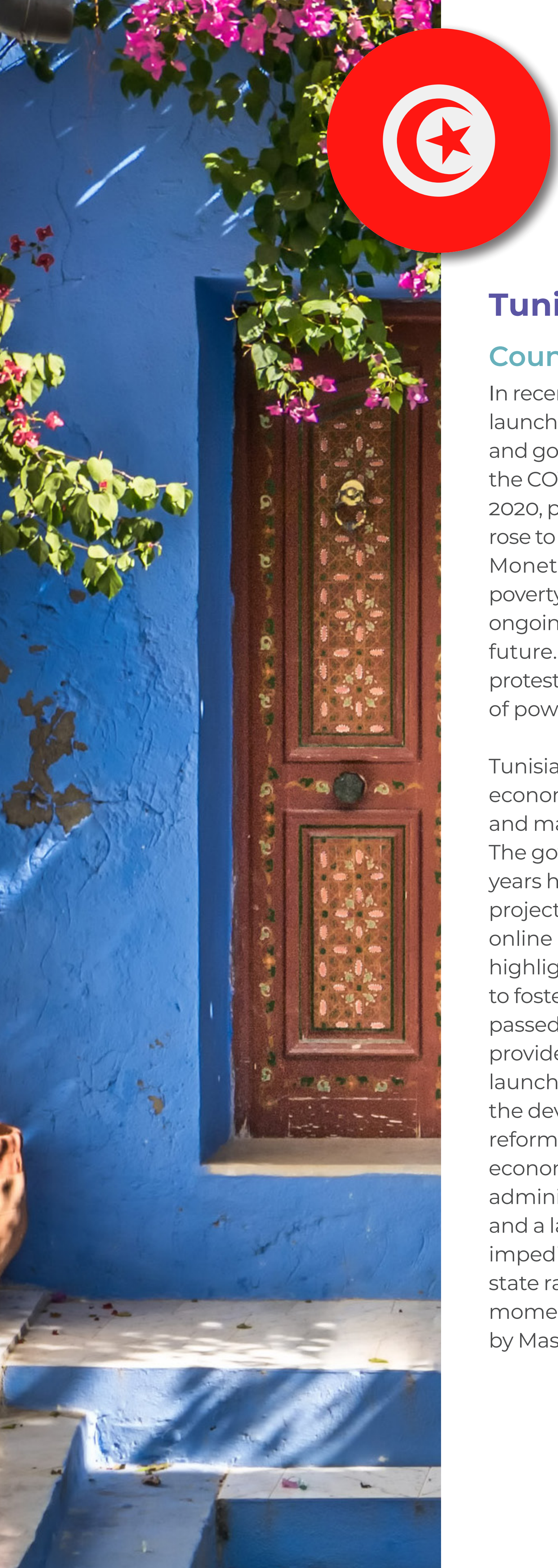
In June 2021, the government issued the amended Electronic and Postal Communication Act, which imposed a levy of SH 10 (approximately USD$0.0043) – SH 10,000 (approximately USD$4.31) on mobile money transactions. The move, which sparked controversy, aimed to raise revenue for the 2021/2022 federal budget. In reaction to widespread outcry, the Ministry of Finance and Planning released an August statement detailing amendments to the Regulations for Electronic Transactions Levy for 2021. The amendments reduced the levies by 30%. The Ministry also held discussions with mobile service providers, who committed to lowering charges for mobile financial transactions by 10%.[125]

Tanzania Instant Payments System (TIPS), July 2021

The central bank began the first implementation phase of its Tanzania Instant Payments System (TIPS), an interoperable, real-time digital payment system that conducts transfers between Digital Financial Service Providers (DFSPs) across the country.[126] The first phase of the four-stage implementation process will cover peer-to-peer (P2P) and person-to-business payments.[127] According to the central bank's **web page** on payment initiatives, "TIPS will increase financial inclusion by improving access and usage of financial services in Tanzania through promoting the interoperability of digital financial services amongst all Payment Service Providers in the country. The TIPS platform facilitates an efficient clearing and settlement platform of digital financial services transactions for all Payment Service Providers (PSPs). It will also increase the efficiency by moving from bilateral interoperability to multilateral interoperability."[128] As of December 2020, there were 32.3 million mobile money accounts in Tanzania, and cheaper and more convenient payments will boost this number even more. TIPS will house all mobile money operators—such as Airtel Money, M-Pesa and Tigo—on one platform, and users will only need to have the name of the transfer recipient in their contacts list in order to make a payment. The project was originally scheduled for a 2020 rollout, but it was delayed due to the COVID-19 pandemic and technical changes.[129]

Directive on Digital Currency and Blockchain, 13 June 2021

President Samia Suluhu Hassan addressed the global rise of digital currencies in a speech, and urged the central bank to begin exploring developments in cryptocurrency and blockchain.[130] The central bank issued a crypto ban in November 2019, but President Hassan's stance could soon see its reversal.[131] A central bank digital currency, coupled with a national digital identity, would be instrumental in promoting financial inclusion in the emerging market.



Tunisia

Country Overview

In recent years, Tunisia—the North African country that launched the Arab Spring—has faced steep economic, financial and governmental challenges, which have been aggravated by the COVID-19 pandemic. The economy nosedived by 8.8% in 2020, poverty and vulnerability worsened, and unemployment rose to 17.8% by the first quarter of 2021.[132] The International Monetary Fund predicts a 2021 growth rate of 3.8%,[133] but poverty and vulnerability will continue to deepen.[134] Meanwhile, ongoing political unrest has lent further uncertainty to Tunisia's future. Thousands of people continue to flock to the streets in protest against—or in support of—President Kais Saied's seizure of power in July.[135]

Tunisia must harness digital transformation in addressing its economic and financial challenges, spearheading recovery and making progress towards sustainable development goals. The government's most ambitious strategy of the past few years has been Digital Tunisia 2020, which included 64 projects towards expanding digital infrastructure, promoting online payment systems and more.[136] One of the strategy's highlights, **Startup Tunisia**, encompassed multiple initiatives to foster entrepreneurship and innovation. The Startup Act, passed in 2018, aims to simplify the launching of startups and provide them financial support,[137] and the central bank launched a fintech regulatory sandbox in 2020. Still, barriers to the development of fintech persist, and Tunisia must make reforms in order to fully develop a competitive, digital economy. Tunisian fintechs report that complex bureaucratic administrative processes, an unfriendly regulatory framework and a lack of partnerships with financial institutions are impeding the development of fintech in the country.[138] The state ranks #78 of 90 economies for digital evolution momentum on the **Digital Intelligence Index (DII)**, developed by Mastercard and Tufts University's Fletcher School.

This year, the Digital Strategy 2025, which replaces Digital Tunisia 2020, was introduced. The strategy outlines ambitious goals towards encouraging digital transformation, but it remains to be seen whether it will be fully and successfully implemented. The central bank, in partnership with the French central bank, successfully conducted an experiment on the use of central bank digital currency (CBDC) in cross-border wire transfers. Going forward, a key challenge will be ensuring that digitalization promotes financial inclusion, and does not widen the digital gap. A mere 36.9% of Tunisian adults have a bank account,[139] and improvements to national digital infrastructure would be instrumental in helping them to access online banking and fintech services. A digital identity could encourage financial inclusion, but it must be accompanied by stronger data protection and cybersecurity standards. In March, the Ministry of Interior again proposed a biometric national ID and a biometric passport, but civil society strongly opposed the draft bill due to data protection and privacy concerns.[140]

Financial Regulatory Authorities

The **Central Bank of Tunisia** is Tunisia's central bank.

The **National Authority for Protection of Personal Data (the Instance)** is Tunisia's data protection agency.

Policy, Laws and Regulations

Cross-Border CBDC Experiment, 08 July 2021

The Tunisian and French central banks successfully completed a joint CBDC experiment, which conducted wire transfers between French and Tunisian commercial banks utilizing a blockchain based wholesale CBDC.[141] The solution would be invaluable in making remittances faster and cheaper. Director General of the Development and Supervision of Payment Systems and Means at the central bank, Mohamed Sadraoui, said, "This platform will likely reinforce transparency, speed and cost savings, all of which are conducive to a better inclusion of the Tunisian diaspora in Europe. The success of this experiment is an opportunity to start thinking about the deployment of alternative channels for cross-border transfers initiated by the Tunisian community in Europe to Tunisia."[142] In 2020, Tunisia received approximately USD$2.1 billion in remittances,[143] about 5.35% of its GDP.[144]

Digital Strategy 2025, 06 February 2021

The Tunisia Digital 2021-2025 strategy outlines six guidelines that aim to drive digital transformation, develop the national fintech ecosystem, promote financial inclusion and attract foreign investment. Key goals include bolstering digital literacy, developing e-payment services, expanding internet access, digitalizing government services, boosting data protection and establishing a cybersecurity policy.[145] The **Global Cybersecurity Index (GCI) 2020**, developed by the United Nations' International Telecomm-unication Union (ITU), ranks Tunisia #45 in the world—out of 194 states—for cybersecurity.

Endnotes

1 Gill, Indermit and Kenan Karakülah. "Did Africa turn a corner in 2020 or did it just dodge a bullet?" The Brookings Institution, 05 February 2021. https://www.brookings.edu/blog/future-development/2021/02/05/did-africa-turn-a-corner-in-2020-or-did-it-just-dodge-a-bullet/.

2 Holtz, Leo. "Mobile money dominates fintech investment in Africa." The Brookings Institution, 30 September 2021. https://www.brookings.edu/blog/africa-in-focus/2021/09/30/mobile-money-dominates-fintech-investment-in-africa/.

3 "African countries with the highest Gross Domestic Product (GDP) in 2021." Statista, September 2021. https://www.statista.com/statistics/1120999/gdp-of-african-countries-by-country/.

4 "The World Bank in Algeria." The World Bank, 14 June 2021. https://www.worldbank.org/en/country/algeria/overview#1.

5 Hamdi, Rania. "Algeria's health system is on the brink of implosion, as coronavirus wave hits." The Africa Report, 04 August 2021. https://www.theafricareport.com/114474/algerias-health-system-is-on-the-brink-of-implosion-as-coronavirus-wave-hits/.

6 Delort, Dorothee and Isabelle Poupaert. "How digital financial services can provide a path toward economic recovery in Algeria." World Bank Blogs, 22 February 2021. https://blogs.worldbank.org/arabvoices/how-digital-financial-services-can-provide-path-toward-economic-recovery-algeria.

7 "Fintech Development in Algeria Lags Behind MENA Counterparts." Fintechnews Africa, 02 June 2021. https://fintechnews.africa/39426/fintech-algeria/fintech-development-in-algeria-lags-behind-mena-counterparts/.

8 "Algeria Officially Launches Its First Ever Fund For Startups, Sets Up Committee For Labelling Startups." Afrikan Heroes, 03 October 2020. https://afrikanheroes.com/2020/10/03/algeria-officially-launches-its-first-ever-fund-for-startups-sets-up-committee-for-labelling-startups/.

9 "DATA PROTECTION AND CYBERSECURITY LAWS IN ALGERIA." CMS, 05 March 2021. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria.

10 « La Cosob lance le premier FinLab en Algérie. » Algerie Eco, 30 September 2021. https://www.algerie-eco.com/2021/09/30/la-cosob-lance-le-premier-finlab-en-algerie/.

11 « Présentation de la stratégie nationale de l'intelligence artificielle 2020-2030. » Algérie Presse Service, 18 January 2021. https://www.aps.dz/sante-science-technologie/116102-enseignement-superieur-presentation-de-la-strategie-nationale-de-l-intelligence-artificielle-2020-2030.

12 "Angola Economic Outlook." African Development Bank. https://www.afdb.org/en/countries/southern-africa/angola/angola-economic-outlook#:~:text=Angola's%20oil%2Ddriven%20economy%20has,an%20estimated%20120.3%25%20in%202020.&text=Lower%20oil%20export%20earnings%20will,surplus%20of%206%25%20in%202019.

13 "The World Bank in Angola." The World Bank, 01 July 2021. https://www.worldbank.org/en/country/angola/overview#1.

14 Mendes, Candido and Henrique Almeida. "Angola Hikes Key Rate to Record High to Contain Inflation." Bloomberg, 02 July 2021. https://www.bloomberg.com/news/articles/2021-07-02/angola-surprises-with-rate-hike-as-focus-shifts-to-inflation.

15 "Angola : Fourth Review Under the Extended Arrangement Under the Extended Fund Facility and Requests for Modifications of Performance Criteria and Waivers for Performance Criteria Applicability and Nonobservance-Press Release; Staff Report; and Statement by the Executive Director for Angola." International Monetary Fund, 19 January 2021. https://www.imf.org/en/Publications/CR/Issues/2021/01/19/Angola-Fourth-Review-Under-the-Extended-Arrangement-Under-the-Extended-Fund-Facility-and-50024.

16 Mendes, Candido. "Angola Resumes Restrictions as Covid Turns Deadlier Than Malaria." Bloomberg, 30 September 2021. https://www.bloomberg.com/news/articles/2021-09-30/angola-resumes-restrictions-as-covid-turns-deadlier-than-malaria.

17 Kimathi, Sharon. "Angolan National Bank and Beta-i create fintech regulatory sandbox." Fintech Futures, 18 September 2020. https://www.fintechfutures.com/2020/09/angolan-national-bank-and-beta-i-create-fintech-regulatory-sandbox/.

18 O'Grady, Vaughan. "Could M-Pesa be a way forward for financial inclusion in Angola?" Developing Telecoms, 21 June 2021. https://developingtelecoms.com/telecom-technology/financial-services/11368-could-m-pesa-be-a-way-forward-for-financial-inclusion-in-angola.html.

19 Burns, Chris. "Tech-driven start-ups deliver a boost to Angola's economy." Euronews, 22 July 2021. https://www.euronews.com/2019/12/19/tech-driven-start-ups-deliver-a-boost-to-angola-s-economy.

20 Harrison, Polly Jean. "Beta-I and the Angola National Bank Collaborate to Create First Fintech Regulatory Sandbox in Angola." The Fintech Times, 18 September 2020. https://thefintechtimes.com/beta-i-and-the-angola-national-bank-collaborate-to-create-first-fintech-regulatory-sandbox-in-angola/.

21 Massala, Guilherme. "Launch of mobile payments system in Angola scheduled for October." Menos Fios, 28 May 2021. https://www.menosfios.com/en/launch-of-mobile-payment-system-in-angola-scheduled-for-october/.

22 "Angola prepares to launch biometric passport." Xinhua, 02 June 2021. http://www.xinhuanet.com/english/africa/2021-06/02/c_139985648.htm.

23 Geto, Daniel. "National Bank of Angola is considering the implementation of digital currencies." Menos Fios, 12 June 2021. https://www.menosfios.com/en/Angola%27s-national-bank-is-considering-the-implementation-of-digital-currencies/.

24 "National Bank of Angola assesses risk of joining 'Blockchain'." Further Africa, 02 October 2020. https://furtherafrica.com/2020/10/02/national-bank-of-angola-assesses-risk-of-joining-blockchain/.

25 "The World Bank in Côte d'Ivoire." The World Bank, 03 May 2021. https://www.worldbank.org/en/country/cotedivoire/overview#1.

26 de Bassompierre, Leanne. "IMF Expects Ivory Coast Economy to Expand About 6.5% This Year." Bloomberg, 24 March 2021. https://www.bloomberg.com/news/articles/2021-03-24/imf-expects-ivory-coast-economy-to-expand-about-6-5-this-year-kmnbuakd.

27 "The World Bank in Côte d'Ivoire." The World Bank, 03 May 2021. https://www.worldbank.org/en/country/cotedivoire/overview#1.

28 "CÔTE D'IVOIRE." International Monetary Fund. https://www.imf.org/en/Countries/CIV.

29 "New opportunities for ICT start-ups in Côte d'Ivoire." Oxford Business Group. https://oxfordbusinessgroup.com/overview/upwardly-mobile-quality-and-availability-digital-services-continues-rise-bringing-new-opportunities.

30 Riquet, Corinne and Max Mattern. "Regulations Drive Success of Digital Finance in Côte d'Ivoire." Consultative Group to Assist the Poor, 02 July 2019. https://www.cgap.org/blog/regulations-drive-success-digital-finance-cote-divoire.

31 "Côte d'Ivoire Population (LIVE)." Worldometer. https://www.worldometers.info/world-population/cote-d-ivoire-population/.

32 "Cote d'Ivoire: Orange's Digital Bank Hits 500,000 Users in Cote d'Ivoire - Further Roll-Outs Planned." AllAfrica, 30 July 2021. https://allafrica.com/stories/202105030687.html.

33 Banda, Manda. "ITFC and BCEAO explore digital currencies." Intelligent CIO, 22 February 2021. https://www.intelligentcio.com/africa/2021/02/22/itfc-and-bceao-explore-digital-currencies/.

34 "Ghana country profile." BBC, 11 December 2020. https://www.bbc.co.uk/news/world-africa-13433790.

35 "The World Bank in Ghana." The World Bank, 15 April 2021. https://www.worldbank.org/en/country/ghana/overview.

36 "The World Bank in Ghana." The World Bank, 15 April 2021. https://www.worldbank.org/en/country/ghana/overview.

37 Larnyoh, Magdalene Teiko. "Fitch Solutions projects Ghana's economy to be the fastest-growing in Sub-Saharan Africa in 2021." Business Insider Africa, 21 July 2021. https://africa.businessinsider.com/local/markets/fitch-solutions-projects-ghanas-economy-to-be-the-fastest-growing-in-sub-saharan/r34qt51.

38 Chabry, Anthony Xavier. "Ghana's digitalization revolution, a catalyst for economic development." Face2Face Africa, 11 July 2021. https://face2faceafrica.com/article/ghanas-digitalization-revolution-a-catalyst-for-economic-development.

39 "Finnovating for Africa 2021: Reimagining the African financial services landscape." Disrupt Africa. https://disrupt-africa.com/finnovating-for-africa/.

40 Collins, Tom. "Kenya and Ghana lead world in mobile money." *African Business*, 26 July 2021. https://african.business/2021/07/technology-information/kenya-and-ghana-lead-world-in-mobile-money/.

41 "Share of population with an account at a financial institution in Ghana from 2018 to 2021." Statista, February 2021. https://www.statista.com/statistics/1176015/bank-account-owners-ghana/.

42 "Ghana Poverty Assessment." The World Bank, 2020. https://openknowledge.worldbank.org/handle/10986/34804.

43 "Press Release: Bank of Ghana partners with Giesecke+Devrient to pilot first general purpose Central Bank Digital Currency in Africa." Bank of Ghana, 11 August 2021. https://www.bog.gov.gh/wp-content/uploads/2021/08/CBDC-Joint-Press-Release-BoG-GD-3.pdf.

44 "Ghana: VP Bawumia Unveils One-Stop Portal Ghana.gov." AllAfrica, 15 July 2021. https://allafrica.com/stories/202107150827.html.

45 "Press Release: Bank of Ghana Sandbox Pilot." Bank of Ghana. https://www.bog.gov.gh/wp-content/uploads/2021/02/PRESS-RELEASE-BANK-OF-GHANA-SANDBOX-PILOT.pdf.

46 "The Start of a New Era in Ghana's Anti-Money Laundering Enforcement." Lexology, 18 March 2021. https://www.lexology.com/library/detail.aspx?g=bbbafc17-b863-4f49-aa7f-8b75fc08a098.

47 "Ghana's Anti-Money Laundering Act 2020, Act 1044." N. Dowuona & Company, 12 April 2021. https://www.ndowuona.com/insights/105-anti-money-laundering-act-2020-act-1044.

48 "Ghana is off the FATF 'grey list' - Finance Minister." GhanaWeb, 01 July 2021. https://www.ghanaweb.com/GhanaHomePage/business/Ghana-is-off-the-FATF-grey-list-Finance-Minister-1298923.

49 "Ghana Introduces Cybersecurity Act." Lexology, 25 May 2021. https://www.lexology.com/library/detail.aspx?g=ca5cb51c-7b36-4943-ac81-f5ccfd2e0370.

50 "The World Bank in Kenya." The World Bank, 30 March 2021. https://www.worldbank.org/en/country/kenya/overview.

51 Herbling, David. "Kenya Sees Economy Expanding at Fastest Pace in a Decade." Bloomberg, 05 August 2021. https://www.bloomberg.com/news/articles/2021-08-05/kenya-forecasts-economy-to-expand-at-fastest-pace-in-a-decade.

52 "Kenya." International Monetary Fund, 23 June 2021. https://www.imf.org/en/Countries/KEN.

53 "The World Bank in Kenya." The World Bank, 30 March 2021. https://www.worldbank.org/en/country/kenya/overview.

54 "Kenya Economic Update: COVID-19 Erodes Progress in Poverty Reduction in Kenya, Increases Number of Poor Citizens." The World Bank, 25 November 2020. https://www.worldbank.org/en/country/kenya/publication/kenya-economic-update-covid-19-erodes-progress-in-poverty-reduction-in-kenya-increases-number-of-poor-citizens.

55 Chitavi, Mike et al. "Kenya Is Becoming a Global Hub of FinTech Innovation." *Harvard Business Review*, 18 February 2021. https://hbr.org/2021/02/kenya-is-becoming-a-global-hub-of-fintech-innovation.

56 "Mobile money revolutionises Kenyan fintech." *Global Business Outlook*, 15 June 2021. https://www.globalbusinessoutlook.com/mobile-money-revolutionises-kenyan-fintech/.

57 "Finnovating for Africa 2021: Reimagining the African financial services landscape." Disrupt Africa. https://disruptafrica.gumroad.com/l/razjs.

58 Creemers, Tijsbert et al. "Five Strategies for Mobile-Payment Banking in Africa." Boston Consulting Group, 13 August 2020. https://www.bcg.com/en-gb/publications/2020/five-strategies-for-mobile-payment-banking-in-africa?mc_cid=9db89d0f52&mc_eid=e740b6a321.

59 "Finnovating for Africa 2021: Reimagining the African financial services landscape." Disrupt Africa. https://disruptafrica.gumroad.com/l/razjs.

60 Wambui, Mary. "Kenya ranked among world's major money laundering, fraud hotbeds." *Nairobi News*, 10 March 2021.

61 "Kenya Replaces Insurance Cards With Fingerprint Biometrics." Find Biometrics, 09 July 2021. https://findbiometrics.com/kenya-replaces-insurance-cards-with-fingerprint-biometrics-070904/.

62 Okoth, Jackson. "CBK Holds Discussions on Digital Currencies." *The Kenyan Wall Street*, 07 June 2021. https://kenyanwallstreet.com/cbk-in-discussions-over-digital-currency/.

63 "The Capital Markets Soundness Report (CMSR) Volume XVIII, Quarter 1 2021." The Capital Markets Authority, April 2021. https://www.cma.or.ke/index php?option=com_content&view=article&id=705:the-capital-markets-soundness-report-cmsr-volume-xviii-quarter-1-2021&catid=12:-press-center&Itemid=207.

64 Kaaru, Steve. "Kenya leads in global P2P volume for second year in a row." CoinGeek, 16 September 2021. https://coingeek.com/kenya-leads-in-global-p2p-volume-for-second-year-in-a-row/.

65 Onyango, Conrad. “Kenyans lead the world in peer to peer crypto trade.” *Quartz Africa*, 23 August 2021. https://qz.com/africa/2050735/kenyans-lead-the-world-in-peer-to-peer-crypto-trade/.

66 “Kenya National Payments System Vision and Strategy 2021-2025.” Central Bank of Kenya. https://www.centralbank.go.ke/wp-content/uploads/2020/12/CBK-NPS-Vision-and-Strategy.pdf.

67 Okwara, Elias. “Kenya appoints its first ever data protection commissioner.” The International Association of Privacy Professionals, 01 December 2020. https://iapp.org/news/a/kenya-appoints-its-first-ever-data-protection-commissioner/.

68 “GDP growth (annual %) – Morocco.” The World Bank. https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=MA.

69 “THE IMPACT OF COVID-19 ON POVERTY IN MOROCCO.” The Borgen Project. https://borgenproject.org/covid-19-and-poverty-in-morocco/.

70 “Morocco.” International Monetary Fund. https://www.imf.org/en/Countries/MAR.

71 “2020 | Evaluation report.” OECD. https://www.oecd.org/derec/italy/italy-evaluation-tous-au-tour-enfance-morocco-2020.pdf.

72 Billah, Azzedine El Mountassir. “Mobile payment and financial inclusion in Morocco.” The Parliament, 20 November 2020. https://www.theparliamentmagazine.eu/news/article/mobile-payment-and-financial-inclusion-in-morocco.

73 Faridi, Omar. “Morocco Is Now Home to Many Fintech Services, Crowdfunding, Lending, Advanced Data Analytics Platforms: Report.” Crowdfund Insider, 19 April 2021. https://www.crowdfundinsider.com/2021/04/174365-morocco-is-now-home-to-many-fintech-services-crowdfunding-lending-advanced-data-analytics-platforms-report/.

74 “Expanding digital and financial inclusion: World Bank supports Morocco’s reforms for social and economic resilience.” The World Bank, 17 June 2021. https://www.worldbank.org/en/news/press-release/2021/06/17/world-bank-supports-morocco-reforms-for-social-and-economic-resilience.

75 Alouazen, Sanae. “Morocco, Luxembourg Sign Memorandum on Digital Transition.” Morocco World News, 27 January 2021. https://www.moroccoworldnews.com/2021/01/333427/morocco-luxembourg-sign-memorandum-on-digital-transition.

76 “Morocco’s central bank confirms exploring digital currency.” Ledger Insights, 25 February 2021. https://www.ledgerinsights.com/morocco-central-bank-confirms-exploring-digital-currency-cbdc/.

77 https://www.ledgerinsights.com/morocco-central-bank-confirms-exploring-digital-currency-cbdc/.

78 Alouazen, Sanae. “Morocco, Luxembourg Sign Memorandum on Digital Transition.” Morocco World News, 27 January 2021. https://www.moroccoworldnews.com/2021/01/333427/morocco-luxembourg-sign-memorandum-on-digital-transition.

79 “Israel tightens ties with Morocco: Cooperation in academia, agriculture and fintech.” Middle East in 24, 13 August 2021. https://middleeast.in-24.com/News/153231.html.

80 “The World Bank in Nigeria.” The World Bank, 03 November 2020. https://www.worldbank.org/en/country/nigeria/overview#1.

81 “Nigeria Economic Update: Resilience through Reforms.” The World Bank, 15 June 2021. https://www.worldbank.org/en/country/nigeria/publication/nigeria-economic-update-resilience-through-reforms.

82 “FAULT LINES WIDEN IN THE GLOBAL RECOVERY.” International Monetary Fund, July 2021. https://www.imf.org/en/Publications/WEO/Issues/2021/07/27/world-economic-outlook-update-july-2021.

83 Nwokoma, Chimgozirim. “Over 150 Nigerian fintech startups reportedly generate annual revenues of over $5 million.” Techpoint Africa, 11 May 2021. https://techpoint.africa/2021/05/11/nigerian-fintech-startups-revenue/.

84 Hodgson, Leah. “Is Africa fintech’s next frontier?” PitchBook, 06 August 2021. https://pitchbook.com/news/articles/Africa-fintech-startups-unicorns.

85 Kanife, Eljike. “Nigeria’s Opay is the only African fintech listed in the 2021 Top 250 by CB Insights.” Technext, 11 October 2021. https://technext.ng/2021/10/11/nigerias-opay-is-the-only-african-fintech-listed-in-the-2021-top-250-by-cb-insights/.

86 Ayileka, Ayomide. “Regulating Fintech space: Promoting innovation or stifling growth?” The Nation, 11 October 2021. https://thenationonlineng.net/regulating-fintech-space-promoting-innovation-or-stifling-growth/.

87 “Community-led approaches to connectivity: How CITAD is bridging the digital divide in northern Nigeria.” Association for Progressive Communications, 26 August 2021. https://www.apc.org/en/node/37551.

88 “Mobile internet user penetration in Nigeria from 2016 to 2026.” Statista, 11 July 2021. https://www.statista.com/statistics/972900/internet-user-reach-nigeria/.

89 Uba, Josephine. “Nigeria: The Most Serious Cyber Security Threats Facing Businesses In Nigeria And How To Mitigate Them.” Mondaq, 23 August 2021. https://www.mondaq.com/nigeria/security/1104438/the-most-serious-cyber-security-threats-facing-businesses-in-nigeria-and-how-to-mitigate-them.

90 Iruoma, Kelechukwu. “Nigerians are pushing back on a new law that mandates linking their national identity numbers to their mobile numbers.” Thomson Reuters Foundation News, 05 August 2021. https://news.trust.org/item/20210805104557-zunak.

91 Diya, Olubusola Oyeyosola et al. “Nigeria: Fintech Half-Year Review 2021 – Recent Regulatory And Legal Developments In Nigeria.” Mondaq, 05 August 2021. https://www.mondaq.com/nigeria/fin-tech/1098176/fintech-half-year-review-2021-recent-regulatory-and-legal-developments-in-nigeria?type=popular.

92 “Nigerian central bank to launch digital currency within days – governor.” Reuters, 07 October 2021. https://www.reuters.com/technology/nigerian-central-bank-launch-digital-currency-within-days-governor-2021-10-07/.

93 Ohuocha, Chijioke and Libby George. “Crypto trading thrives in Nigeria despite official disapproval.” Reuters, 12 October 2021. https://www.reuters.com/article/crypto-currency-nigeria/crypto-trading-thrives-in-nigeria-despite-official-disapproval-idUSL8N2R31LA.

94 Diya, Olubusola Oyeyosola et al. “Nigeria: Fintech Half-Year Review 2021 – Recent Regulatory And Legal Developments In Nigeria.” Mondaq, 05 August 2021. https://www.mondaq.com/nigeria/fin-tech/1098176/fintech-half-year-review-2021-recent-regulatory-and-legal-developments-in-nigeria?type=popular.

95 Onaleye, Tomiwa. “CBN’s BVN Verification Ban: What it Means for Nigerian Fintechs and their Customers.” Technext, 09 April 2021. https://technext.ng/2021/04/09/cbns-bvn-verification-ban-what-it-means-for-nigerian-fintechs-and-their-customers/.

96 "Issuance of Regulatory Framework for Open Banking in Nigeria." Central Bank of Nigeria, 17 February 2021. https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf.

97 "Nigerian Crypto Ban Hasn't Ended Use of Digital Currency." PYMNTS, 12 October 2021. https://www.pymnts.com/cryptocurrency/2021/nigerian-crypto-ban-hasnt-ended-use-of-digital-currency/.

98 Avan-Nomayo, Osato. "Nigeria's SEC says central bank's crypto ban disrupted the market." Cointelegraph, 16 April 2021. https://cointelegraph.com/news/nigeria-s-sec-says-central-bank-s-crypto-ban-disrupted-the-market.

99 Beaubien, Jason. "The Country With The World's Worst Inequality Is ..." NPR, 02 April 2018. https://www.npr.org/sections/goatsandsoda/2018/04/02/598864666/the-country-with-the-worlds-worst-inequality-is.

100 "The World Bank in South Africa." The World Bank, 18 March 2021. https://www.worldbank.org/en/country/southafrica/overview.

101 Warah, Rasna. "COVID-19 has exposed South Africa's glaring and enduring inequalities." One, 02 August 2021. https://www.one.org/africa/blog/covid19-exposed-south-africa-inequalities/.

102 Devermont, Judd and Marielle Harris. "Digital Africa: Leveling Up through Governance and Trade." Center for Strategic & International Studies, 09 June 2021. https://www.csis.org/analysis/digital-africa-leveling-through-governance-and-trade.

103 Mlaba, Khanyi. "How Is South Africa's Digital Divide Making Inequality Worse in the Country?" Global Citizen, 03 August 2021. https://www.globalcitizen.org/en/content/south-africa-digital-divide-makes-inequality-worse/.

104 Ventura, Luca. "World's Most Unbanked Countries 2021." Global Finance, 17 February 2021. https://www.gfmag.com/global-data/economic-data/worlds-most-unbanked-countries.

105 "South Africa's consumer appetite for digital payments takes off, Mastercard study finds." *The Paypers*, 07 May 2021. https://thepaypers.com/mobile-payments/south-africas-consumer-appetite-for-digital-payments-takes-off-mastercard-study-finds--1248865#.

106 Macdonald, Ayang. "Delays persist in South Africa's automated biometric identification project completion." Biometric Update, 16 March 2021. https://www.biometricupdate.com/202103/delays-persist-in-south-africas-automated-biometric-identification-project-completion.

107 "BIS Innovation Hub and central banks of Australia, Malaysia, Singapore and South Africa will test CBDCs for international settlements." Bank for International Settlements, 02 September 2021. https://www.bis.org/press/p210902.htm.

108 "South Africa." Remitscope. https://remitscope.org/africa/south_africa.

109 Bowan, Nerushka. "After 7-year wait, South Africa's Data Protection Act enters into force." International Association of Privacy Professionals, 01 July 2020. https://iapp.org/news/a/after-a-7-year-wait-south-africas-data-protection-act-enters-into-force/.

110 "Transfer of Personal Information out of South Africa." POPI Act Compliance. https://www.popiact-compliance.co.za/popia-information/14-transfer-of-personal-information-out-of-south-africa.

111 Bowan, Nerushka. "After 7-year wait, South Africa's Data Protection Act enters into force." International Association of Privacy Professionals, 01 July 2020. https://iapp.org/news/a/after-a-7-year-wait-south-africas-data-protection-act-enters-into-force/.

112 "Position Paper on Crypto Assets." Intergovernmental Fintech Working Group – Crypto Assets Regulatory Working Group, 11 June 2021. https://www.resbank.co.za/content/dam/sarb/publications/media-releases/2021/fintech/IFWG%20CAR%20WG%20Position%20paper%20on%20crypto%20assets.pdf.

113 Henderson, Roxanne and Prinesha Naidoo. "South Africa Moves to Tighten Crypto Regulation After Scams." Bloomberg, 29 June 2021. https://www.bloomberg.com/news/articles/2021-06-29/regulatory-clock-ticks-for-cryptocurrency-assets-in-south-africa.

114 Karombo, Tawanda. "In crypto, South Africa is forging a different path than the rest of Africa." *Quartz Africa*, 17 June 2021. https://qz.com/africa/2021680/south-africa-approach-to-bitcoin-regulation-is-unique-in-africa/.

115 Pickworth, Evan. "PODCAST | What are the implications of the recently enacted Cybercrimes and Cybersecurity Act?" Business Day, 02 July 2021. https://www.businesslive.co.za/bd/companies/telecoms-and-technology/2021-07-02-podcast-what-are-the-implications-of-the-recently-enacted-cybercrimes-and-cybersecurity-act/.

116 "The World Bank in Tanzania." The World Bank. https://www.worldbank.org/en/country/tanzania/overview.

117 "The World Bank in Tanzania." The World Bank. https://www.worldbank.org/en/country/tanzania/overview.

118 "Tanzania Has an Opportunity to Ignite Inclusive Economic Growth by Transforming Its Tourism Sector." The World Bank, 29 July 2021. https://www.worldbank.org/en/news/press-release/2021/07/29/tanzania-has-an-opportunity-to-ignite-inclusive-economic-growth-by-transforming-its-tourism-sector.

119 "1.7 Billion Unbanked - Leadership Vanguard explores financial inclusion in Tanzania." Xynteo, 08 May 2019. https://xynteo.com/insights/latest/17-billion-unbanked-leadership-vanguard-explores-financial-inclusion-tanzania.

120 Kemp, Simon. "DIGITAL 2021: TANZANIA." DataReportal, 21 February 2021. https://datareportal.com/reports/digital-2021-tanzania.

121 "Mapping the Tanzanian Fintech Start-up Landscape." United Nations Capital Development Fund, 27 May 2021. https://www.uncdf.org/article/6789/mapping-the-tanzanian-fintech-start-up-landscape#:~:text=The%20assessment%20identified%2033%20fintech,finance%2C%20investments%2C%20and%20insurance.

122 Drake, Ed. "Tanzania president urges central bank to consider digital currency." *CoinGeek*, 18 June 2021. https://coingeek.com/tanzania-president-urges-central-bank-to-consider-digital-currency/.

123 Thomson, Mpoki. "Tanzania: Digital Economy Blueprint Coming." AllAfrica, 17 June 2021. https://allafrica.com/stories/202106170981.html.

124 "Tanzania: World Bank supports expanded access to opportunities and services, especially for women and youth." The World Bank, 27 May 2021. https://www.worldbank.org/en/news/press-release/2021/05/27/tanzania-world-bank-supports-expanded-access-to-opportunities-and-services-especially-for-women-and-youth.

125 O'Grady, Vaughan. "Tanzania reduces mobile money transaction levy." Developing Telecoms, 02 September 2021. https://developingtelecoms.com/telecom-business/telecom-regulation/11829-tanzania-reduces-mobile-money-transaction-levy.html.

126 Minja, Dativa. "Tanzania: BoT to Pilot New Payment System." AllAfrica, 10 July 2021. https://allafrica.com/stories/202107100102.html.

127 Mirondo, Rosemary. "How sending cash will be easier, cheaper from July." The Citizen, 12 February 2021. https://www.thecitizen.co.tz/tanzania/news/business/how-sending-cash-will-be-easier-cheaper-from-july-3289274.

128 "Payment Systems Initiatives." Bank of Tanzania. https://www.bot.go.tz/PaymentSystem/Initiatives.

129 Mirondo, Rosemary. "How sending cash will be easier, cheaper from July." *The Citizen*, 12 February 2021. https://www.thecitizen.co.tz/tanzania/news/business/how-sending-cash-will-be-easier-cheaper-from-july-3289274.

130 Shome, Arnab. "Tanzanian President Urges Central Bank to Prepare for Crypto." *Finance Magnates*, 14 June 2021. https://www.financemagnates.com/cryptocurrency/news/tanzanian-president-urges-central-bank-to-prepare-for-crypto/.

131 Dausen, Nuzulack. "Tanzania cbank says it is working on president's cryptocurrency push." *Reuters*, 25 June 2021. https://www.reuters.com/technology/tanzania-cbank-says-it-is-working-presidents-cryptocurrency-push-2021-06-25/.

132 "The World Bank in Tunisia." The World Bank, 21 June 2021. https://www.worldbank.org/en/country/tunisia/overview#1.

133 "Tunisia." International Monetary Fund. https://www.imf.org/en/Countries/TUN.

134 "The World Bank in Tunisia." The World Bank, 21 June 2021. https://www.worldbank.org/en/country/tunisia/overview#1.

135 Amara, Tarek. "Thousands protest against Tunisia leader with government awaited." Reuters, 10 October 2021. https://www.reuters.com/world/africa/thousands-protest-against-tunisia-leader-with-government-awaited-2021-10-10/.

136 "The Tunisian Startup Act." The Carnegie Endowment for International Peace, 26 June 2018. https://carnegieendowment.org/sada/76685.

137 Hinrichsen, Simone. "Exploring the Rising Tunisian Start-up Ecosystem." GSMA, 02 November 2020. https://www.gsma.com/mobilefordevelopment/blog/exploring-the-rising-tunisian-start-up-ecosystem/.

138 Amara, Ismail. "Fintech, a new horizon." TIMUN, 05 May 2021. https://timun.tn/2021/03/05/fintech-a-new-horizon/.

139 "The World's Unbanked Population." Acuant, 25 November 2020. https://www.acuant.com/blog/the-worlds-unbanked-population/.

140 "Statement: Tunisia's newly proposed biometric ID and e-passport threaten privacy." Access Now, 09 March 2021. https://www.accessnow.org/tunisia-biometric-id-passport-threaten-privacy/.

141 "Central banks of France, Tunisia in wholesale cross border CBDC trial." Ledger Insights, 19 July 2021. https://www.ledgerinsights.com/central-bank-of-france-tunisia-in-wholesale-cross-border-cbdc-trial/.

142 "Central Bank of Tunisia tests CBDC pilot with Central Bank of France." Unlock, 14 July 2021. https://www.unlock-bc.com/news/2021-07-14/central-bank-of-tunisia-tests-cbdc-pilot-with-central-bank-of-france/.

143 "Personal remittances, received (current US$)." The World Bank. https://data.worldbank.org/indicator/BX.TRF.PWKR.CD.DT?locations=TN.

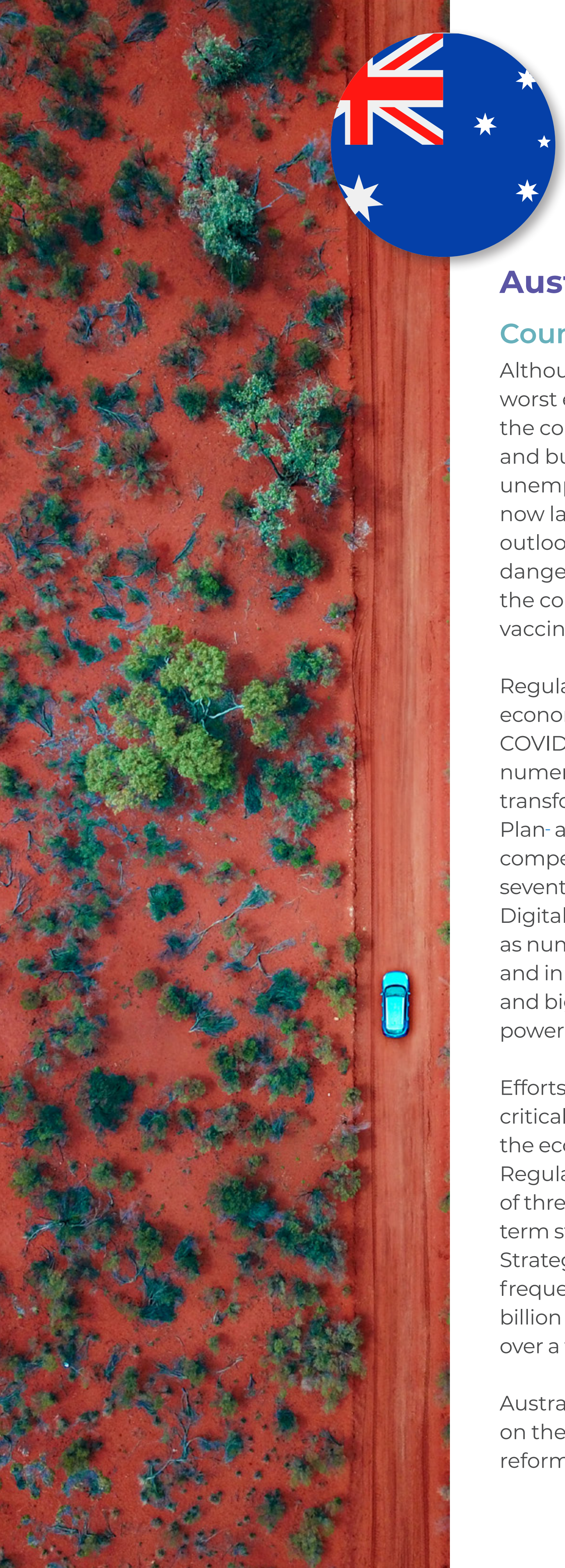
144 "Personal remittances, received (% of GDP) – Tunisia." The World Bank. https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=TN.

145 "National strategic plan 'Tunisia Digital 2021-2025,' being finalised (official)." Tunis Daily News, 01 April 2021. http://www.tdailynews.net/storyad-z12562030.

Asia-Pacific

Dynamic Asia-Pacific is home to some of the world's most exciting fintech hotspots, from established hubs like Singapore and Sydney to up-and-coming ecosystems across India and Southeast Asia. Surges in e-commerce and digital payments amidst the COVID-19 pandemic, friendly regulatory environments and steep competition made 2020 and 2021 big years for fintech growth across the region, and this development is only set to continue. Young and tech-savvy populations from India to Vietnam have accelerated the uptake of digital solutions, and even in the rapidly aging South

Korea, contactless culture has progressed at breakneck pace. In emerging markets like India, Indonesia, Malaysia, Thailand and Vietnam, digital transformation has been particularly accentuated, and regulators, financial institutions and startups are keen to develop and adopt innovative technologies such as artificial intelligence and blockchain. Innovation in payments will be an especially important area to watch. Australia, Hong Kong, India, Japan, Malaysia, New Zealand, Taiwan and Thailand are exploring central bank digital currency (CBDC), which would revolutionize payment systems and promote financial inclusion. Central banks hope that CBDC will draw interest away from privately-issued digital currencies, which are being increasingly regulated in Asia-Pacific. Dovetailing with digital transformation, data protection regulations are being enacted and strengthened throughout the region, just three years after the EU's General Data Protection Regulation (GDPR) went into effect.



Australia

Country Overview

Although Australia's GDP contracted by 1.1% in 2020,[1] its worst economic performance in almost three decades,[2] the country has had a swift and strong recovery. Consumer and business spending are high, exports are booming, unemployment has dipped to 5.1%[3] and the economy is now larger than it was pre-pandemic.[4] Australia's promising outlook is at risk, however, as a June 2021 outbreak of the dangerous COVID-19 Delta variant placed about half of the country's population under lockdown,[5] and a slow vaccination rate has compounded this uncertain landscape.

Regulators must accelerate the digitalization of the economy in order to secure Australia's recovery from the COVID-19 pandemic. The government has spearheaded numerous initiatives aimed at bolstering Australia's digital transformation, such as the Artificial Intelligence (AI) Action Plan and the Digital Economy Strategy, as the country's competitiveness has lagged in recent years. Australia ranked seventeenth in the world for its digital economy on the 2020 Digital Intelligence Index, a downgrade from its 2017 ranking as number eleven.[6] Greater investments in digital talent and innovative technologies like cloud, internet of things and big data could help the country contend with digital powerhouses such as the EU, Korea, Singapore and Taiwan.

Efforts toward strengthening cybersecurity will be especially critical in safeguarding financial stability and future-proofing the economy. In April 2021, the Australian Prudential Regulation Authority (APRA) identified cybersecurity as one of three main areas integral to the financial sector's long-term strength and resilience.[7] The national Cyber Security Strategy, released in August 2020 amidst increasingly frequent and sophisticated cyberattacks, allocates AU$1.67 billion (approximately USD$1.25 billion) towards cybersecurity over a ten-year period.

Australia's ambitious 2021 digital agenda also focuses on the expansion of the national digital identity scheme, reforms to the anti-money laundering and counter-terrorist financing framework and amendments to the Consumer Data Right framework. The Reserve Bank of Australia has been investigating the risks and benefits of issuing a central bank digital currency (CBDC). In November, the central bank partnered with Commonwealth Bank, National Australia Bank, financial services company Perpetual and blockchain software technology company ConsenSys to launch a project exploring a DLT-based, wholesale CBDC.

Financial Regulatory Authorities

The **Reserve Bank of Australia (RBA)** is Australia's central bank, charged with issuing the country's currency and maintaining economic stability. The Reserve Bank's Payments System Board governs and develops payments system policy.

The **Australian Competition and Consumer Commission (ACCC)** is a regulatory commission operating under the Department of the Treasury. The Commission is mandated with protecting consumer and business rights, industry regulation, and preventing anti-competitive market and business practices.

The **Australian Securities and Investments Commission (ASIC)** is the supervisory body overseeing the country's securities market. The commission primarily enforces trading practices and laws against misconduct in the financial sector.

The **Australian Prudential Regulatory Authority (APRA)** promotes financial stability and supervises institutions in the banking and insurance sectors.

The **Council of Financial Regulators (CFR)** is an independent coordinating body for the Country's main financial regulatory agencies. The members are the RBA, ASIC, the Australian Prudential Regulatory Authority (APRA), and the Department of the Treasury.

The **Department of the Treasury** is Australia's main economic policymaker. The Treasury is also responsible for the nation's federal budget and market regulation.

The **Office of the Australian Information Commissioner's (OAIC)** is the national data protection agency that enforces the country's Privacy Act and other related privacy laws. The commission dispenses guidance to entities regarding Privacy Act compliance.

Policy, Laws and Regulations

Non-Bank Lending and Financing Sector Risk Assessment, 24 June 2021

The Australian Transaction Reports and Analysis Centre (AUSTRAC) published its *Non-Bank Lending and Financing Sector Risk Assessment* for money laundering and terrorist financing. AUSTRAC designates the overall threat of money laundering and terrorist financing to the non-bank lending and financing sector to be at a medium level, while terrorist financing alone presents a low threat. The principal threat to the sector is fraud, especially loan application fraud, identity fraud and welfare fraud. Main vulnerabilities include cash deposits facilitated through third-party branches or agents, online delivery channels and a low rate of direct customer interaction. Cash deposits facilitated through third-party branches or agents limits institutions' ability to conduct oversight and detect suspicious activity, particularly when the transaction falls below the transaction reporting threshold. Although individuals present a lower risk of money laundering and terrorist financing than do non-individuals, a low rate of direct customer interaction further inhibits institutions from conducting oversight and lowers transparency. The increased use of online delivery channels has also complicated the threat landscape as it facilitates cyber fraud, as with the cases of fraudulent loan applications.

Action Plan for Artificial Intelligence, 17 June 2021

The government released the AI Action Plan, which outlines measures towards making Australia a global leader in the development and adoption of "trusted, secure and responsible AI." The four focus areas towards achieving this goal include:

- "Developing and adopting AI to transform Australian businesses
- Creating an environment to grow and attract the world's best AI talent
- Using cutting edge AI technologies to solve Australia's national challenges
- Making Australia a global leader in responsible and inclusive AI"[8]

The action plan includes a AU$124.1 million (approximately USD$93 million) investment towards implementation of the measures, alongside the establishment of a National AI Centre, four Capability Centres and a Next Generation AI Graduate program.

AML/CTF Reforms, 15 June 2021

The Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument 2021 (No. 1) was registered in the federal register of legislation. The instrument implements some of the changes made by the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020 by amending several chapters of the AML/CTF framework. Amendments to Chapter 3 on correspondent banking now require a correspondent to assess ML/TF risks of a correspondent banking relationship when conducting initial due diligence, as well as ongoing due diligence. Amendments to Chapter 6 specify the requirements for a reporting entity when there is suspicion as to the veracity or adequacy of previously obtained information per customer due diligence and know-your-customer (KYC). The reporting entity must take swift measures to gather and obtain additional KYC information, and update and verify existing KYC information. Amendments to Chapter 7 (reliance on third parties) expand the procedures that may be utilized for customer identification. Per the explanatory statement accompanying the instrument, "These are customer due diligence procedures that have been carried out by another person in accordance with one or more laws of a foreign country. The foreign law or laws must give effect to the FATF Recommendations relating to the identification and verification of customers, beneficial owners and agents, and record-keeping of these procedures."

Data-Matching Program Regarding Cryptocurrency Designated Service Providers, 08 June 2021

The notice "Commissioner of Taxation – Notice of a data-matching program - Cryptocurrency 2020-21 to 2022-23 financial years" was published in the federal register of legislation. The notice announces that the Australian Taxation Office (ATO) will acquire account identification and transaction data from cryptocurrency designated service providers for 2021 through 2023, as an extension of the data-matching program first launched in April of 2019. The data to be obtained includes client identification details and transaction details. The ATO has expressed concern that the anonymity in the trade of crypto assets has facilitated tax evasion.

Proposed Updates to the ePayments Code, 21 May 2021

The Australian Securities and Investments Commission (ASIC) published a consultation paper detailing proposed updates to the ePayments Code, "a voluntary code of practice that regulates electronic payments." ASIC proposes to make the code mandatory, allow the authority to conduct "targeted ad hoc monitoring of compliance," extend the code to small businesses and incorporate biometric authentication into the code. Biometric authentication would be defined and incorporated due to the increasing use of biometrics (e.g., fingerprints) in the authentication of transactions. The current code does not mention biometric authentication, as it was not widely utilized the last time the code was reviewed. The updated ePayments Code is expected to be released in late 2021.

Government Launches Digital Economy Strategy, 06 May 2021

As part of the 2021 Federal Budget, the government launched the Digital Economy Strategy, which allocates AUS $1.2 billion (approximately USD$901 million) towards digitalization policies and actions. The government aims to become a "modern and leading digital economy by 2030." Initiatives include:

- "Over [AU]$100 million to support digital skills for Australians
- Building Australia's capability in Artificial Intelligence
- Enhancing Government services
- Investment incentives
- Helping small and medium businesses
- Unlocking the value of data in the economy
- Strengthening safety, security and trust"[9]

The government will also seek to bolster **cybersecurity** by:

- Allocating AU$43.8 million (approximately USD$32.9 million) towards expanding the Cyber Security Skills Partnership Innovation Fund
- Establishing a 'Secure G' Connectivity Test Lab "in partnership with the private sector to trial innovative approaches to network security and data protections"[10]
- Creating a National Data Security Action Plan that establishes a roadmap for the development of clear data security standards
- Piloting three Cyber Hubs "to enable leading agencies such as Defence, Home Affairs and Services Australia to provide cyber services for those agencies that cannot match their breadth and depth of skills"[11]

The Australian government has been especially keen to digitalize its services, promote digitalization in the private sector and invest in innovative technologies. Per the **Digital Transformation Strategy**, launched in 2018, Australia seeks to become one of the globe's top three digital governments by 2025.

Updated New Payments Platform Roadmap, 29 April 2021

The Australian New Payments Platform (NPP) issued its updated New Payments Platform (NPP) Roadmap, along with updates on its increasing use. The NPP, launched in February 2018, is an open access infrastructure designed to facilitate near real-time, 24/7 payments in Australia. As of April 2021, 2.2 million transactions are conducted per day on the NPP, and it is utilized by over 105 financial institutions. The Updated NPP Roadmap addresses the progress in the development of a capability that enables customers to authorize third parties to initiate payments from their bank accounts, using the NPP. Due to numerous factors, including the COVID-19 pandemic, the implementation date is expected to be in early-to-mid-2022.

Update to Victoria's e-Signature Law, 23 March 2021

The state of Victoria passed the Justice Legislation Amendment (System Enhancements and Other Matters) Bill 2021, which amends the Electronic Transactions (Victoria) Act 2000 and allows for the electronic signing and remote witnessing of legal documents. Documents include deeds, mortgages, wills and powers of attorney. The law makes permanent emergency measures that were temporarily instituted due to the COVID-19 pandemic. It went into effect 26 April 2021.

Cyber Operational Resilience Intelligence-Led Exercises Framework, 07 December 2020

The Council of Financial Regulators (CFR) unveiled its Cyber Operational Resilience Intelligence-Led Exercises (CORIE) pilot program guideline for financial institutions in Australia. The

---

Victoria's amended law is progressive in that it permanently allows electronic signatures and remote witnessing to be used for critical estate planning documents, including wills and powers of attorney. Globally, many jurisictions have been slow to permit e-signatures for such documents—although in many cases, e-signature laws were enacted a decade or two before.

CORIE framework, developed in response to increasing cyber threats to the financial sector, utilizes targeted threat intelligence to test institutions' cyber resilience and help regulators understand systemic weaknesses in the sector's cyber readiness. According to a **press release**, "CORIE's exercises will mimic the tactics, techniques and procedures (TTPs) of real-life adversaries, creating and utilising tools, and using techniques that may not have been anticipated and planned for. These exercises measure the ability of an organisation to detect, respond and recover from the operations of a real adversary based on such TTPs." CORIE has begun as an industry pilot program composed of key financial institutions, invited by the CFR, to provide feedback on the framework and gauge its effectiveness.

Legislation

Consultation on Phase 2 of Digital Identity Legislation, 14 June 2021

Consultation on Phase 2 of the Digital Identity Legislation closed July 14, and the bill is expected to be introduced to Parliament in late 2021 after a third phase of drafting and consultation. The Digital Identity Legislation aims to expand the Australian digital identity framework into the private sector and state and territory governments, in what the government dubs a "whole-of-economy" solution. Per Phase 2 of the drafting process, the government maintained proposals for a permanent oversight authority, an accreditation system and non-mandatory participation; introduced an interoperability principle and changed the definition of digital identity. Digital identity is thus defined as "a distinct electronic representation of an individual which enables that individual to be sufficiently distinguished when interacting online, including when accessing online services." The interoperability principle clarifies how system participants work together. The legislation also aims to secure privacy consumer safeguards by law. Under the current Digital Identity scheme, Australians can access over 75 government services through two accredited identity service providers, Australia Post and myGovID. According to the Minister for Employment, Workforce, Skills, Small and Family Business, Stuart Robert, over 2.5 million Australians and 1.27 million businesses utilize digital identity to access government services.[12]

Amendments to the Consumer Data Right Rules, 30 June 2021

The Australian Treasury issued exposure draft amendments to the Consumer Data Right (CDR) rules, the third version of the rules. The CDR, introduced in 2017, aims to give Australians greater control over the use and disclosure of their data within the economy. The draft amendments seek to enable greater participation in open banking. Barriers to entry, including the cost of accreditation, have dissuaded some businesses from adopting it. They introduce a sponsored accreditation model, by which an accredited person can sponsor a party seeking to become accredited. Parties seeking accreditation could also forego accreditation by becoming a CDR representative, and an accredited person would assume liability on their behalf.

The draft amendments also grant consumers more flexibility and power over their data. Consumers would be allowed to share data with a trusted professional advisor, including lawyers, financial counselors, financial planners, mortgage brokers, registered tax agents and qualified accountants. Per the proposed "CDR insight," consumers could consent to the sharing of their data outside the CDR framework for low-risk, prescribed purposes necessary for the consumer to receive a service. Prescribed purposes include consumer identification and verification of the consumer's account balance, income and expenses. Under the current CDR, both joint account holders must indicate their willingness to share account data in the case that one account holder seeks to share it. The draft amendments allow for one joint account holder to independently share data by consenting to an accredited party, and either of the joint account holders can invalidate the setting.

Ransomware Payments Bill 2021, 20 June 2021

The Ransomware Payments Bill 2021, introduced in the Parliament of the Commonwealth of Australia, introduces a requirement for all Commonwealth entities, state or territory agencies, businesses and others to report ransomware payments made in response to a ransomware attack. Obliged entities must report all ransomware payments to the Australian Cyber Security Centre (ACSC). Ransomware attacks have become increasingly prevalent in Australia and around the globe as the COVID-19 pandemic spurred entities to digitalize. According to the ACSC, Australians report an average of 164 cybercrimes per day.[13]

Hong Kong

Country Overview

Although Hong Kong faces competition by rapidly digitalizing Asian powerhouses like India and Singapore, it is poised to make incredible strides in open banking and other fintech innovations as it emerges from the COVID-19 pandemic. The health crisis drove a 6.1% shrinkage in Hong Kong's 2020 GDP, its largest annual contraction on record,[14] but the wealthy and innovative special administrative region is expected to make a strong recovery. Indeed, the economy expanded by 7.9% in the first quarter of 2021,[15] its strongest quarterly performance in eleven years.[16]

In ensuring a stable recovery and securing Hong Kong's status as a modern, global financial hub, digitalization will be key. In February 2021, Financial Secretary Paul Chan released the 2021-2022 budget, which allocates HK $120 billion (approximately USD$15.5 billion) towards strengthening digital transformation, the market recovery process and Hong Kong's competitiveness.[17] Hong Kong already ranks third globally and second in the APAC region in digital evolution, according to the Digital Intelligence Index (DII) 2020 prepared by Mastercard and Tufts University's Fletcher School. The pandemic further sped up digitalization in Hong Kong as consumer preferences shifted and banks rushed to adopt digital solutions, including increased investment in AI.[18] Alongside a boost in the use of digital payments, e-commerce sales soared amidst containment measures and political protests, and the market is expected to grow at a compound annual growth rate of 8.3% between 2021 and 2024.[19]

The Hong Kong Monetary Authority (HKMA) has been especially eager to cultivate the city's vibrant fintech ecosystem, and has encouraged the accelerated adoption of online banking, open banking and other future-proof solutions. Eight virtual banks—licensed by the HKMA—launched in 2020,[20] and virtual banks are expected to yield HK$76 billion in revenue per year by 2025, a combined market share of 19.3%.[21] Meanwhile, the HKMA is pushing small and medium-sized lenders to digitalize their operations.

Hong Kong's 2021 digital agenda focuses on strengthening the fintech sector and its open banking framework, regulating crypto, an investigation into a possible e-HKD, a digital yuan cross-border retail payment system and a multiple central bank digital currency (CBDC) bridge project. A key challenge will be navigating a continuously evolving cyberthreat landscape as digitalization presents new and sophisticated risks. In 2020, cybercrime in Hong Kong skyrocketed by 55% compared to 2019,[22] with a notable increase in cyber fraud tactics like phishing. Hong Kong has no comprehensive national cybersecurity framework, which would be instrumental in protecting its digital economy and bolstering its competitiveness.

Financial Regulatory Authorities

The **Hong Kong Monetary Authority (HKMA)** is the jurisdiction's central bank reporting to the Financial Secretary. The bank's primary objective is to ensure the stability of the territory's financial system and currency.

The **Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD)** is the main data protection authority in the jurisdiction. The statutory body enforces the Personal Data Privacy Ordinance (PDPO) and issues various regulations and guidelines implementing requirements under the PDPO.

Other Regulatory Authorities

The **Financial Services and the Treasury Bureau (FSTB)** develops and implements government policy on finance and treasury.

Policy, Laws and Regulations

Hong Kong Monetary Authority to Begin Study on Use Cases of Central Bank Digital Currency, 08 June 2021

As part of its Fintech Development Strategy ("**Fintech 2025**"), the HKMA announced that it has been working in partnership with the Bank for International Settlements (BIS) in researching retail CBDCs, and that it will now begin to study use cases and risks of CBDCs. Project Aurum will test both hybrid CBDC and private CBDC-backed stablecoin models. The HKMA also announced that it was entering a second phase of testing to explore the linkage of China's digital yuan with Hong Kong's domestic payments system to assess the CBDC's feasibility in cross-border transfers.

Fintech 2025 seeks to further integrate fintech technologies with the financial sector, develop next-generation data infrastructure, bolster the fintech workforce, prepare Hong Kong for the advent of CBDCs and cultivate the fintech ecosystem through funding and policies. Towards these goals, the HKMA will create a Fintech Cross-Agency Co-ordination Group to develop policies in support of fintech, strengthen the Fintech Supervisory Sandbox and build the Commercial Data Interchange (CDI), a digital identity and distributed ledger technology (DLT)-based platform that facilitates consent-based data sharing. To encourage the adoption of fintech by banks, the HKMA will issue a Tech Baseline Assessment to help pinpoint fintech business areas or technologies in need of support from the authority. The Hong Kong Growth Portfolio, a HK$22.4 billion (approximately USD$2.9 billion) investment fund[23] to support key companies and projects, is in development, as is the Industry Projects Masters Network scheme, which aims to cultivate fintech talent by offering internship opportunities to postgraduate students.

Circular on iAM Smart in Remote Onboarding, 24 May 2021

The HKMA issued a circular to authorized institutions (AIs) to promote the wider adoption of the iAM Smart (internet Access by Mobile in a Smart way) mobile app in remote onboarding. Launched in December 2020, the iAM Smart app offers digital identity services, including authentication, form-filling, personalized notifications and digital signing. Holders of a Hong Kong Identity Card (HKIC) aged 11 and above are eligible to register for the app. In order to clarify the use of iAM with regard to AML/CFT compliance, the Hong Kong Association of Banks (HKAB), with help from the HKMA, updated the relevant FAQs. The circular states “that when iAM Smart is used for identity verification, record keeping requirements may be met by retaining the specific data or information obtained from iAm Smart through Application Programming Interface, showing the customer’s iAM Smart authentication result and verified Hong Kong Identity Card data. AIs do not need to obtain additional identification documents solely for record keeping purposes.”

Penalties on Unlicensed Crypto Exchanges, 21 May 2021

In their report *Public Consultation on Legislative Proposals to Enhance Anti-Money Laundering and Counter-Terrorist Financing Regulation in Hong Kong*, the Financial Services and the Treasury Bureau (FSTB) proposed regulations and penalties on unlicensed virtual asset service providers (VASPs) in line with Financial Action Task Force (FATF) standards. Per the proposals, unlicensed VASPs would be prohibited from actively marketing their services and face a fine of HK$5,000,000 (approximately USD$644,000) and imprisonment of seven years for conducting a regulated virtual asset activity. Continued offenses would incur a fine of HK$100,000 (approximately USD$12,900) per day. Non-compliance with AML/CFT requirements; the provision of false, deceptive or misleading statements in a license application; and "fraudulent or reckless misrepresentation for the purpose of inducing another person to acquire or dispose of a VA" will incur a fine of HK$1,000,000 (approximately USD$129,000) and imprisonment of two years. The Securities and Futures Commission (SFC) would administer the new licensing framework for VASPs.

Implementation Plan for Phases III and IV for Open Banking API, 13 May 2021

HKMA announced its implementation plan for Phases III (account information) and Phase IV (transactions) of the **Open API Framework for the Hong Kong Banking Sector**, which was launched in July 2018 to support the safe development and adoption of open banking products and services. The framework's 28 participating banks will begin to progressively implement Phases III and IV by December 2021, with an initial focus on deposit account information and online merchant payments. The HKMA's approach centers on minimizing risk and lowering implementation costs. Its document, ***The Next Phase of the Banking Open API Journey***, outlines essential practices in the implementation of Phases III and IV, including the need to:

- "Adopt appropriate risk management strategies
- Introduce appropriate protection mechanisms
- Design compelling banking API propositions for customers
- Understand the range of bank capabilities required
- Understand the range of TSP capabilities required
- Select one or more appropriate business/finance models
- Monitor the banking Open API ecosystem"[24]

The HKMA will also support the Hong Kong Association of Banks (HKAB) in developing standards regarding customer experience and authentication, technical and data standards, information security and operation standards. The standards and a revised Common Baseline document have an expected publication date of December 2021.

Multiple Central Bank Digital Currency Bridge Project, 23 February 2021

A joint statement announced the addition of the Central Bank of the United Arab Emirates and the Digital Currency Institute of the People's Bank of China to the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project, spearheaded by the HKMA and the Bank of Thailand. The project, supported by the Bank for International Settlements Innovation Hub, explores the use of a CBDC and DLT in instantaneous cross-border payments, and investigates scalability, interoperability, privacy and governance. It aims to simplify cross-border fund transfers by lowering costs, reducing inefficiencies and easing the burden of complicated regulatory compliance.

White Paper on the Value of Regulatory Technology in the Financial Sector, 02 November 2020

The Hong Kong Monetary Authority published a white paper entitled *Transforming Risk Management and Compliance: Harnessing the Power of Regtech*, which outlines the state of regtech in Hong Kong banking, alongside actions that the HKMA will take in facilitating its adoption. Regtech solutions can reduce costs, boost efficiency and improve risk management, and they are instrumental in maintaining the competitiveness of Hong Kong's banking sector. The six main fields in which regtech solutions are applied include regulatory compliance obligations, conduct and consumer protection, regulatory and tax reporting, governance and accountability, risk management and financial crime. Of the banks surveyed for the paper, one-third had already implemented at least one regtech solution, while cost and capabilities constraints have prevented more banks from adopting regtech. The paper reviews the five core areas making Hong Kong a global leader in regtech, which includes boosting awareness, promoting solution innovation, continued regulator engagement with the ecosystem, developing the talent pool and sustaining adoption.

India

Country Overview

India has been devastated by the COVID-19 pandemic, which has led to an enormous loss of life, strained the financial sector and crippled health infrastructure in the developing country. May 2021 official statistics report a total death toll of over 300,000 people, with estimates from *The New York Times* as high as 1.6 – 4.2 million.[25] Restrictions have disrupted supply chains and driven labor shortages, hurting small businesses and macroeconomic activity,[26] and the second wave of infections could delay India's fragile economic recovery as consumer confidence shrinks, unemployment rises and medical expenses mount.[27]

The overall growth outlook for 2021 remains optimistic, however. India's economy shrunk by 7.7% in 2020, but the Organisation for Economic Co-operation and Development predicts it will be the fastest-growing G20 economy in 2021, with a GDP growth of 9.9%.[28] Assuming there is no third wave of COVID-19, Deloitte economist Rumki Majumdar forecasts strong economic activity in the second half of the financial year as consumer and investment spending increase, case numbers drop and vaccinations accelerate.[29]

Digital transformation, which sped up in response to the pandemic, will shape India's recovery. Indeed, India ranked #4 in the "Break Out Economies" category of the Digital Evolution Scorecard 2020, developed by Tufts University's Fletcher School in partnership with Mastercard. Banks are increasingly digitalizing their operations, digital payments have soared and e-commerce is expected to grow 84% over the next four years.[30] The fintech ecosystem rapidly expanded in 2020, bringing in USD$2.7 billion USD in investments, and India is poised to be a global hotspot for the development of artificial intelligence-based solutions.

India's 2021 digital agenda focuses on strengthening the payments system, exploring blockchain-based innovations and encouraging digital financial inclusion. Promoting digital financial inclusion will be instrumental in ensuring that

India's rapid digitalization does not further widen socioeconomic disparities, especially between urban and rural areas. The Ministry of Finance is also developing the "The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021," which will provide a framework for the regulation of digital currencies, and the central bank is discussing the possibility of developing a central bank digital currency. A national cybersecurity framework would further solidify India's ambitious goals in developing a globally competitive fintech ecosystem and digital economy.

Financial Regulatory Authorities

The **Reserve Bank of India (RBI)** is the central bank of India in charge of issuing and supplying the Indian rupee. The bank is the primary regulator for the commercial banking industry, as well as nonbanking finance companies.

The **Insurance Regulatory and Development Authority of India (IRDAI)** is an independent statutory body tasked with regulating and promoting the insurance and reinsurance industries in India.

The **Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI)** is an independent government-mandated business that facilitates operations for the country's Registration System for the securities market.

The **Securities Exchange Board of India (SEBI)** regulates business on stock exchanges and protects the interests of investors.

Policy, Laws and Regulations

Central Bank Considers Possible CBDC, 22 July 2021

Reserve Bank of India Deputy Governor T Rabi Sankar addressed the possibility of an investigation into a central bank digital currency (CBDC). Speaking at a webinar, Sankar stated that the central bank might soon begin pilot tests on a CBDC, with both wholesale and retail use cases. Sankar also noted that a digital rupee could undermine the popularity of virtual currencies and protect consumers from their volatility.[31]

Published 26 February 2021, the Reserve Bank of India's ***Report on Currency and Finance 2020-21*** briefly addresses the opportunities and risks presented by CBDCs, alongside potential regulatory updates. A CBDC can encourage financial inclusion, aid in monitoring transactions and act as an instrument of sterilization in emerging markets, all of which could strengthen India's digital economy and help it to compete with digital powerhouses like Germany and China. On the other hand, a CBDC can disintermediate the banking system, thus threatening growth and financial stability, though the report notes that a two-tier renumeration system would be an effective solution in safeguarding against this possibility. Furthermore, a CBDC and its accompanying regulations must take into account the risks of money laundering and terrorist financing. A CBDC designed to allow for anonymity at the individual level could facilitate ML/TF, so appropriate AML/CFT controls must be instituted.

Circular on Video-Based Customer Identification in KYC, 10 May 2021

The Reserve Bank of India issued a circular announcing an amendment to the Master Direction (MD) on KYC, which seeks to facilitate the use of video-based customer identification and simplify the periodic updating of KYC. The circular expands the definition of the video-based customer identification process (V-CIP) and outlines requirements on records and data management, operating procedure, and cybersecurity and resilience frameworks for regulated entities (REs).

Per the circular, "Video based Customer Identification Process (V-CIP) is an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to face CIP for the purpose of this Master Direction."

Regulated entities may utilize V-CIP to conduct customer due diligence for the onboarding of individual customers, proprietors per proprietorship firms, authorized signatories and beneficial owners per legal entity customers; the conversion of accounts opened by one-time passcode (OTP)-based eKYC; and the periodic updating of KYC for eligible customers. The data and recordings obtained from V-CIP must be stored within India, and accounts opened utilizing OTP-based eKYC may not be active for more than a year unless V-CIP is conducted. Regulated entities must take a risk-based approach to the periodic updating of KYC. The updated regulation went into immediate effect.

Report on Digital Financial Inclusion and Confidence in Electronic Payments, 10 May 2021

The National Institution for Transformation India (NITI Aayog) published the report *Connected Commerce: Creating a Roadmap for a Digitally Inclusive Bharat*, based on a discussion series hosted by NITI Aayog and Mastercard. The report addresses digital financial inclusion, cybersecurity and the fintech ecosystem in a post-pandemic India, and outlines policy recommendations. Digital payments will be especially crucial in promoting digital financial inclusion, and regulators must enable non-banking financial companies (NBFC) to issue cards and conduct e-KYC. The report notes that the partnership between banks and non-banks is a "best of both worlds" approach that "should be allowed to flourish."

In order to strengthen the e-commerce and digital transactions landscapes for both consumers and merchants, regulators must allow for the entry of non-banks into payment schemes, enable the increased adoption of automated infrastructure developments like interoperable QRs, encourage innovation and investment in the acquisition space and promote the development of solutions like offline payments and cloud tokenization. Cyberattacks have risen in tandem with an increase in digital transactions, and the COVID-19 pandemic drove a surge in phishing and identity thefts. The central bank must work to bolster cyber resilience while minimizing friction to user experience, and the government is currently examining a new National Cyber Security Strategy. Enabling improved information-sharing will be key in detecting and deterring attacks.

Discussion Paper on Blockchain Technology and Competition, 12 April 2021

The *Discussion paper on blockchain technology and competition*, published by the Competition Commission of India, addresses regulatory and policy issues that could arise from the adoption of blockchain-based technologies, amongst other matters. A key challenge will be to maintain the appropriate balance between security concerns and fostering innovation. Primary concerns include jurisdictional issues and anonymity, ambiguity about legal status and classification of organizational structure of blockchains, compliance with data privacy and protection laws, localized data processing, issues related to smart contracts and lack of a medium of exchange for executing transactions through permission-less blockchains. India's draft Data Protection Bill 2019 poses numerous challenges to blockchain-based applications, which could prohibit their development if the bill is not harmonized. As blockchain does not allow for the erasure of data, it violates the bill's "right to restrict or prevent continuing disclosure of personal data," or the "right to be forgotten." Blockchain can also operate across multiple jurisdictions, thus violating the Data Protection Bill's requirement that personal data be processed within India. At the time of writing, the Data Protection Bill is being examined by a Joint Parliamentary Committee.

In January, the Ministry of Electronics and Information Technology (MEITY) published a draft of the **National Blockchain Strategy**, which overviews architecture options, the value of blockchain in e-governance, challenges to its adoption and a possible National Level Blockchain Framework. The National Level Blockchain Framework "can aid in scaling deployments for developed applications, emerge shared infrastructure and also enable cross domain application development," and could be accessed through a National Blockchain API. National services like eSign, ePramaan (an e-authentication framework) and DigiLocker (which provides access to documents) could be integrated with the National Level Blockchain Framework.

Central Bank Statement on Improving Domestic Payment and Settlement Systems, 07 April 2021

The Reserve Bank of India issued its Governor's Statement, which addresses future initiatives on improving the domestic payment and settlement systems. The statement proposes that the RBI-operated Centralised Payment Systems (CPSs), from which banks are currently excluded, be opened to membership for "non-bank payment system operators Prepaid Payment Instrument (PPI) issuers, card networks, White label ATM operators and Trade Receivables Discounting System (TReDS) platforms regulated by the Reserve Bank." The statement further outlines a proposal to allow cash withdrawals for full-KYC prepaid PPIs of non-bank PPI issuers and "to make interoperability mandatory for full-KYC PPIs and for all payment acceptance infrastructure."

The statement comes on the heels of a 05 February 2021 RBI **statement** that addresses initiatives to improve the domestic payment and settlement systems. The statement lays out several regulatory measures in the works, including the establishment of a 24/7 helpline for digital payment services and guidelines for operators and participants of authorized payment systems regarding cybersecurity risks in outsourcing.

Central Bank Extends Deadline for Mandatory Additional Factor of Authentication for Automatic Recurring Debit Payments, 31 March 2021

The Reserve Bank of India announced in December 2020 that it would mandate an additional factor of authentication (AFA) in the case of automatic recurring debit payments, to be instituted 31 March 2021. In response to pressure from banks, the RBI extended the deadline by six months, to 30 September 2021. Once the new requirement is in effect, banks must inform customers as to auto-debit recurring payments below INR 5000 (approximately USD$67) by card, wallet and Unified Payments Interface (UPI). Customers must approve the transaction, which will be debited automatically from then on. Transactions above the INR 5000 threshold will require the use of a one-time password (OTP). Banks will be fined 5 lakh (approximately USD$.07) for every lapse. The move comes as part of the RBI's endeavor to bolster security of digital payments, alongside its increased adoption. In January 2021, the RBI raised the threshold for contactless recurring transactions from INR 2000 to INR 5000 (approximately USD$26.76 to $67).

Circular on IT Security for Digital Payment Products and Services, 18 February 2021

The Reserve Bank of India issued a circular entitled "Master Direction on Digital Payment Security Controls," which lays out guidelines to strengthen IT security for digital payment products and services. Key guidelines address fraud and risk management, authentication framework, customer protection, mobile payments application security controls and card payments security standards. Regulated entities must establish a policy for digital payment products and services that addresses risk management and mitigation measures, the product or service's inherent risk, customer experience and payment security requirements with regard to Functionality, Security and Performance (FSP), and regulated entities must appropriately identify, analyze, monitor and manage the specified risks, including compliance and fraud risks. Risk assessments must address interoperability aspects, the reconciliation process, outsourcing, customer experience, fraud risks, risks stemming from the integration of the digital platform with other systems, compliance with cybersecurity requirements, business continuity and service availability, amongst other matters. Regulated entities must also safeguard the robustness and scalability of the digital payment architecture "commensurate with the transaction volumes and customer growth."

Indonesia

Country Overview

Indonesia, home to Southeast Asia's largest economy and the 10th-largest global economy per purchasing power parity (PPP), has been decimated by the COVID-19 pandemic. The health crisis has exacerbated poverty, strained the healthcare system and driven a 2.07% contraction in the 2020 economy, Indonesia's first recession since the 1997 Asian Financial Crisis.

Despite this grim outlook, Indonesia is on the brink of incredible digital transformation. Its economy has rapidly digitalized, and the value of the digital economy is projected to reach USD$124 billion by 2025, a 65% increase from USD$44 billion in 2020. A young and tech-savvy population, alongside a rising middle class, has bolstered the growth of e-commerce, and the country has a robust tech startup landscape. Government regulations are sparse, however, and regulators must provide more support to small and medium-sized enterprises (SMEs) in order to further aid the development and adoption of innovative solutions.

Indonesia's 2021 digital agenda focuses on the development of artificial intelligence, a risk-based approach to the payment licensing framework, regulating crypto assets and combatting money laundering and terrorist financing in the payments sector. Central bank Governor Perry Warjiyo announced on 25 May 2021 that the bank is planning to introduce a digital rupiah, but he did not offer a timeline. A key challenge will be ensuring that digitalization does not further aggravate socioeconomic disparities, especially as the developing country emerges from the pandemic.

Financial Regulatory Authorities

Bank Indonesia is the central bank of Indonesia.

The Financial Services Authority of Indonesia (Otoritas Jasa Keuangan or OJK) regulates and oversees the financial sector.

Policy, Laws and Regulations

Regulation on Payments System in Effect, 01 July 2021

Bank Indonesia Regulation No. 22/23/PBI/2020 on Payment System went into effect. The regulation aims to support the bank's 2025 Indonesia Payment System Blueprint, launched in 2019, and makes major changes to the payment licensing framework. The updated licensing framework takes a risk-based approach in classifying payment sector companies, which will be placed into one of two categories and a further sub-category. Payment service providers—which shall include e-wallet, e-money, payment gateway, funds transfer and merchant acquiring services —must obtain a license from the central bank. Payment system infrastructure operators, which includes clearing and settlement services, must obtain an appointment from the central bank. Both classifications are further divided into sub-categories: systemic payment companies, critical payment categories and general payment categories. In designating a classification, the central bank will consider numerous factors, including the companies' market share, value of transactions processed and interconnectivity of systems with other infrastructure participants. Bank Indonesia will evaluate payment companies that already have a license and convert their licenses if needed.

Central Bank Bans Use of Cryptocurrency in Payments, 15 June 2021

The Governor of Bank Indonesia, Perry Warjiyo, announced that the bank would ban the use of cryptocurrencies in payments and "other financial services tools." According to Governor Warjiyo, cryptocurrency is not a legitimate payment instrument per the Constitution, Bank Indonesia law and currency law. The move follows a recent crackdown on three crypto trading platforms, which were forced to shut down operations for failure to have a license. The central bank is currently working on a cryptocurrency framework, and a discussion on a cryptocurrency tax is underway. The proposed tax would be .05%.

Memorandum of Understanding on Money Laundering in Payments, June 2021

Governor Warjiyo and Managing Director of Brunei Darussalam Central Bank (BDCB), Rokiah Badar, signed a memorandum of understanding (MoU) on cooperation in combatting money laundering and terrorist financing in the payments system. According to a statement by Governor Warjiyo, the regulators would engage in policy dialogue, data and information exchange, and human resources capacity building.

National Artificial Intelligence Strategy, August 2020

The government unveiled a national artificial intelligence strategy, which outlines guidelines for the development and adoption of AI solutions between 2020 and 2045. The strategy focuses on AI in education and research, mobility, smart cities, food security, bureaucratic reform and health services.

"We are all determined to create an independent, advanced and prosperous Indonesia. Let us successfully reform Indonesia from being a natural resource-based country to an innovation-based country," said Research and Technology Minister and National Research and Innovation Agency (BRIN) head, Bambang Brodjonegoro.

Legislation

Personal Data Protection Bill, June 2021

The Indonesian House of Representatives is considering a Personal Data Protection Bill ("The Privacy Bill"), which grants data subjects several rights to control and manage their data and imposes requirements on companies to demonstrate compliance. Data rights may be suspended in cases of national defense and security, law enforcement, supervision of the financial or monetary sector, state administration and financial system stability.

Per new requirements on the cross-border transfer of personal data, personal data may be transferred if:

- The recipient jurisdiction adheres to data protection standards that are equivalent to, or greater than, that provided by the Privacy Bill
- An international treaty between Indonesia and the recipient jurisdiction allows for the transfer of data
- The data subject has granted consent; or
- There is an agreement such that the data transferor can impose data protection requirements on the recipient that are equivalent to or greater than that provided by the Privacy Bill.

The bill, developed by the **Ministry of Communication and Informatics (MOCI)**, would be instrumental in shaping the digital economy, as Indonesia currently lacks a national personal data protection framework.

Japan

Country Overview

Although Japan is renowned for its wealthy economy and innovative technologies, the country scores low on indicators for digital competitiveness and digital talent per the IMD World Digital Competitiveness Ranking 2020. Usage of digital government services, mobile banking and e-commerce lags well behind ratings for other advanced economies. This puts Japan's status as the world's third-largest economy at risk of being surpassed by digital powerhouses like Germany and India.[32]

Meanwhile, Japan has grappled with the devastating effects of the COVID-19 pandemic, which led to three states of emergency and a 4.8% contraction in the 2020 GDP.[33] The Organisation for Economic Co-operation and Development (OECD) predicts a modest 2021 economic expansion of 2.6%, down from 2.7%, due to containment measures instituted in April.[34] Its slow vaccine rollout, alongside the risk of further outbreaks and restrictions, could threaten Japan's fragile recovery. The financial sector remains stable overall, however, and Mitsubishi UFJ Financial Group—Japan's largest bank—reported a 47% rise in net profit for the year ending in March 2021.[35]

The COVID-19 pandemic highlighted weaknesses in Japanese digitalization, but it has also offered the country a chance to accelerate its efforts. In 2020, traditionally cash-reliant Japanese flocked to digital payment solutions. E-commerce sales are estimated to have soared by 10.1%[36] and top banks began research into digital currencies and electronic money.[37] Japan's COVID-19 recovery package, introduced in December 2020, allocates JPY 1 trillion (approximately USD$9 billion) towards digital transformation.[38]

Prime Minister Yoshihide Suga, who came into power September 2020, has been vehement in spearheading digitalization with a mind towards boosting efficiency and productivity. His 2021 digital platform focuses on the digitalization of government, society and economy; **it also encompasses** a central bank digital currency (CBDC) experiment and the beginning stages of the development of a national AI framework. In May 2021, Suga stated that the government was working towards achieving a "free and open digital space" in the Indo-Pacific region.[39] A key challenge will be ensuring that cybersecurity readiness is strengthened alongside digitalization, as Japan's current cybersecurity framework is insubstantial to protect against a growing risk landscape.[40] Indeed, the government plans to establish a cross-sectoral unit in 2022 dedicated to studying cyberattacks and developing stronger defenses.[41]

Financial Regulatory Authorities

The Bank of Japan is the central bank and primary monetary policymaker for the country.

The Personal Information Protection Commission (PPC) is the central data protection authority in Japan. The agency enforces the 2003 Act on the Protection of Personal Information (APPI).

The Financial Services Agency (FSA) is responsible for overseeing banking, securities, exchange and insurance sectors in Japan.

Other Regulatory Authorities

The Japan Financial Intelligence Center (JAFIC) is an independent agency that enforces the Act on the Prevention of Transfer of Criminal Proceeds.

The Ministry of Trade, Economy and Industry (METI) seeks to develop the Japanese economy and industry by promoting the economic vitality of private companies and external economic relationships.

Policy, Laws and Regulations

Parliament Passes Set of Digital Reform Laws, Including Digital Agency Law, 12 May 2021

The Japanese parliament—the Diet—passed a set of digital reform laws, including the Digital Agency Law, which will establish a Digital Agency in September 2021. The government agency, to be headed by a cabinet minister and a top administrative official, will promote digitalization in government and the private sector while ensuring the protection of personal data. It will also be tasked with encouraging the use of the My Number system, a 12-digit number issued to all citizens and residents that enables access to online public services. The laws seek to revamp historically paper-reliant government and administrative services and oust the use of the hanko seal, an individualized stamp used to sign official documents. Local governments will be required to utilize computer systems to improve the provision of public services.

An October 2020 move by Prime Minister Suga will have banks and other financial institutions leverage electronic signature technology and digitize their forms by the end of 2022. Companies have traditionally filed paper documents with the Financial Services Agency, which has reduced efficiency and driven up costs.[42] In a 16 March 2021 **speech** entitled "Integrating Information and Financial Systems: Beyond As-a-Service," Bank of Japan Governor Haruhiko Kuroda addressed the need to digitalize the "paper-bound" work culture in Japan. Goals in supporting innovation must center on improving business efficiency and "creating new business models linking information."

Central Bank Issues Announcement on Central Bank Digital Currency Experiment, 05 April 2021

The central bank issued a press release announcing that its Proof of Concept (PoC) Phase 1 of a CBDC experiment had begun. During the PoC Phase 1—which will last until March 2022—the bank will test basic functions of a CBDC system, including issuance, distribution and redemption. A second Proof of Concept phase will then analyze more in-depth functions and issues, like limits on the amount of CBDC an entity can hold.[43] A possible third stage of testing would create a pilot program involving payment service providers and end users. Central bank Governor Haruhiko Kuroda stated in March 2021 that, although there is no plan to issue a digital yen, the bank aims to make necessary preparations in light of "the advent of digital society."[44]

On 08 October 2020, the Bank of Japan published a **policy document** on CBDCs, which outlined three primary motivations for the development of a CBDC. Drivers include improving the stability and efficiency of payment and settlement systems; providing an alternate payment method if cash use significantly declines; and supporting an increasingly digital society. In January 2020, then-Parliamentary Vice Minister for Foreign Affairs Norihiro Nakayama said, "China is moving toward issuing digital yuan, so we'd like to propose measures to counter such attempts,"[45] pointing towards the longstanding China-Japan rivalry.

On 02 July 2020, the Bank of Japan published a **research paper** on CBDCs, which largely addressed how to facilitate offline payments. This is of particular importance to the country in light of recent earthquakes and power outages.

Amendments to the Enforcement Rules for the Act on the Protection of Personal Information, 23 March 2021

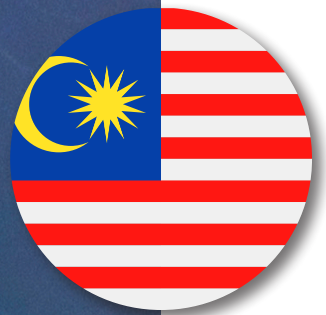
The Personal Information Protection Commission published amendments to the Enforcement Rules for the Act on the Protection of Personal Information in the official gazette, thus further implementing provisions of the Act Amending the Act on Protection of Personal Information (APPI). The amended APPI, approved by the Japanese Diet on 05 June 2020, strengthens the rights of data subjects and imposes new requirements on entities that process personal data. It obliged entities to report data breaches to the PPC, expands the PPC's powers such that it can request reports or investigate offshore companies, increases penalties in the case of non-compliance and introduces the concept of pseudonymization. Pseudonymization is a data management procedure by which data subjects' personally identifiable information is replaced with a pseudonym, thus protecting their rights and enabling processors to more readily use their information. The amended APPI also expands data subjects' rights to deletion and cessation of the use of personal data, and allows data subjects to select the method of receiving their data (writing or email), per the right of access. Like the EU's General Data Protection Regulation (GDPR), the APPI has extraterritorial scope, applying to all entities that process personal data of Japanese citizens, regardless of the entities' physical location. The amended APPI enables the PPC to request that foreign obliged entities report on their processing activities, and the PPC will be able to impose fines on them in the case of non-compliance. The Act will come into effect 01 April 2022.

Financial Services Agency Adopts Financial Action Task Force Guidelines on Virtual Assets and Virtual Asset Service Providers, 31 March 2021

The Financial Services Agency (FSA) announced that it will implement the Financial Action Task Force (FATF)'s "Travel Rule" per its guidelines on virtual assets (VAs) and virtual asset service providers (VASPs). The Travel Rule, which requires the exchange of identification data between senders (originators) and recipients (beneficiaries) of digital funds transfers, seeks to prevent ML/TF by cracking down on anonymity in wire and crypto transactions. Required information aligns closely with customer due diligence information standards, and includes the originator's name, address, birth date, birth place, account number and identity number, as well as the beneficiary's name and account or virtual wallet number. The rule will go into effect in 2022.

Draft Report on Governance Innovation, 19 February 2021

The Ministry of Economy, Trade and Industry published a draft report entitled *Governance Innovation v.2: A Guide to Designing and Implementing Agile Governance*, following a first report published in July 2020. The draft presents the ideas of the Study Group on a New Governance Model in Society 5.0, a research group that has been investigating means to achieve the Society 5.0 policy. The ambitious policy seeks to bolster economic development and address social challenges through the use of artificial intelligence, Internet of Things, big data and cyber-physical systems. Society 5.0 will be driven by a human-centric approach and by continuously adapting to changes brought on by emerging technologies. Agile governance will be flexible and adaptable to this constantly evolving landscape, and its governance model will hinge on an analysis of conditions and risks, continuously revised goals, transparency and accountability, inclusiveness and the participation of multiple stakeholders in its design, amongst other criteria. The report raises important implications in the realization of Society 5.0, including the protection of data privacy, regulating AI and defending against increasingly sophisticated cyberattacks. Indeed, Society 5.0 could be crucial in revolutionizing tradition-heavy Japanese society—which Prime Minister Suga has eagerly sought to modernize—but it will also require regulatory frameworks to mitigate the challenges and risks posed by digitalization.



Malaysia

Country Overview

As Malaysia emerges from the COVID-19 pandemic, its government is keen to cultivate the digital economy, bolster its regional competitiveness and attract new entrants and funding to the fintech ecosystem. The COVID-19 pandemic drove a GDP shrinkage of 5.6% in 2020, Malaysia's worst economic performance since the 1998 Asian Financial Crisis,[46] but the economy is projected to grow by 6.7% in 2021.[47] Meanwhile, the health crisis spurred on the increasing adoption of digital solutions. In 2020, e-commerce skyrocketed by 87%, contactless payments surged[48] and 36% of all digital service consumers were new.[49] Digital talent is significantly lacking, however,[50] and slow broadband speed and high costs have impeded the greater adoption of digital services by Malaysian businesses.[51]

Malaysian regulators spearheaded numerous efforts in 2020 to strengthen cybersecurity, promote the adoption of innovative technologies and regulate digital assets. In June 2020, Bank Negara published new eKYC guidelines enabling the use of video calls and AI in remote identity verification during customer onboarding, applicable to banks and other financial institutions. The Federal 2021 budget, announced in December 2020 and Malaysia's largest yet,[52] allocated RM I billion (approximately $242.5 million USD) towards promoting cybersecurity, the digital transformation of SMEs, digital talent, connectivity and Internet of Things.[53]

The 2021 digital agenda focuses on further developing the digital economy and fostering a competitive digital banking landscape. In June 2021, Suhaimi Ali, Director of Financial Development and Innovation at Bank Negara, stated that the authority plans on running a proof-of-concept project to assess a possible central bank digital currency (CBDC), with a focus on wholesale CBDCs. Other future plans include the development of a new biometric National Digital Identity (NID) framework, which can be utilized to access online government and financial services, and the construction of an artificial intelligence park, which the government hopes will attract foreign direct investment and encourage the development of innovative technologies. The government's 12th Malaysia Plan (12MP), 2021-2025—which is in its final stage of development—seeks to strengthen the Malaysian economy and combat poverty, and includes initiatives to boost digitalization and the adoption of high-tech. As Malaysia undergoes its rapid digital transformation, regulators must ensure that the increasingly tech-based society does not further exclude people living in rural areas.

Financial Regulatory Authorities

Bank Negara Malaysia (BNM) is the central bank of Malaysia.

The Securities Commission Malaysia regulates and develops the capital markets in Malaysia.

Policy, Laws and Regulations

Government Unveils Digital Economy Blueprint, 19 February 2021

The government unveiled its Digital Economy Blueprint, a ten-year plan comprised of six strategic areas, including 22 strategies, 48 national initiatives and 28 sectoral initiatives. The six strategic areas aim to "drive digital transformation in the public sector, boost economic competitiveness through digitalisation, build enabling digital infrastructure, build agile and competent digital talent, create an inclusive digital society, build trusted, secure and ethical digital environment." The blueprint will unfurl over three implementation phases. Phase 1 from 2021-2022 will focus on strengthening the foundation for adoption of digital solutions;

Malaysia's decade-long digital strategy will enable the country to learn from other countries in terms of what has worked and what has not. Canada's Pan-Canandian Trust Framework expected to launch in 2022 and the European Union's forthcoming digital wallet could serve as a model as Malaysia builds out its digital infrastructure. Privacy and data protection laws could also be enacted. With digital banking licenses being issued, Malaysia could be a model digital economy in the coming years.

phase 2 from 2023-2025 centers on inclusive digital transformation; and phase 3 from 2026-2030 aims to make Malaysia a regional leader in digital content and cybersecurity. Over the next five years, the initiatives seek to attract two new unicorns, spearhead the growth of 5000 startups and convert 875,000 micro, small and medium enterprises to e-commerce. A series of partnerships between the public and private sectors will develop a stronger digital infrastructure and overall ecosystem, and by 2022, all public agencies will offer cashless transactions as a principal option. The government aims for the initiatives to boost economic productivity by 30% by 2030 and attract RM 70 billion (approximately USD$16.8 billion) in investments in the digital sector.

Central Bank Launches Digital Banking Framework, 31 December 2020

Bank Negara issued the Policy Document on Licensing Framework for Digital Banks, which allows for qualified entities to apply for a digital banking license. To receive a license, entities must have at least RM 300 million (approximately USD$72 million) in capital funds. The bidding process ended on 30 June 2021, and the central bank revealed that 29 companies had filed applications,[54] of which five will be chosen and announced by the first quarter of 2022. The move to open its banking sector to non-financial entities hints at Malaysia's serious intentions in cultivating competition in its domestic banking sector, as well as competing with other ASEAN markets like Hong Kong, the Philippines and Singapore, all of which have similarly encouraged new entrants to the banking sector.

Securities Commission Issues Updated Digital Assets Guidelines, 28 October 2020

The Securities Commission (SC) issued its revised Guidelines on Digital Assets, which outlines requirements for initial exchange offering (IEO) operators, digital asset custodians and issuers. Issuers must prepare a white paper that includes important information on the digital token for potential investors, including characteristics of the digital token; challenges, risks and mitigation measures; a technical description of the digital token; and the business plan of the issuer, amongst other requirements. IEO operators must conduct customer due diligence, review the issuer's proposal and white paper, and assess the issuer's ability to comply with the DA Guidelines and national AML/CTF framework. In order to register as a digital asset custodian with the SC, applicants must meet fit and proper requirements, have appropriate security arrangements and have sufficient financial and human resources to conduct operations. The document also overviews marketing, promotion, reporting and auditing requirements.

Government Launches National Cybersecurity Strategy, 01 October 2020

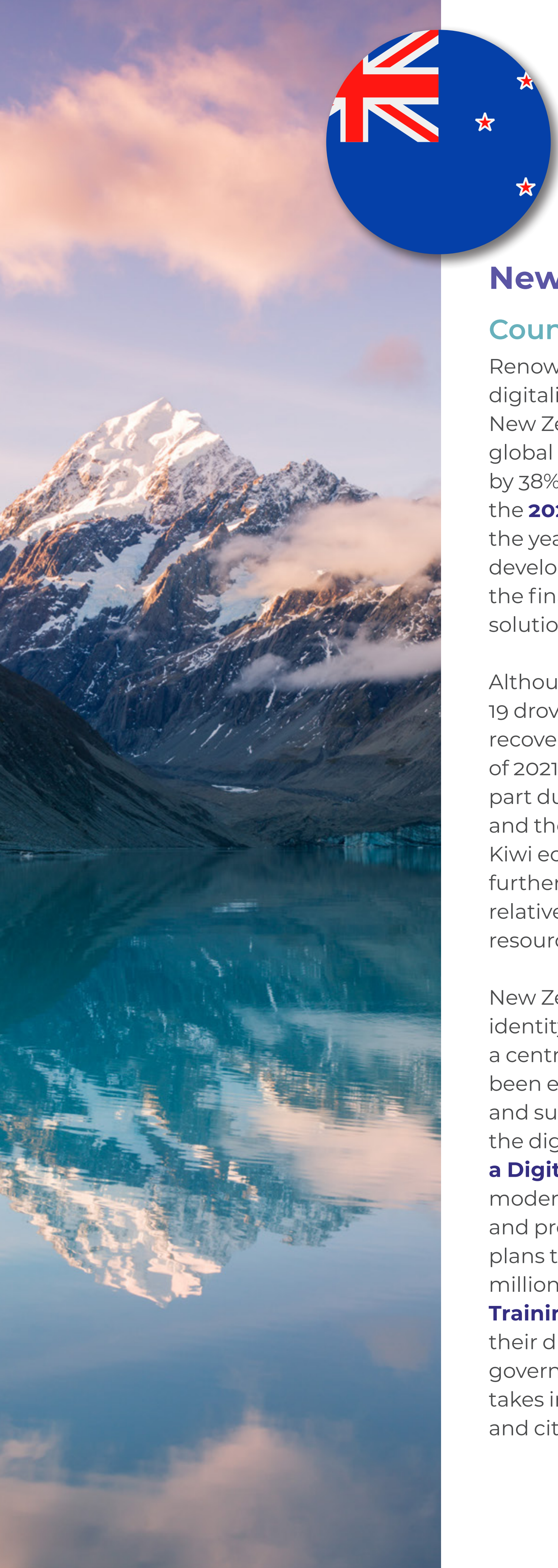
The government launched the Malaysian Cyber Security Strategy (MCSS) 2020-2024, which outlines five pillars and allocates RM 1.8 billion (approximately USD$434. 8 million) towards strengthening the country's cybersecurity framework. The five pillars seek to enhance governance of the management of national cybersecurity, strengthen and enforce existing laws and regulations, enhance the capabilities of experts and boost cybersecurity awareness, provide support for research and development and strengthen international cooperation. Malaysia is already a global cybersecurity leader, ranking five out of 194 states[55] in the 2020 Global Cybersecurity Index issued by the International Telecoms Union, a United Nations agency. Of the index's five categories, Malaysia earned top marks in three of them: a legal framework for handling security and crime; capacity measures based on R&D, education and training; and international partnerships and information sharing.[56]

GLOBAL POSITION

Malaysia is highly ranked in cybersecurity because it has policies focused on developing a solid national strategy.

RANK	COUNTRY	POINTS
1	U.S.	100.00
2	U.K.	99.54
2	Saudi Arabia	99.54
2	Estonia	99.48
5	Singapore	98.52
5	South Korea	98.52
5	Spain	98.52
8	Malaysia	98.06
8	Russia	98.06
8	UAE	98.06
12	Japan	97.82
40	China	92.53
Last	North Korea	1.35

Source: International Telecoms Union



New Zealand

Country Overview

Renowned for its political and social stability, rapid digitalization and deft response to the COVID-19 pandemic, New Zealand is poised to become a major regional and global fintech hub. Its fintech sector revenue has skyrocketed by 38% since 2016,[57] and the island country ranked #30 on the **2021 Global Fintech Rankings**, up fifteen spots from the year before. The government eagerly supports the development and uptake of emerging technologies, and the financial sector has quickly adopted innovative banking solutions.

Although a strict springtime lockdown in response to COVID-19 drove a 2.9% downturn in GDP in 2020,[58] New Zealand's recovery has been swift and strong. GDP in the first quarter of 2021 surged by 1.6%—three times the forecasted rate[59]—in part due to increased retail spending and a housing boom,[60] and the International Monetary Fund (IMF) predicts that the Kiwi economy will expand by 4% in 2021.[61] The health crisis has further accelerated digital transformation, and New Zealand's relatively unscathed status has freed up government resources toward strengthening the digital economy.

New Zealand's 2021 digital agenda focuses on a digital identity framework, cybersecurity and an investigation into a central bank digital currency (CBDC). Regulators have also been eager to boost the digitalization of government services and support small and medium-sized enterprises (SMEs) in the digitalization of business operations. The **Strategy for a Digital Public Service**, published in March 2020, seeks to modernize the public sector, improve customer experience and promote economic growth. In addition, the government plans to invest NZ $44 million (approximately USD$30.88 million) over the next two years toward the **Digital Boost Training Programme**, which will help 30,000 SMEs to bolster their digital skills and capabilities. Throughout its policies, the government emphasizes a "human-centric" approach that takes into consideration ethical implications of technology and citizen's wellbeing and input.

Financial Regulatory Authorities

The **Reserve Bank of New Zealand (RBA)** is the central bank of New Zealand. The Bank's primary functions are to maintain price stability through effective monetary policy and maintain a healthy financial system for the country.

The **Office of the Privacy Commissioner (OPC)** is the primary data protection authority in New Zealand. The OPC develops and promotes personal information protection among consumers and businesses and enforces the country's Privacy Act, last updated in 2020.

The **Commission for Financial Capability (CFFC)** is a British Crown agency that supports and promotes the growth of New Zealanders' financial capability and financial health.

The **Financial Markets Authority (FMA)** is the financial regulatory authority in New Zealand. The government agency regulates and enforces financial regulations for all financial markets and exchanges.

The **Ministry of Business, Innovation and Employment (MBIE)** is a federal government agency that develops policy, advice and regulations that aim to strengthen the country's economic growth.

Policy, Laws and Regulations

Central Bank on Potential CBDC, 07 July 2021

The central bank issued a statement confirming that it will issue consultations from August to November 2021 seeking feedback on the future of money and payments in New Zealand, especially in response to digital innovations. Per the statement, "The first consultation will introduce and seek feedback on the broad concepts of money and cash stewardship, and outline specific topics to be covered in the rest of the series. Subsequent papers will look at the potential for a Central Bank Digital Currency (CBDC) to work alongside cash as government-backed money, issues arising from new electronic money forms including crypto assets (such as BitCoin) and stable coins (such as proposed by a Facebook-led consortium), and how the cash system might need to change to continue to meet the needs of users." The central banks notes that a CBDC could be valuable in addressing disadvantages brought on by dwindling cash use, but it maintains that continued access to cash is critical.

Digital Identity Trust Framework, 03 May 2021

The government has approved a proposal to create a Digital Identity Trust Framework, which will establish rules for the delivery of digital identity services applicable to service, technology and information providers. In developing the framework, lawmakers will ground it on five proposed components:

- "**Accreditation** — establishing a body to accredit participants and a mechanism to demonstrate accreditation
- **Legal enforcemen**t — establishing mechanisms to make the rules legally binding upon accredited participants
- **Governance** — establishing a governing body to update and maintain the Trust Framework's rules
- **Participants** — defining the participants in a trusted digital identity system and the roles that they will play
- **Rules** — the standards and legislation participants will abide by, with a focus on identification, privacy and security. These may be existing or in development"[62]

The rules will be composed of five areas: identification management, information and data management, security and risk management, privacy requirements and sharing tool requirements. The bill is expected to be released later in 2021.

Cyber Resilience Guidance, 28 April 2021

The central bank published the *Guidance on Cyber Resilience*, which outlines expectations for all regulated entities regarding cyber resilience. Per the guidance, the board and senior management of regulated entities must establish a cyber resilience framework, promote a culture of cybersecurity awareness, participate in information sharing and adhere to five capability building components. The capability building components include to identify, to protect, to detect, and to respond and recover. In the case that an entity relies on a third-party service provider, the board and senior management must manage the relationship such that cybersecurity risks are mitigated. Regulated entities must inform the central bank "early in their decision-making process" if they outsource critical functions to cloud service providers.

Privacy Act 2020 Enters into Effect, 01 December 2020

The Privacy Act 2020, which expands privacy protections for New Zealanders and imposes stricter requirements on businesses and organizations for the handling of personal information, went into effect. Should a serious data breach occur, obliged entities must notify the Office of the Privacy Commissioner and the affected individuals "as soon as possible." The Privacy Commissioner can request an entity to confirm whether they hold an individual's personal data, and direct the entity to provide the individual access to their data. The Privacy Commissioner may also issue notices to obliged entities requiring them to take actions toward compliance with the Privacy Act. The Act expands criminal offences, including the destruction of personal data in the knowledge that access to it has been requested, and imposes a fine of up to AU$10,000 (approximately USD$7,400). The Act also introduced a new data localization requirement. Per principle 12, an entity may only send personal data overseas if the recipient organization or business adheres to similar protections as outlined in the Privacy Act. As with the EU's General Data Protection Regulation (GDPR), the Privacy Act has extraterritorial effect. It applies to any business or organization "carrying on business" in New Zealand, even if it does not have a physical presence in the country.

The Philippines

Country Overview

The Philippines has undergone a surge in growth over the past decade, with an average annual economic growth rate of 6.4% during 2010-2019, a significant reduction in poverty and an increase in real wages.[63] Although the COVID-19 pandemic slowed this rapid progress with an economic contraction of 9.5% in 2020—the Philippines' largest shrinkage on record[64]—the island country's overall outlook remains optimistic. The International Monetary Fund (IMF) estimates that its GDP will expand by 5.4% in 2021 and 7% in 2022,[65] although these forecasts might be downgraded if an outbreak of the highly infectious COVID-19 Delta variant drives further restrictions.

Digital transformation will be instrumental as the Philippines emerges from the health crisis and looks to expand its economy and achieve upper middle-income country status. The Philippines has lagged in its digital transformation compared to other Southeast Asian states, but a young and tech-savvy population, shifting consumer preferences and a spate of new regulations point toward promising growth for this emerging market. The COVID-19 pandemic drove increases in e-commerce and digital payments,[66] and the Philippines has the world's third-highest rate of cryptocurrency use.[67]

The Philippines' 2021 digital agenda focuses on digital payments, the launch of a national Artificial Intelligence Roadmap, an exploration into a possible central bank digital currency (CBDC), the digitalization of government services, a national digital identity framework and updating the national cybersecurity framework. The Department of Information and Communications Technology (DICT) is working with the Australian government to improve the Philippines' National Cybersecurity Plan.[68] As the Philippines digitalizes, regulators have been eager to ensure that digitalization efforts encourage digital financial inclusion. Around 51.2 million Filipinos—71% of the population—are unbanked due to a lack of accessibility, information and resources.[69] In April 2020, the central bank eased know-your-customer (KYC) requirements to expand access to banking services.[70]

Financial Regulatory Authorities

The **Bangko Sentral ng Pilipinas (BSP)** is the central bank of the Philippines.

The **National Privacy Commission (NPC)** monitors compliance with the Data Privacy Act 2012.

The **Securities and Exchange Commission (SEC)** regulates and supervises the corporate sector, capital market participants, the securities and investment instruments market, and the investing public.

Policy, Laws and Regulations

Central Bank Investigating CBDCs, May 2021

BSP Governor Benjamin Diokno stated in a virtual briefing that the bank was preparing to conduct a study of the payments and settlement system "vis-a-vis its digitalization agenda to assess any gaps that may be addressed by a CBDC."[71] The development of a CBDC would align with financial inclusion goals per the Digital Payments Transformation Roadmap. Governor Diokno noted that, although the bank does not plan to issue a CBDC in the near future, it is monitoring developments in private digital currencies and CBDCs in global and domestic markets. His statements follow the April publication of a BSP **report** on the opportunities and challenges in CBDCs, CBDC technology and global developments. The report recommends that the central bank conduct further research into improvements to the domestic payments and settlement system, privately-issued digital currencies in the Philippines, and digital currencies—both privately-issued and CBDCs—across the globe. The report further recommends that the central bank focus on capacity building, technical assistance on a legal framework, the development of an implementation roadmap and possible collaboration with other central banks, financial institutions or international organizations.

Artificial Intelligence Roadmap, 05 May 2021

The Department of Trade and Industry (DTI) unveiled via Zoom a national Artificial Intelligence Roadmap, which includes 42 strategic tasks related to regulation, research and development, digitalization, infrastructure and workforce development.[72] A key goal will be the establishment of the National Center for AI Research (N-CAIR), which will aim to encourage companies' adoption of AI and help small businesses to boost productivity.

"The country's AI roadmap will position the Philippines as an AI center of excellence and a big data processing and analytics hub providing high-value data analytics and AI services to the world," said Trade Secretary Ramon Lopez.[73]

PhilSys National Digital ID System Goes Live, 30 April 2021

The Philippine Identification System (PhilSys) was established by the Philippine Identification System Act (Republic Act No. 11055). Signed into law by President Rodrigo Duterte in August 2018, PhilSys seeks to provide every citizen and permanent resident with valid proof of identification and set the foundation for a digital economy. According to the National Economic and Development Authority (NEDA), PhilSys aims to promote financial inclusion, reduce fraud, give citizens more control over their personal data, facilitate the ease of doing business and make services more accessible.

The PhilSys ID, also known as the Philippine Identification Card (PhilID), includes thirteen data components, including name, photograph, birth date, birthplace, blood type and biometrics (fingerprints and iris scan). To participate in the system, citizens and permanent residents must first complete an online registration, then visit a registration center for the collection of biometric information and to open a bank account. Upon completion of the registration, PhilSys provides participants with their PhilID and two sets of numbers, the PhilSys Number (PSN) and PhilSys Card Number (PCN). The PSN is a permanent identification number containing their sensitive data, and the PCN is used for routine transactions. All citizens and permanent residents are required to participate in PhilSys. As of 03 July 2021, over a million PhilID cards had been issued, and almost 16.2 million Filipinos had completed the collection and enrollment of biometric data per step two of the registration process.[74] As of June 2021, around 3.7 million bank accounts had been opened since the launch of the system.[75]

Law to Strengthen Anti-Money Laundering and Counter-Terrorist Financing Framework, 29 January 2021

President Rodrigo Duterte signed a law strengthening the national anti-money laundering and counter-terrorist financing framework in advance of a Financial Action Task Force (FATF) 01 February 2021 deadline. The law broadens the powers of the Anti-Money Laundering Council (AMLC), enabling it to apply for court summons and search and seizure warrants; impose financial sanctions pertaining to terrorist financing; and monitor transactions by Philippines-based online casino workers, as well as real-estate firms and brokers handling cash transactions of over PHP 7.5 million (approximately USD $160,000).[76] The law also bolsters cooperation between the Philippines and transactional investigations and prosecutions regarding money laundering and terrorist financing. Before the passage of the law, the Philippines was at risk of being placed on FATF's grey list, which would have subjected it to increased monitoring by the global financial watchdog.

Digital Payments Transformation Roadmap, 12 October 2020

The central bank unveiled the *Digital Payments Transformation Roadmap 2020-2023*, which outlines short-term strategic outcomes toward bolstering financial inclusion and the digital economy through the development of digital payment innovations. Key targets for 2023 include strengthening consumer preference for digital payments and promoting "more innovative and responsive digital financial services." The central bank aims for 50% of retail payments to be conducted digitally with the introduction of more convenient payment options; 70% of Filipino adults to be financially included; the launch of PhilSys-based KYC to drive financial inclusion; and the "availability of a next generation payment and settlement system to facilitate real time processing of financial transactions."

The Republic Of Korea

Country Overview

Wealthy and innovative South Korea ranks #1 in BloombergNEF's 2020 national digitalization ranking[77] and is a world leader in internet penetration, digital payments and R&D expenditure. Korean banks have surged ahead of their global counterparts in swiftly adopting open banking, digital payments and other disruptive technologies, and tech-savvy citizens have been quick to adapt. There is even a new buzzword—"untact"—to describe Korea's increasingly digital culture. First developed by marketers in 2017, "untact" has become widely used in referring to contactless activities and services,[78] and it is a central tenet of President Moon Jae-in's platform.

South Korea's rapid digitalization and strong financial policies were on full display amidst the height of the COVID-19 pandemic, which was skillfully managed by the government. A swift and tactical approach led to drastically fewer deaths and less severe economic effects than seen in other advanced countries. The GDP contracted by 1% in 2020[79] and economic recovery has been quick, with a GDP growth of 1.6% in the first quarter of 2021.[80] In responding to the health crisis, the government successfully deployed digital solutions for public health measures, digital government, remote education and work,[81] and Koreans flocked to digital payments and e-commerce.[82]

South Korea's COVID-19 recovery strategy—the Digital New Deal—will further drive digital transformation in the economy and secure the country's status as a tech hub. The 160 trillion won (approximately USD$133 billion) deal, announced in July 2020, seeks to completely reshape Korean economy and society, with a focus on bolstering job growth and "untact" industries like remote education and health.[83] It allocates KRW 58.2 trillion (approximately USD$51 billion) towards the development of technologies like artificial intelligence, big data solutions and 5G networks over 2021-2025.

The 2021 digital agenda emphasizes financial innovation and digital finance, an investigation into the possible development of a central bank digital currency, developing the fintech ecosystem, financial consumer protection, strengthening cybersecurity and regulating crypto. Although digitalization in Korea promises to bring a trove of benefits to the economy and society, regulators must ensure that its rapid changes do not alienate the country's aging population and other vulnerable groups.

Financial Regulatory Authorities

The **Bank of Korea** is the central bank of the Republic of Korea. The bank's primary objective is to maintain the country's price stability and it often targets inflation, especially consumer price inflation.

The **Personal Information Protection Commission (PIPC)**, established under the country's Personal Information Protection Act (PIPA), is the primary data protection authority in South Korea. The independent commission develops policies and coordinates communication between government agencies regarding personal data processing. However, the **Ministry of the Interior and Safety (MOIS)** is charged with the enforcement of the country's Personal Information Protection Act (PIPA).

The **Financial Services Commission (FSC)** is South Korea's primary financial regulator.

Other Regulatory Authorities

The **Korea Internet and Security Agency (KISA)** is a statutory organization established by the Act on Promotion of Information and Communications Network Utilization and Information Protection (ETC) that assists government agencies with data breach resolution and research. The agency also provides advice on personal data protection security standards and policies.

Policy, Laws and Regulations

Bill Regulating Crypto Assets, 26 May 2021

The Act for Fostering the Virtual Asset Industry and Protecting Investors was introduced, which seeks to strengthen user protection and crack down on rampant hacking and fraud in the crypto industry. The bill would impose stringent entry barriers on entities seeking to operate virtual asset businesses, and would require all virtual asset businesses to join a virtual asset industry association.[84] The bill follows another draft law aimed at regulating crypto. On 07 May 2021, the Virtual Assets Act bill was introduced, which similarly aims to protect investors. Both bills would establish various requirements on virtual asset exchanges, trustee companies and wallet companies regarding fair trade practices and accreditation, registration and reporting.

Bank of Korea's Central Bank Digital Currency Platform, 24 May 2021

The Bank of Korea announced that it is seeking a technology supplier to build a test platform for a central bank digital currency. The pilot phase will test the use of a digital won in settlements and remittances through simulations of commercial banks and retail outlets. Although the central bank does not have concrete plans to issue a digital won, it aims to prepare for the possibility amidst a decline in cash transactions.[85] The trial program will begin in August 2021 and run through June 2022.

Partial Amendment to Information Act Imposes Requirements on Virtual Asset Service Providers, 25 March 2021

The Partial Amendment to the Act on Reporting and Use of Specific Financial Transaction Information, passed by Korea's parliament, the National Assembly, went into effect. The Partial Amendment, the first of its kind in Korea, allows for the operation of cryptocurrency exchanges by legitimizing virtual asset ownership and trading. Under the changes, virtual asset service providers (VASPs) must adhere to anti-money laundering requirements, including suspicious transaction reports, currency transaction reports and customer due diligence. VASPs shall conduct enhanced customer due diligence by requiring customer registration of an authorized Korean bank account, and VASPs shall report the registration to the Korean Financial Intelligence Unit (KoFIU) before September 2021. VASPs are also required to apply for an information security certificate with several prerequisites for approval, including the implementation of suitable technical solutions for sharing real-identity information with transaction counterparties. The Enforcement Decree, which also went into effect 25 March 2021, clarifies that "Qualified VASPs" per the Partial Amendment include cryptocurrency exchanges, custody service providers and wallet service providers.

Financial Consumer Protection Act Goes Into Effect, 25 March 2021

The Financial Consumer Protection Act (FCPA) streamlines previously fragmented statutes and regulations on the protection of financial consumers into one framework, expands the rights of financial consumers and imposes strict penalties for non-compliance. The act applies the six existing Sales Principles to a broader category of financial products, including financial products offered by banks, insurance companies, financial investment firms, P2P lending firms, registered private lenders, specialized credit finance companies and savings banks. The Sales Principles include the principle of suitability, the principle of adequacy, the duty to explain, the prohibition on unfair practices, the prohibition on misleading or unsolicited recommendations and the prohibition on false or exaggerated advertisements. The act also enables consumers to terminate a contract if an obliged entity violates a Sales Principle and withdraw from a subscription to financial products within a cooling-off period of seven to fifteen days. Should an obliged entity commit a major violation of the Sales Principles, punitive fines of up to 50% of revenue garnered through non-compliance may be imposed.

Announcement on Strengthening Cybersecurity, 18 February 2021

The Ministry of Science and ICT (MSIT) announced that it planned to allocate 670 billion won (approximately USD$607 million) towards strengthening national cybersecurity over 2021-2023. The ministry will collaborate with major cloud and data center companies to develop an infrastructure that can gather threat information in real time and notify companies, and provide security solutions to 1300 SMEs per year. Korean companies experienced a 2% rate of security information violations in 2020, which the ministry aims to reduce to less than 1.5% by 2030. The plan also intends to boost Korea's ranking in the United Nations' Global Cybersecurity Index, to number five by 2023.[86]

Financial Services Commission Announces Work Plan for Financial Innovation and Digital Finance, 28 January 2021

The Financial Services Commission unveiled a brief work plan for financial innovation and digital finance, which seeks to advance the fintech industry, promote online-based financial services and establish digital finance infrastructures. The three priorities hinge on key policy tasks, including the establishment of a digital sandbox for fintech startups, enhanced regulatory support, the improvement of rules on data privacy and ensuring the "stable operation of open banking services." The FSC will also encourage the use of big data analytics and artificial intelligence in financial services.

Financial Services Commission Announces 2021 Work Plan, 18 January 2021

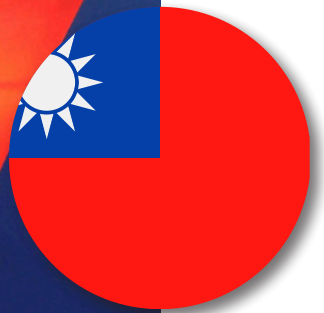
The Financial Services Commission announced its 2021 Work Plan, which outlines its key achievements for 2017-2020 and its four major policy tasks for 2021. The 2021 policy tasks aim to:

- "Maintain the COVID-19 financial support and manage potential risks
- Pursue new deal financing & promote green finance
- Promoting financial innovation and further advancement of digital finance
- Work on financial consumer protection and strengthen support for financially vulnerable groups"[87]

The plan seeks to future-proof key growth areas due to South Korea's low birth rate and aging population, as well as establish regulatory and supervisory frameworks in response to emerging technologies. In supporting financial innovation, digital finance and the New Deal, the FSC outlines several key goals, including the increased usage of contactless financial services, expanded financial assistance to innovative firms, the establishment of a digital finance infrastructure and the accelerated growth of the fintech industry. Toward these ends, the FSC aims to allow credit card companies to provide open banking services; establish standards on the use of mobile-based, contactless authentication and identity verification systems; bolster investment and sandbox initiatives for fintech companies; support the development of AI-based financial services and promote the use of big data. As the digital economy rapidly grows and becomes more complex, regulators must ensure that financial and digital divides do not widen. The plan thus addresses financial consumer protection and heightened support for financially vulnerable groups, with goals to strengthen investor protection in capital markets, improve support programs and bolster management of "damage-prone" areas like crypto assets.

Proposed Amendment to the Electronic Financial Transactions Act Submitted to the National Assembly, 27 November 2020

The Proposed Amendment to the Electronic Financial Transactions Act (EFTA) was submitted to the National Assembly in a move to strengthen financial security and support the digitalization of the financial industry by simplifying and improving the existing law. **The Electronic Financial Transactions Act** aims to promote economic development by ensuring the safety and reliability of electronic financial transactions, and is applicable to electronic financial businesses like electronic funds transfer services. The Proposed Amendment to the EFTA implements the Digital Finance Transformation Plan, published in July 2020 by the Financial Services Commission, and streamlines the regulatory framework for several e-money and e-payment services, establishes infrastructure for digital financial transactions, strengthens protections for digital finance users and strengthens data security.[88] The draft law also aims to safeguard and promote the continuity, scalability and stability of the open banking system.[89]



Taiwan

Country Overview

Taiwan skillfully leveraged innovative technologies in managing the COVID-19 pandemic, which led to relatively few cases, spared the nation from economic devastation and drove further digital transformation. GDP expanded by 2.98% in 2020, making Taiwan Asia's top-performing economy of the year,[90] and economic growth is forecasted to surge by 5.46% in 2021.[91] The Institute for Management Development (IMD) ranked wealthy and fintech-friendly Taiwan as the world's 8th most competitive economy in its 2021 World Competitiveness Yearbook.

In August 2020, President Tsai Ing-wen laid out an ambitious goal for the Taiwanese economy. "We are going to make Taiwan the number one center in Asia for capital movement and establish ourselves as a wealth management center," said Tsai. "This means loosening rules and providing more diversified financial products and services."[92] Also in August 2020, the Financial Supervisory Commission released its fintech development roadmap, which will facilitate data sharing amongst financial holding companies' subsidiaries.[93] Indeed, the accelerated adoption of disruptive technologies like open data and AI will be key in revolutionizing the Taiwanese financial and banking sectors, whose services and products are increasingly offered by competitors in fintech.

Taiwan has already made great strides towards digital transformation in finance and banking. The September 2020 Bill on the Development of Artificial Intelligence establishes a regulatory framework to promote the safe use of AI in the economy, which could be key in promoting technologies that support remote onboarding and biometric authentication. The city of Taipei, per a February 2021 **white paper** on digital transformation, also plans to spearhead the adoption of innovation in the economy. The paper outlines fifteen action plans to boost the development of digital infrastructure, a "stay-at-home economy," contactless services and digital talent, hinging on key initiatives like the establishment of a big data center and the promotion of digital payments.

Taiwan's 2021 digital platform focuses on bolstering the national cybersecurity framework, reconciling the national data protection framework with the EU's GDPR, regulating virtual currencies and promoting digital transformation. Its agenda strikes an expert balance in fostering digitalization while also mitigating the risks that come with it, like increased data protection concerns, sophisticated cyberthreats and AML/CFT risks in virtual currencies. In June 2021, the central bank revealed that it has been investigating the possible introduction of a central bank digital currency, but that it does not have a timeframe for its development.[94]

Financial Regulatory Authorities

The Central Bank of the Republic of China (Taiwan) is the central bank of Taiwan. The bank issues the country's currency and develops monetary and payment system policies. The bank operates through several departments, including a Department of Banking.

The Financial Supervisory Commission (FSC) is the independent government agency supervising and regulating the securities markets, as well as the banking and insurance sectors.

Policy, Laws and Regulations

Draft Regulations on AML Measures Regarding Virtual Currencies, 25 May 2021

The Taiwanese Financial Supervision and Administration Commission issued its draft Measures for Preventing Money Laundering and Combating Capital Terrorism on Virtual Currency Platforms and Transaction Business Undertakings, which outlines 18 regulations based on recommendations from the Financial Action Task Force (FATF). The regulations require operators of virtual currency platforms to conduct customer due diligence, continuous review of customer identity and continuous monitoring of customer transactions, as well as report on suspicious activities and adopt the FATF's "Travel Rule." Per the travel rule—which seeks to crack down on the exploitation of crypto's anonymity for the purposes of AML/CFT—originators and beneficiaries of digital funds transfers must share identification information, including name and account number. Other key requirements address the declaration of currency transactions above a certain amount, the implementation content of the internal control and audit system, preservation of the business record and the notification method and procedure.

The Financial Supervisory Commission has been especially eager to impose transaction reporting requirements. On 20 April 2021, the authority announced that, effective 01 July 2021, all cryptocurrency exchanges must report cash transactions of over NT $500,000 (approximately USD$17,770) or its equivalent in a foreign currency.[95]

National Cybersecurity Strategy, 04 May 2021

President Tsai Ing-wen announced at a CYBERSEC 2021 event that the government would soon introduce a "Cybersecurity is National Security Strategy 2.0," upgraded from a first version launched in 2018. The strategy will establish a ministry of digital development and a department for cybersecurity in an aim to safeguard critical infrastructure and core databases, implement new regulations and foster talent.[96] The spring of 2021 saw a spate of high-profile cyberattacks against Taiwanese companies, which have increasingly moved to incorporate cybersecurity in their business models. Cyberattacks against Taiwanese government agencies have especially risen, and the Taiwanese Ministry of Foreign Affairs was attacked forty times more in 2020 than in 2018.[97]

Order on the Operation of the MyData Platform, 14 April 2021

The executive order on the promulgation of Operation Directions Governing the Interconnection of MyData was published in the official gazette, thus officially launching the MyData platform, in partnership with fifteen Taiwanese banks. The MyData platform, which has been in trial operation since July 2020, gives individuals control over their personal data by allowing them to download personalized data and consent to its transmission to third parties. Banks have been utilizing the platform to offer financial services like online credit card applications, online loans and remote deposit account openings. The order also provides an overview of operation of the MyData platform, alongside requirements for entities seeking to function as a data or service provider on the platform.

Amendment to Act Governing Electronic Payment Institutions, 27 January 2021

A presidential order promulgating the amendment to the Act Governing Electronic Payment Institutions was published in the official gazette. The amended act clarifies a previously fragmented payments framework, facilitates the development of electronic and mobile payments, boosts convenience in payments, promotes financial inclusion and adopts a risk-based approach in regulating the electronic and mobile payments industries. In a move towards encouraging competition, development of fintech companies and innovations in payments, the amended act widens the scope of businesses that qualify as electronic payment institutions (EPI), including secondary businesses that are complementary to EPIs.[98] The amended act also enables inter-EPI fund settlements, without the previous requirement of bank involvement, thus encouraging EPIs to expand their businesses. With FSC approval, EPIs may establish foreign branches and conduct cross-border transactions. EPIs may also open accounts with non-bank institutions, like credit departments of cooperatives and associations, in a move to encourage financial inclusion in underserved communities.

Legislation

Draft Amendments to the Personal Data Protection Act, 16 April 2021

The Draft Amendments to Articles 2 and 3 of the Personal Data Protection Act was submitted to the Taiwanese Legislative Yuan. The bill seeks to align the Taiwanese data protection framework more closely with the EU's GDPR. It amends issues on the right of access by data subjects and includes "online identifiers" in the statutory definition of personal data. The amendments follow the introduction of the Digital Rights and Personal Data Protection Commission Organisation bill, which aims to bring Taiwan's data protection framework in adherence with the GDPR such that an adequacy regime may be established for the cross-border transfer of personal data between Taiwan and the EU. The Digital Rights and Personal Data Protection Commission Organisation bill would also establish a national data protection authority.

Thailand

Country Overview

Thailand has long been a notable emerging market due to its solid GDP growth, poverty reduction and modernization efforts, but in recent years its progress has stalled. A slowdown in public investments, lower demand for exports, challenges to agricultural production and education system shortcomings have all contributed to faltering economic and social outcomes.[99] The COVID-19 pandemic further exacerbated Thailand's weakening economic performance as exports shrunk and the tourism sector came to a halt.

The Thai economy contracted by 6.1% in 2020,[100] with a shrinkage of 2.6% in the first quarter of 2021,[101] and its recovery is forecasted to be slow and rocky.[102] In April 2021, Thailand's most severe outbreak of COVID-19 infections hit, further dampening the country's economic prospects. The central bank maintains that the Thai banking system is still strong, with high capital buffers and liquidity safeguarding against a more drastic economic performance.[103]

Meanwhile, the pandemic drove surges in e-commerce, digital payments and overall digitalization efforts in Thailand. The Thai government has historically been eager to promote digital transformation in the economy and society. In 2016, the government launched the Thailand 4.0 initiative, which has sought to propel economic growth through the development and adoption of innovative technologies. Alongside expansions in smartphone ownership and internet connectivity, Thai banks have increasingly invested in digital infrastructures[104] like blockchain technology and mobile banking solutions. Shifting consumer preferences, especially given Thailand's young and tech-savvy population, will further encourage competition in the banking sector. A key challenge will be ensuring that digitalization does not widen socioeconomic inequalities between Bangkok and rural areas.

Thailand's 2021 digital agenda focuses on the possible development of a central bank digital currency (CBDC), regulating virtual currencies, improvements to the AML/CFT framework and adopting innovative technologies while mitigating risk. The Bank of Thailand's **Strategic Plan 2020-2022** identified seven strategic challenges to address, including the rapid digitalization of the financial sector, cyber threats and challenges to the central bank's independence. Additionally, the Electronic Transactions Development Agency (ETDA) is reportedly developing a Digi-ID and spearheading the widespread government adoption of e-signatures.[105] A more digitally robust Thailand could help to reassert the country's status as a major emerging market, attract more foreign direct investment, bolster its reputation as a Southeast Asian innovation hub and reach its goal of being a high-income country.

Financial Regulatory Authorities

The Bank of Thailand (BOT) is the central bank of Thailand.

The Securities and Exchange Commission (SEC) supervises the Thai capital market and ensures fairness and transparency.

Other Regulatory Authorities

The Anti-Money Laundering Office (AMLO) enforces the Anti-Money Laundering Act 1999.

Policy, Laws and Regulations

Thai Cabinet Postpones Enforcement of Personal Data Protection Act, 05 May 2021

Due to the COVID-19 pandemic, the Thai Cabinet postponed the enforcement of the Personal Data Protection Act (PDPA) to 01 June 2022. The PDPA, which was published in May 2019, draws on the EU's General Data Protection Regulation (GDPR) and outlines requirements for the processing of personal data and the responsibilities of data controllers and processors. The law has extraterritorial scope, so it applies to any entity that utilizes the personal data of a Thai citizen, even if the entity does not reside in Thailand. In the case of cross-border transfers of personal data, the recipient country must adhere to "adequate personal data protection standards." The PDPA will also establish a national data protection agency to monitor compliance, called the Personal Data Protection Committee (PDPC).

Anti-Money Laundering Office Announces New Identity Verification Requirement for Crypto Exchanges, 03 May 2021

The Anti-Money Laundering Office announced that crypto exchanges must conduct identity verification of new customers in-person, utilizing a dip-chip machine. The dip-chip machine will scan chips embedded in Thai ID cards, precluding investors from submitting documents online as previously allowed. The move aims to tamp down on document forgery and the exploitation of anonymity in crypto for illegal activities, and could prevent non-Thais from accessing exchanges. Thai interest in crypto assets has soared, with the number of accounts registered with Thai crypto exchanges at 700,000 in early May, up from 160,000 at the end of 2020.[106] The Bank of Thailand is concerned about the possible implications of the widespread adoption of privately-issued currencies, which could threaten financial stability, and the strict measure could significantly deter potential new investors. The requirement went into effect 01 July 2021.

Thailand and Singapore Launch Linkage of Real-Time Payment Systems, 29 April 2021

The Bank of Thailand and the Monetary Authority of Singapore (MAS) introduced the linkage of Thailand's PromptPay and Singapore's PayNow real-time retail payment systems. The first system of its kind in the world, customers at participating banks will be able to make real-time transactions of up to S $1000 or THB 25,000 per day across the two countries. The system will be simple to use—similar to using PromptPay and PayNow's domestic interfaces—and customers will need only a mobile number to complete a transaction. Transfers of funds will take mere minutes. In Thailand, Bangkok Bank Kasikornbank, Krung Thai Bank and Siam Commercial Bank will offer the service, although the Bank of Thailand and the Monetary Authority of Singapore plan to increasingly scale up the system to include more participants and allow for a higher limit on funds. Eventually, the partnership aims to broaden the linkage to encompass other retail payment systems across ASEAN.

Cross-border linkages of real-time payment systems is very exciting and will make the world a little smaller. The security and convenience Singapore and Thailand have brought to their banking customers is just the beginning. Future linkages to more countries' real-time payment systems will improve international commerce.

"This service by the MAS and the BOT will effectively address customers' long-standing pain points in the area of cross-border transfers and remittances, including long transaction times and high costs," BOT Governor Sethaput Suthiwartnarueput said in a joint statement.

Bank of Thailand Investigating a CBDC, 01 April 2021

The Bank of Thailand published a discussion paper entitled *The Way Forward for Retail Central Bank Digital Currency in Thailand*, which overviews the bank's investigation into the possible introduction of a retail CBDC, alongside the opportunities, risks and challenges it would present. Through Project Inthanon, a 2018-2020 pilot project in partnership with eight commercial banks, the Bank of Thailand successfully created a proof-of-concept wholesale CBDC prototype based on distributed ledger technology (DLT). The prototype was tested in several use cases, including a successful cross-border transfer in partnership with the Hong Kong Monetary Authority. In late 2020, the central bank began to explore the role of a CBDC in business, for functions like trade and conditional payments. On 07 March 2021, the Bank of Thailand published a **report** entitled *Central Bank Digital Currency: The Future of Payments for Corporates - Leveraging Technology to Enhance Efficiency and Innovation in the Business Sector*, which outlines this recent phase of investigation.

The discussion paper identifies the emergence of privately-issued digital currencies as the principal motivation in exploring the possible development of a CBDC. A widespread usage of privately-issued currencies could eventually put Thailand's monetary and financial stability, users and payment systems at risk. A CBDC would offer a safe, reliable and accessible alternative, but it would also pose risks, including the disintermediation of financial intermediaries and an increased possibility of bank runs.

A CBDC system would also require "maintenance of high security standards and public trust." Despite such risks and challenges, the Bank of Thailand remains confident in its risk mitigation measures, and identifies three capacities in ensuring a successful CBDC implementation: user accessibility, digital infrastructure and legal and regulatory frameworks. Going forward, the central bank does not believe there is an immediate need to issue a CBDC, but still aims to take the necessary steps towards its possible development. Per the paper, over 2021-22, "...we intend to focus our efforts on the research and development of a retail CBDC while closely monitoring business adoption, consumer trends and technology advancements."

Bank of Thailand Stablecoins Regulation Policy, 19 March 2021

The Bank of Thailand released its stablecoins regulation policy in a press release, which briefly outlines requirements for baht-backed stablecoins. Since they are pegged to the local currency, baht-backed stablecoins are classified as e-money per the Payment Systems Act 2017. Entities seeking to provide services involving baht-backed stablecoins are required to first consult with the Bank of Thailand. Before pursuing regulatory guidelines on other stablecoins, the bank welcomes comments and feedback. The press release reiterates the bank's interest in adopting innovative technologies, and points to its investigation into the development of a retail CBDC. The policy comes a day after the bank banned the use of the Thai Baht Digital (THT), a stablecoin issued on the Terra platform.

Anti-Money Laundering Office Publishes Guidelines on Risk Factors and Risk Management in Money Laundering, Terrorist Financing and Proliferation Financing (ML/TF/PF), 27 January 2021

The Anti-Money Laundering Office passed a spate of guidelines to further implement provisions of the Ministerial Regulation on Customer Due Diligence, which came into effect 12 August 2020. The regulation:

- Clarifies and expands upon the definition of a Politically Exposed Person (PEP)
- Strengthens customer due diligence and know-your-customer (KYC) measures in certain contexts
- Streamlines risk assessment and mitigation measures to more closely align with international standards

- Requires that, in the case of the international transfer of electronic funds below THB 50,000 (approximately USD$1500), the transferring financial institution transmit information on the parties involved to the receiving financial institution[107]

The regulation applies to financial institutions and other entities.

The **Guideline for Consideration of ML/TF/PF Risk Factors** requires obliged entities to apply appropriate risk assessment measures in conducting business. This includes monitoring the customer profile, transaction patterns, products and services, delivery channels and geographic location. Closely related, The **Guidelines for Formulating Policies and Procedures for Assessment, Management and Mitigation of ML/TF/PF Risks** calls for a risk-based approach to the adoption and implementation of AML/CFT policies and procedures.

The **Guidelines for Customer and Beneficial Owner Verification and Identification** provides an overview of methods and requirements for verifying and identifying customers and beneficial owners, such as checking information against government agency databases and certifying accuracy. The guidelines come on the heels of a 14 December 2020 **announcement** from the Anti-Money Laundering Office on exemptions from beneficial ownership identification requirements. Financial institutions and other firms are exempt from conducting beneficial ownership identification when dealing with customers from foreign governments, state agencies and listed companies from jurisdictions that present low ML/TF risks.

On 01 February 2021, the Anti-Money Laundering Office published another document further implementing provisions of the Ministerial Regulation on Customer Due Diligence. The **Guidelines for Formulating ML/TF/PF Risk Management Measures Arising From the Release of New Products, Services and Technologies** calls for obliged entities to conduct a risk assessment prior to the release of a new product.

Bank of Thailand Publishes Annual Report 2020, January 2021

The Bank of Thailand published its Annual Report 2020, which overviews the effects of the COVID-19 pandemic, its activities for 2020 and its future goals. Major focuses for 2020 included the alleviation of pandemic-related strain on the financial sector and Thai citizens, continued investigation into the development of a CBDC and the strengthening of the digital payments infrastructure. Going forward, the bank will focus on promoting innovation through the regulatory sandbox, integrating digital technology and data into operations, boosting monetary and fiscal transparency, reducing inequality and utilizing supervisory technology in overseeing financial stability and responding to new risks. The report also emphasizes the importance in securing Thailand's cybersecurity resilience readiness in the financial sector, which will require improvements to IT risk management systems, developing and implementing monitoring tools to detect and deter risks, bolstering cybersecurity awareness and establishing cybersecurity partnerships within the sector.

Guidelines for PromptPay Services for e-Money Services, 29 December 2020

The Bank of Thailand published a circular on "Guidelines for PromptPay services for e-Money services," which repeals and replaces a previous circular. The new circular takes into account the emergence of technological innovations in remote identification for the KYC process, particularly the use of biometrics for identity verification. The approval of biometrics in identity verification for PromptPay, a money transfer platform created by the Thai government, comes amidst a system-wide effort to modernize Thai banking services. In 2020, the Bank of Thailand published guidelines approving the use of biometric technology for KYC by financial services. The guidelines require financial institutions to adhere to certain security standards, accurately assess the customer and institute an operational risk management system. Facilitating remote onboarding and other digital banking services is key in promoting financial inclusion, especially amidst COVID-19 lockdowns and other safety-related measures. Indeed, PromptPay saw an 11.4% increase in usage in 2020 compared to 2019,[108] and Kasikornbank (KBank) revealed that transactions on its K Plus mobile banking app grew by 71%.[109] The Bank of Thailand is reportedly considering the implications of allowing for the establishment of virtual banks, which would facilitate increased access to financial services, boost efficiency and encourage competition and innovation.[110]

Vietnam

Country Overview

Vietnam was relatively unscathed by the COVID-19 pandemic, which has allowed its government to focus less on recovery and more on spearheading ambitious economic, digital and social reforms. Indeed, the Southeast Asian nation had one of the world's highest economic growth rates in 2020, at 2.9%, and it is projected to grow by 6.5% in 2021.[111] Alongside its promising economic prospects, the traditionally agrarian and cash-reliant country is in the midst of a booming digital transformation. Although cash use remains high and many consumers are skeptical of e-commerce, Vietnam's young and tech-savvy population, increasing internet connectivity and shifting consumer preferences have accelerated the country's digitalization of economy and society. Indeed, Vietnam ranks fifth in the world for its digital evolution momentum on the **2020 Digital Intelligence Index (DII),** developed by Tufts University's Fletcher School and Mastercard.

The COVID-19 pandemic was particularly instrumental in driving Vietnamese towards digital payment solutions. E-commerce soared by 18% in 2020 from 2019[112] and contactless payments penetration was up 230% in the first quarter of 2021 compared to the same period in 2020.[113] This trend is only expected to accelerate, with mobile transactions forecasted to grow by 300% between 2021 and 2025.[114] The digital economy as a whole is projected to reach USD$52 billion by 2025.[115]

The Vietnamese government and banking sector have welcomed this surge in digitalization, which will attract more fintech and foreign direct investment funds, boost financial inclusion and help Vietnam to compete with other ASEAN and global markets. Banks have readily adopted digital solutions like biometric authentication and online banking, and the government has been especially eager to tap into 2020's digital wave. On 03 June 2020, the government passed the "National digital transformation program to 2025, with orientation to 2030," which aims to develop and support Internet of Things (IoT) infrastructure, digital government platforms and network security, with 70% of all customer transactions completed through digital channels by 2025.[116] The 2021 digital agenda focuses on the development of artificial intelligence, online banking solutions, data protection and the regulation of cryptocurrencies. A regulatory sandbox for fintech is reportedly in the works. Going forward, the government must ensure that its regulatory framework keeps up with the rapid pace of digitalization and mitigates the risks that come with it.

Financial Regulatory Authorities

The State Bank of Vietnam (SBV) is the central bank of Vietnam.

The National Financial Supervisory Commission (NFSC) supports the Prime Minister in the supervision of the financial markets.

Policy, Laws and Regulations

Ministry of Finance Commissions Research Group on Cryptocurrencies, 30 March 2021

The Ministry of Finance commissioned a research group to study cryptocurrencies, with the goal of eventually developing legislative reform. The research group has been assigned with understanding the cryptocurrency industry, crafting legislation that takes into account its rapidly evolving landscape, recommending structural changes that create supervisory bodies and recommending measures to these bodies. In developing legislation, the research group will analyze crypto regulations from Japan, the EU and US. The group is composed of nine members from state agencies and is headed by Phạm Hồng Sơn, deputy chairman of the State Securities Commission. The issuance, supply and use of virtual currencies are currently illegal in Vietnam, and violations can incur fines of up to VND 300,000,000 (approximately USD$12,900) or imprisonment of up to three years.[117] However, the possession of crypto assets is not explicitly prohibited, which has created uncertainty. A more comprehensive regulatory framework would be beneficial in allowing Vietnam to tax cryptocurrency holdings, clear up legal uncertainties and ensure that dealings in virtual currencies adhere to AML legislation.

The State Bank has been particularly adamant in cracking down on crypto ever since a high-profile 2018 crypto scam cost investors a total of approximately USD$658 million.[118] In January 2021, the State Bank issued a directive to organizations issuing bank cards, intermediary payment service providers and representative offices of foreign banks, calling on them to monitor transactions to ensure they do not involve illegal activity, including cryptocurrency.[119]

Vietnam Unveils National Strategy on R&D and Application of Artificial Intelligence, 17 March 2021

Vietnamese Prime Minister promulgated the National Strategy on the Research, Development and Application of Artificial Intelligence until 2030, which outlines goals for 2025 and 2030. Targets for 2025 include boosting the number of AI startups and investment funds for the sector, alongside the widespread adoption of AI in public administration. Targets for 2030 include establishing Vietnam amongst the top four ASEAN countries and top fifty global countries for AI, the creation of three national centers for big data storage and high-performance computing, the creation of three national AI innovation centers and the application of AI towards encouraging economic growth. The plan further outlines goals for fifteen government ministries, including the State Bank. Overarching themes include bolstering public sector productivity, lowering costs and waiting times, and strengthening national security. Vietnam has already made significant strides towards the digitalization of government. In December 2020, the Vietnamese Ministry of Information and Communications inaugurated the national data portal, which will enable citizens' digital access to documents, apps, services and tools supplied by government agencies.

Ministry of Public Security Releases Second Version of Draft Decree on Personal Data Protection, 09 February 2021

The Ministry of Public Security (MPS) released the second version of the Draft Decree on Personal Data Protection, the first version of which was issued in 2019. The new draft is more comprehensive and imposes stricter noncompliance measures. Like Europe's GDPR, the decree has extraterritorial scope in that it would apply to all organizations and individuals that conduct activities related to the processing of Vietnamese' personal data, even if the organization or individual is not physically located in Vietnam. Proposed regulations include the creation of a Personal Data Protection Committee (PDP Committee) to oversee compliance, a fine of up to 5% of total revenue generated in Vietnam for a repeat violation, notification of the data subjects of all personal data processing activities and obtaining data subjects' consent before processing of personal data. Cross-border transfers of personal data may only be conducted if certain conditions have been met, including data subjects' consent, the storage of the original data within Vietnam and written permission by the PDP Committee. The processing of sensitive personal data must be registered with the PDP Committee before the start of processing.

State Bank Issues Circular on Remote Onboarding and eKYC, 04 December 2020

The State Bank of Vietnam issued Circular 16, which enables remote onboarding (the "e-method") for the opening of individuals' payment accounts and eKYC. Banks and foreign banks' branches (banking entities) that employ the e-method must include several steps in their procedures:

- Collection of information for the individual payment account opening dossier as required
- Verification of KYC information
- Warning to customers regarding prohibited acts during the opening and use of accounts by the e-method
- Require customers to sign the payment account opening and user agreement
- Inform customers about important account details such as activation date and transaction limit[120]

For the eKYC, banking entities may develop their own procedures as long as minimum standards are met, including adequate procedures for risk management, storing and preserving eKYC information. Banking entities must also take a risk-based approach to setting transaction limits, with a cap on debit transactions at VND 100 million (approximately USD$4,380) per customer per month. The threshold may be higher if banks conduct video calls to verify the customer's identity. The circular went into effect 05 March 2021.

Endnotes

1 Hutchens, Gareth et al. "GDP figures show economy shrank in 2020 but grew 3.1 per cent in December quarter." Australian Broadcasting Corporation, 02 March 2021. https://www.abc.net.au/news/2021-03-03/gdp-december-quarter-2021/13210412.

2 "Australia in first recession for nearly 30 years." BBC, 02 September 2020. https://www.bbc.co.uk/news/business-53994318.

3 Pandey, Swati. "Analysis: Shut off from the world, Australia fosters red-hot growth at home." Reuters, 28 June 2021. https://www.reuters.com/world/asia-pacific/shut-off-world-australia-fosters-red-hot-growth-home-2021-06-27/.

4 Pandey, Swati. "Australia's economy booms to pre-pandemic levels as consumers, businesses spend." Reuters, 02 June 2021. https://www.reuters.com/world/asia-pacific/australia-gdp-climbs-18-q1-back-pre-pandemic-time-2021-06-02/.

5 "Australia Covid: Seventh city locks down amid vaccine chaos." BBC, 01 July 2020. https://www.bbc.co.uk/news/world-australia-57661144.

6 Kowalkiewicz, Marek. "Did someone drop a zero? Australia's digital economy budget spend should be 10 times bigger." The Conversation, 12 May 2021. https://theconversation.com/did-someone-drop-a-zero-australias-digital-economy-budget-spend-should-be-10-times-bigger-160626.

7 Libatique, Roxanne. "What key issues must the financial sector address post COVID-19?" Insurance Business, 29 April 2021. https://www.insurancebusinessmag.com/au/news/breaking-news/what-key-issues-must-the-financial-sector-address-post-covid19-253567.aspx.

8 "Australia's AI Action Plan." June 2021. https://www.industry.gov.au/sites/default/files/June%202021/document/australias-ai-action-plan.pdf.

9 "Digital Economy Strategy 2030." https://digitaleconomy.pmc.gov.au/sites/default/files/2021-05/digital-economy-strategy.pdf.

10 "Australia's Digital Economy." https://digitaleconomy.pmc.gov.au/strategy/foundations/cyber-security.

11 "Australia's Digital Economy." https://digitaleconomy.pmc.gov.au/strategy/foundations/cyber-security.

12 Brookes, Joseph. "Govt unveils digital ID private sector expansion plans." InnovationAus, 10 June 2021. https://www.innovationaus.com/govt-unveils-digital-id-private-sector-expansion-plans/.

13 Khadem, Nassim. "Are Australians at a 'turning point' on cybersecurity or still unprepared?" Australian Broadcasting Corporation, 10 January 2021. https://www.abc.net.au/news/2021-01-11/australians-turning-point-on-cyber-security-cyberattacks-crime/13018884.

14 Leung, Kanis. "Hong Kong economy suffers biggest annual contraction on record, shrinking 6.1 per cent as coronavirus hammers tourism, local spending." South China Morning Post, 29 January 2021. https://www.scmp.com/news/hong-kong/hong-kong-economy/article/3119795/hong-kong-economy-suffers-biggest-annual.

15 Lee, Yen Nee. "Hong Kong's economy is not out of the woods despite sharp rebound, says commerce secretary." CNBC, 03 June 2021. https://www.cnbc.com/2021/06/03/hong-kong-economy-commerce-secretary-on-trade-recovery-from-covid.html.

16 Leung, Kanis. "Hong Kong economy grows 7.9 per cent in first quarter, higher than projected." South China Morning Post, 14 May 2021. https://www.scmp.com/news/hong-kong/hong-kong-economy/article/3133494/coronavirus-hong-kong-economy-grows-79-cent-first.

17 "Hong Kong Budget 2021-22: Blueprint for Economic Recovery." China Briefing, 10 March 2021. https://www.china-briefing.com/news/hong-kong-budget-2021-22-blueprint-for-economic-recovery/.

18 Alois, JD. "Artificial Intelligence in Banking: Hong Kong Academy of Finance Publishes Report on AI and Fintech." Crowdfund Insider, 21 August 2020. https://www.crowdfundinsider.com/2020/08/165566-artificial-intelligence-in-banking-hong-kong-academy-of-finance-publishes-report-on-ai-and-fintech/.

19 "Hong Kong's e-commerce growth will continue beyond COVID-19 pandemic, says GlobalData." GlobalData, 22 March 2021. https://www.globaldata.com/hong-kongs-e-commerce-growth-will-continue-beyond-covid-19-pandemic-says-globaldata/.

20 "Hong Kong's Fintech Industry Booms As Consumers Turn To Mobile Solutions." Forbes, 01 March 2021. https://www.forbes.com/sites/hongkong/2021/03/01/hong-kongs-fintech-industry-booms-as-consumers-turn-to-mobile-solutions/?sh=30e4f6054a6e.

21 Yiu, Enoch. "HKMA piles pressure on small lenders to digitise as Hong Kong's virtual banks gain traction with customers." The South China Morning Post, 17 March 2021. https://www.scmp.com/business/banking-finance/article/3125662/hkma-piles-pressure-small-lenders-digitise-hong-kongs.

22 Bower, Matt et al. "A guide to Hong Kong's cyber security laws and practices." Allen & Overy. https://www.jdsupra.com/legalnews/a-guide-to-hong-kong-s-cyber-security-1037956/?origin=CEG&utm_source=CEG&utm_medium=email&utm_campaign=CustomEmailDigest&utm_term=jds-article&utm_content=article-link.

23 Tsang, Denise. "Hong Kong closer to launching unprecedented HK$22.4 billion investment vehicle with appointment of top executives." The South China Morning Post, 30 September 2020. https://www.scmp.com/news/hong-kong/hong-kong-economy/article/3103734/hong-kong-closer-launching-unprecedented-hk224.

24 "The Next Phase of the Banking Open API Journey." Hong Kong Monetary Authority and Accenture. https://www.hkma.gov.hk/media/eng/doc/key-functions/ifc/fintech/The_Next_Phase_of_the_Banking_Open_API_Journey.pdf.

25 Gamio, Lazaro and James Glanz. "Just How Big Could India's True Covid Toll Be?" The New York Times, 25 May 2021. https://www.nytimes.com/interactive/2021/05/25/world/asia/india-covid-death-estimates.html.

26 Kumar, Manoj. "Coronavirus curbs in India disrupt supply chains, stoke economy worries." Reuters, 15 April 2021. https://www.reuters.com/world/india/coronavirus-curbs-india-disrupt-supply-chains-stoke-economy-worries-2021-04-15/.

27 Li, Shan and Vibhuti Agarwal. "India's Covid-19 Surge to Hamper Economic Recovery."

28 Mishra, Ankit. "Leading Experts Weigh In On Growing India's Economy From Covid-19." Forbes, 15 June 2021. https://www.forbes.com/sites/ankitmishra/2021/06/15/leading-experts-weigh-in-on-growing-indias-economy-from-covid-19/?sh=685047d53929.

29 Mukherji, Biman. "When will India's economy recover from its second COVID wave? Economists are split." Fortune, 01 June 2021. https://fortune.com/2021/06/01/india-economy-gdp-recovery-covid-second-wave/.

30 "Indian e-commerce to grow 84% in 4 years, helped by Covid-19 impact: Study." Business Standard, 10 March 2021. https://www.business-standard.com/article/economy-policy/indian-e-commerce-to-grow-84-in-4-years-helped-by-covid-19-impact-study-121031000846_1.html.

31 "It's time for digital currency to counter crypto, says RBI." The Times of India, 23 July 2021. https://timesofindia.indiatimes.com/business/india-business/its-time-for-digital-currency-to-counter-crypto-says-rbi/articleshow/84662839.cms.

32 "How Japan can make digital 'big moves' to drive growth and productivity." McKinsey, 24 February 2021. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-japan-can-make-digital-big-moves-to-drive-growth-and-productivity.

33 "Japan's economy shrinks 4.8% in 2020 due to Covid." BBC, 15 February 2021. https://www.bbc.co.uk/news/business-56066065.

34 "OECD raises 2021 global growth outlook while cutting Japan forecast." The Japan Times, 31 May 2021. https://www.japantimes.co.jp/news/2021/05/31/business/economy-business/oecd-2021-outlook/.

35 Obe, Mitsuru. "MUFG's 47% earnings jump in 2020 shows banks can thrive amid COVID." Nikkei Asia, 17 May 2021. https://asia.nikkei.com/Business/Finance/MUFG-s-47-earnings-jump-in-2020-shows-banks-can-thrive-amid-COVID.

36 "COVID-19 accelerates e-commerce market growth in Japan, says GlobalData." GlobalData, 22 January 2021. https://www.globaldata.com/covid-19-accelerates-e-commerce-market-growth-japan-says-globaldata/.

37 Faridi, Omar. "Digital Transformation: Japan's Big Banks are Studying Virtual Currencies and how to Make Banks and Cashless Payments Systems Interoperable." Crowdfund Insider, 05 June 2020. https://www.crowdfundinsider.com/2020/06/162359-digital-transformation-japans-big-banks-are-studying-virtual-currencies-and-how-to-make-banks-and-cashless-payments-systems-interoperable/.

38 Kihara, Leika and Tetsushi Kajimoto. "Japan unveils $708 billion in fresh stimulus with eye on post-COVID growth." Reuters, 07 December 2020. https://www.reuters.com/article/us-japan-economy-stimulus-idUSKBN28I02Y.

39 Suzuki, Wataru. "Suga vows to lead 'free and open digital space' in Indo-Pacific." Nikkei Asia, 20 May 2021. https://asia.nikkei.com/Spotlight/The-Future-of-Asia/The-Future-of-Asia-2021/Suga-vows-to-lead-free-and-open-digital-space-in-Indo-Pacific.

40 Tsukimori, Osamu. "As cyberattacks rise globally, Japan's digital security found lacking." The Japan Times, 18 September 2020. https://www.japantimes.co.jp/news/2020/09/18/business/japans-cybersecurity-lacking/.

41 Tajima, Yukio. "Japan calls on industry and academia to fortify cyber defenses." Nikkei Asia, 21 October 2020. https://asia.nikkei.com/Business/Technology/Japan-calls-on-industry-and-academia-to-fortify-cyber-defenses.

42 Okabe, Takanori. "Suga digitization push to put all financial filings online by 2022." Nikkei Asia, 15 October 2020. https://asia.nikkei.com/Business/Finance/Suga-digitization-push-to-put-all-financial-filings-online-by-2022.

43 "Japan's central bank kicks off experiments on issuing digital currency." Reuters, 05 April 2021. https://www.reuters.com/article/us-japan-economy-cbdc-idUSKBN2BS0EG.

44 Kuroda, Haruhiko. "Integrating Information and Financial Systems: Beyond As-a-Service." Bank of Japan, 16 March 2021. https://www.boj.or.jp/en/announcements/press/koen_2021/data/ko210316a.pdf.

45 Kajimoto, Tetsushi and Leika Kihara. "Japan ruling party lawmakers to float idea of issuing digital currency." Reuters, 24 January 2020. https://www.reuters.com/article/uk-japan-economy-digital-idUKKBN1ZN0QK.

46 Anand, Ram. "Malaysia's GDP shrinks 5.6% in 2020, worst performance since 1998." The Straits Times, 11 February 2021. https://www.straitstimes.com/business/economy/malaysias-economy-shrinks-faster-than-expected-in-q4-on-tighter-covid-19-curbs.

47 "Malaysian economy showing signs of recovery, projected to grow by 6.7 percent in 2021 following a contraction of 5.8 percent in 2020." The World Bank, 17 December 2020. https://www.worldbank.org/en/news/press-release/2020/12/17/malaysian-economy-showing-signs-of-recovery-projected-to-grow-by-67-percent-in-2021-following-a-contraction-of-58-percent-in-2020.

48 "Contactless payments exceed 50% of transactions." The Star, 23 January 2021. https://www.thestar.com.my/metro/metro-news/2021/01/23/contactless-payments-exceed-50-of-transactions.

49 e-Conomy SEA 2020. Google, Temasek and Bain & Company. https://storage.googleapis.com/gweb-economy-sea.appspot.com/assets/pdf/e-Conomy_SEA_2020_Report.pdf.

50 Lim, Jotham. "TechTalk: Hiring digital talent during MCO 2.0." The Edge Markets, 01 March 2020. https://www.theedgemarkets.com/article/techtalk-hiring-digital-talent-during-mco-20.

51 "Malaysia's Digital Economy – A New Driver of Development." The World Bank, 25 June 2021. https://www.worldbank.org/en/results/2021/06/25/malaysia-s-digital-economy-a-new-driver-of-development.

52 Anand, Ram. "Malaysian PM Muhyiddin's federal budget passes Parliament test." The Straits Times, 26 November 2020. https://www.straitstimes.com/asia/se-asia/malaysian-pm-muhyiddins-federal-budget-passes-parliament-test.

53 "Malaysia Digital Economy." International Trade Administration, 08 December 2020. https://www.trade.gov/market-intelligence/malaysia-digital-economy.

54 Fong, Vincent. "Bank Negara Malaysia Received 29 Applications for Digital Banking License." Fintech News Malaysia, 02 July 2020. https://fintechnews.my/28039/virtual-banking/bank-negara-received-29-applications-for-digital-banking-license/.

55 "Global Cybersecurity Index 2020." ITU Publications, 2021. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.

56 Culpan, Tim. "This Asian Nation Is a Quiet Leader in Cybersecurity." Bloomberg, 01 July 2021. https://www.bloomberg.com/opinion/articles/2021-07-01/malaysia-makes-the-cybersecurity-top-10-with-some-help-from-its-friends.

57 "Will New Zealand become a technological hub? Which are the big tech companies there?" Kalkine Media, 14 June 2021. https://kalkinemedia.com/nz/stocks/technology/will-new-zealand-become-a-technological-hub-which-are-the-big-tech-companies-there.

58 "New Zealand's economy hits record decline in 2020." DW, 18 March 2021. https://www.dw.com/en/new-zealands-economy-hits-record-decline-in-2020/a-56909686.

59 Withers, Tracy. "New Zealand Avoids Recession as Economic Growth Surges." Bloomberg, 16 June 2021. https://www.bloomberg.com/news/articles/2021-06-16/new-zealand-avoids-double-dip-recession-as-economic-growth-jumps.

60 Menon, Praveen. "NZ economy surges as housing, retail drive post-COVID recovery." Reuters, June 16 2021. https://www.reuters.com/world/asia-pacific/nz-economy-surges-housing-retail-drive-post-covid-recovery-2021-06-16/.

61 Raman, Nara et al. "The Land of the Long White Cloud: Turning New Zealand's Recovery into Sustained Growth." International Monetary Fund, 27 May 2021. https://www.imf.org/en/News/Articles/2021/05/25/na052521-the-land-of-the-long-white-cloud-turning-new-zealands-recovery-into-sustained-growth.

62 "Digital Identity Trust Framework." Digital.govt.nz, 12 February 2021. https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/digital-identity-trust-framework/.

63 "Overview Philippines." World Bank, 07 April 2021. https://www.worldbank.org/en/country/philippines/overview.

64 "Philippine economy shrank at record pace in 2020, outlook gloomy." Al Jazeera, 28 January 2021. https://www.aljazeera.com/economy/2021/1/28/philippine-economy-shrank-at-record-pace-in-2020-outlook-gloomy.

65 "IMF Staff Completes Virtual 2021 Article IV Mission to the Philippines." International Monetary Fund, 15 June 2021. https://www.imf.org/en/News/Articles/2021/06/15/pr21177-imf-staff-completes-virtual-2021-article-iv-mission-to-the-philippines.

66 Lim, Jamilah. "Are digital banking entrants in Philippines a catalyst for a digital economy boom?" Tech Wire Asia, 09 June 2021. https://techwireasia.com/2021/06/are-digital-banking-entrants-in-philippines-a-catalyst-for-a-digital-economy-boom/.

67 England, Joanna. "Cryptocurrency to become mainstream in the Philippines." FinTech Magazine, 23 March 2021. https://fintechmagazine.com/digital-payments/cryptocurrency-become-mainstream-philippines.

68 Marasigan, Lorenz S. "PHL partners with Australian institute to enhance National Cybersecurity Plan." Business Mirror, 22 June 2021. https://businessmirror.com.ph/2021/06/22/phl-partners-with-australian-institute-to-enhance-national-cybersecurity-plan/.

69 "Why Filipinos Remain Unbanked: Addressing Banking Challenges In The Philippines." PearlPay, 01 February 2021. https://pearlpay.com/why-filipinos-remain-unbanked/.

70 Abdullah, Saliha Naila A. "BSP Relaxes KYC Requirements to Facilitate Access to Financial Services." MFBR, 20 April 2020. http://mfbr.com.ph/2020/04/20/bsp-relaxes-kyc-requirements-to-facilitate-access-to-financial-services/.

71 Caraballo, Mayvelin U. "BSP looks deeper into CBDC viability." The Manila Times, 09 May 2021. https://www.manilatimes.net/2021/05/09/business/sunday-business/bsp-looks-deeper-into-cbdc-viability/871488.

72 "Philippines plans to establish artificial intelligence research center." Business World, 06 May 2021. https://www.bworldonline.com/philippines-plans-to-establish-artificial-intelligence-research-center/.

73 "DTI to launch National Artificial Intelligence Roadmap." Department of Trade and Industry. https://www.dti.gov.ph/archives/national-artificial-intelligence-roadmap/.

74 Burt, Chris. "Digital ID rollout passes 1M cards in Philippines." Biometric Update, 06 July 2021. https://www.biometricupdate.com/202107/digital-id-rollout-passes-1m-cards-in-philippines.

75 Gatpolintan, Leslie. "3.7M PhilSys registrants now have bank accounts." Philippine News Agency, 23 June 2021. https://www.pna.gov.ph/articles/1144760.

76 "Philippines' Duterte tightens anti-money laundering rules to avoid `grey list'." Reuters, 30 January 2021. https://www.reuters.com/article/us-philippines-moneylaundering/philippines-duterte-tightens-anti-money-laundering-rules-to-avoid-grey-list-idUSKBN29Z0IJ.

77 "South Korea, Singapore, Germany Lead BNEF Ranking of Top Digitalization Markets." BloombergNEF, 24 September 2020. https://about.bnef.com/blog/south-korea-singapore-germany-lead-bnef-ranking-of-top-digitalization-markets/.

78 Lee, Julie Yoonnyung. "Digital technology has helped South Koreans cope with the pandemic. But the elderly have been left behind in the new contact-free era." BBC, 05 August 2020. https://www.bbc.com/worklife/article/20200803-south-korea-contact-free-untact-society-after-coronavirus.

79 Pesek, William. "South Korea Shows OECD How It's Done In Covid-19 Era." Forbes, 29 January 2021. https://www.forbes.com/sites/williampesek/2021/01/29/south-korea-shows-oecd-how-its-done-in-covid-19-era/?sh=418e7e172ea8.

80 Kim, Sam. "Korean Economy Joins China in Surpassing Pre-Pandemic Peak." Bloomberg, 27 April 2021. https://www.bloomberg.com/news/articles/2021-04-26/south-korea-s-economy-grows-more-than-expected-on-investment.

81 "Learning from Korea's Digital Response to COVID-19." World Bank, https://olc.worldbank.org/content/learning-korea%E2%80%99s-digital-response-covid-19.

82 "COVID-19 accelerates e-commerce growth in South Korea, says GlobalData." GlobalData, 09 October 2020. https://www.globaldata.com/covid-19-accelerates-e-commerce-growth-south-korea-says-globaldata/.

83 Kim, Sam. "South Korea Doubles Spending Plan for 'New Deal' to Reshape Economy." BNN Bloomberg, 14 July 2020. https://www.bnnbloomberg.ca/south-korea-doubles-spending-plan-for-new-deal-to-reshape-economy-1.1464887.

84 Im, Felix. "The South Korean parliament has begun discussing a number of bills specifically addressing crypto." Coindesk, 07 June 2021. https://www.coindesk.com/south-korean-parliament-discusses-crypto-bills-for-first-time.

85 Kim, Cynthia. "S. Korea's c.bank moves to develop pilot digital currency." Reuters, 23 May 2021. https://www.reuters.com/business/finance/s-koreas-cbank-moves-develop-pilot-digital-currency-2021-05-24/.

86 "S. Korea to spend 670 bln won on cyber security by 2023." Yonhap News Agency, 18 February 2021. https://en.yna.co.kr/view/AEN20210218006100320.

87 "FSC Announces 2021 Work Plan." Financial Services Commission, 19 January 2021. https://www.fsc.go.kr/eng/pr010101/75201.

88 Cho, Ik Hwan. "In review: digital markets, funding and payment services in South Korea." Lexology, 27 April 2021. https://www.lexology.com/library/detail.aspx?g=9f88650c-d5b1-4d19-86c6-96075c1b639e.

89 Cho, Ik Hwan et al. "Proposed Amendment to Electronic Financial Transaction Act to Transform the Korean Financial Industry." Kim & Chang, 25 March 2021. https://www.kimchang.com/jp/insights/detail.kc?sch_section=4&idx=22885.

90 Lee, Yen Nee. "Taiwan's economy outgrows China's for the first time in 30 years, as chips demand soars." CNBC, 01 February 2021. https://www.cnbc.com/2021/02/01/taiwan-economy-outgrows-china-first-time-in-decades-as-chips-demand-rises.html.

91 Taiwan raises 2021 economic growth forecast to 5.46%." Reuters, 04 June 2021. https://www.reuters.com/article/taiwan-economy-gdp-idUST8N2GJ025.

92 On, Angelica Oung. "Updating Taiwan's Banking System with Fintech." 24 March, 2021. https://topics.amcham.com.tw/2021/03/

taiwan-banking-system-fintech/.

93 Kao, Shih-ching. FSC introduces fintech roadmap. Taipei Times, 29 August 2020. https://www.taipeitimes.com/News/biz/archives/2020/08/29/2003742443.

94 Yang, Sophia. "Taiwan Central Bank's 'govcoin' not ready for rollout yet." Taiwan News, 18 June 2021. https://www.taiwannews.com.tw/en/news/4226514.

95 Kao, Shih-ching. "New cryptocurrency rules to take effect on July 1." Taipei Times, 21 April 2021. https://www.taipeitimes.com/News/biz/archives/2021/04/21/2003756045.

96 Chang, Ya-chun. "Taiwan's president announces new cybersecurity unit." 04 May 2021. https://www.taiwannews.com.tw/en/news/4194694.

97 Lange, Libby and Doowan Lee. "Disinformation, Annexation, & Deterrence: Why the CCP Is More Likely to Subvert Taiwan Than Invade." Lawfare, 22 June 2021. https://www.lawfareblog.com/disinformation-annexation-deterrence-why-ccp-more-likely-subvert-taiwan-invade-0.

98 "Good News For Global Fintechs: Proposed Amendment To Taiwan's Act Governing Electronic Payment Institutions Aims To Consolidate The Development Of Electronic Money And Payment Industries And Streamline The Provision Of Payments." The National Law Review, 18 November 2020. https://www.natlawreview.com/article/good-news-global-fintechs-proposed-amendment-to-taiwan-s-act-governing-electronic.

99 "Overview." The World Bank, May 2021. https://www.worldbank.org/en/country/thailand/overview.

100 Yuda, Masayuki. "Thailand GDP shrinks at fastest pace in over 2 decades." Nikkei Asia, 15 February 2021. https://asia.nikkei.com/Economy/Thailand-GDP-shrinks-at-fastest-pace-in-over-2-decades.

101 "Thailand Q1 slump eases, outlook cut as Covid-19 woes linger." Business Times, 18 May 2021. https://www.businesstimes.com.sg/government-economy/thailand-q1-slump-eases-outlook-cut-as-covid-19-woes-linger-0.

102 "Thai economic recovery slow but financial positions strong -central bank chief." Reuters, 06 May 2021. https://www.reuters.com/article/thailand-economy-idUSL4N2MT40Y.

103 "Thai banks strong, can weather economic uncertainty- c.bank." Reuters, 17 May 2021. https://www.reuters.com/article/thailand-banks-loans-idUSL3N2N41GA.

104 "Digital-savvy customers pushing Thai banks to embrace fintech: S&P." The Business Times, 26 August 2020. https://www.businesstimes.com.sg/banking-finance/digital-savvy-customers-pushing-thai-banks-to-embrace-fintech-sp.

105 Lim, Tian Jiao. "Exclusive: Thailand's vision for trusted digital ID." GovInsider, 20 August 2020. https://govinsider.asia/transformation/thailands-vision-for-a-self-sovereign-digital-id/.

106 Young, Martin. "Thailand to introduce in-person KYC for crypto exchanges." Cointelegraph, 03 May 2021. https://cointelegraph.com/news/thailand-to-introduce-in-person-kyc-for-crypto-exchanges.

107 Rujirawanichtep, Teelada and Napat Siri-armart. "Thailand: Anti-Money Laundering Law In Thailand Due To Be Updated." Mondaq, 07 April 2021. https://www.mondaq.com/money-laundering/1055490/anti-money-laundering-law-in-thailand-due-to-be-updated.

108 "Pandemic speeds up digital drive." Bangkok Post, 02 January 2021. https://www.bangkokpost.com/business/2044455/pandemic-speeds-up-digital-drive.

109 Khajangson, Wongsakrit et al. "Fintech 2021—Thailand." Chambers and Partners, 18 March 2021. https://practiceguides.chambers.com/practice-guides/fintech-2021/thailand/trends-and-developments.

110 "Virtual banks aim to make real impact." Bangkok Post, 24 May 2021. https://www.bangkokpost.com/business/2120607/virtual-banks-aim-to-make-real-impact.

111 Dabla-Norris, Era and Yuanyan Sophia Zhang. "Vietnam: Successfully Navigating the Pandemic." International Monetary Fund, 10 March 2021. https://www.imf.org/en/News/Articles/2021/03/09/na031021-vietnam-successfully-navigating-the-pandemic.

112 "Vietnam's e-commerce market generates $11.8 billion in 2020." VietNamNet, 26 January 2021. https://www.google.com/search?q=vietnam+net+news&rlz=1C1GCEB_enUS949US949&oq=vietnam+net+news&aqs=chrome..69i57j0i22i30l2.2799j0j7&sourceid=chrome&ie=UTF-8.

113 "Visa study finds Vietnamese consumers keen to adopt digital payments to adapt during COVID-19." Visa, 28 April 2021. https://www.visa.com.vn/en_VN/about-visa/newsroom/press-releases/visa-study-finds-vietnamese-consumers-keen-to-adopt-digital-payments-to-adapt-during-covid-19.html.

114 Fintech and Digital Banking 2025 Asia Pacific. Backbase, February 2021. http://go.backbase.com/rs/987-MGR-655/images/Backbase_Fintech_%26_Digital_Banking_2025_APAC_2nd_Edition.pdf?utm_source=Organic&utm_medium=Website&utm_campaign=%5BOM%5D%20IDC%202025&_ga=2.57252578.951222327.1623849348-666338040.1623849348.

115 Boudreau, John and Xuan Quynh Nguyen. "Alibaba, Warburg Want Piece of Vietnam's Online Boom." Bloomberg, 01 June 2021. https://www.bloomberg.com/news/articles/2021-06-01/e-commerce-giants-take-aim-at-vietnam-s-booming-online-market.

116 "Vietnam National Digital Transformation Program Until 2025 And Direction Towards 2030." Renovacloud. https://renovacloud.com/vietnam-national-digital-transformation-program-until-2025-and-direction-towards-2030/?lang=en.

117 "Cryptocurrency Trading Risks In Vietnam." Lexology, 31 March 2021. https://www.lexology.com/library/detail.aspx?g=9b145865-da54-4036-9e4e-9bc95e873a79.

118 Meyer, David. "Vietnam Is Outraged Over a $658 Million Cryptocurrency Scam." Fortune, 12 April 2018. https://fortune.com/2018/04/12/icos-cryptocurrency-scam-vietnam/.

119 Indochine Counsel. "Cryptocurrency in Vietnam." Lexology, 18 January 2021. https://www.lexology.com/library/detail.aspx?g=893ff626-3bc9-4f96-be8d-bc22637b8a65.

120 "eKYC Allowed for Opening of Payment Accounts in Vietnam." Indochine Counsel, December 2020. https://www.indochinecounsel.com/upload/news/SpecialAlert_eKYCAllowedforOpeningofPaymentAccountsinVietnam_Dec2020.pdf.

About the Report

This information is OneSpan's interpretation of the compliance requirements as of the date of publication. Please note that not all interpretations or requirements of the applicable laws are well-settled and its application is fact- and context-specific. The information contained in this document should not be relied upon as legal advice or to determine how the law applies to your business or organization. We encourage you to seek guidance from your legal counsel with regard to law applying specifically to your business or organization and how to ensure compliance. This information is provided "as-is" and may be updated or changed without notice. OneSpan does not accept liability for the contents of these materials.

About OneSpan

OneSpan helps protect the world from digital fraud by establishing trust in people's identities, the devices they use and the transactions they execute. We make digital banking accessible, secure, easy and valuable. OneSpan's Trusted Identity platform and security solutions significantly reduce digital transaction fraud and enable regulatory compliance for more than half of the top 100 global banks and thousands of financial institutions around the world. Whether automating agreements with identity verification and e-signatures, reducing fraud using advanced analytics, or transparently securing financial transactions, OneSpan helps lower costs and accelerate customer acquisition while improving the user experience.
Learn more at **OneSpan.com**.

SOCIAL MEDIA

CONTACT US

OneSpan.com/contact-us


OneSpan
THE UNITED STATES OF AMERICA
FEDERAL RESERVE NOTE
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
中国人民银行
Bank of England
FIVE Pounds
Twenty Pounds
BCE ECB EZB EKT EKP 2002
5 EURO