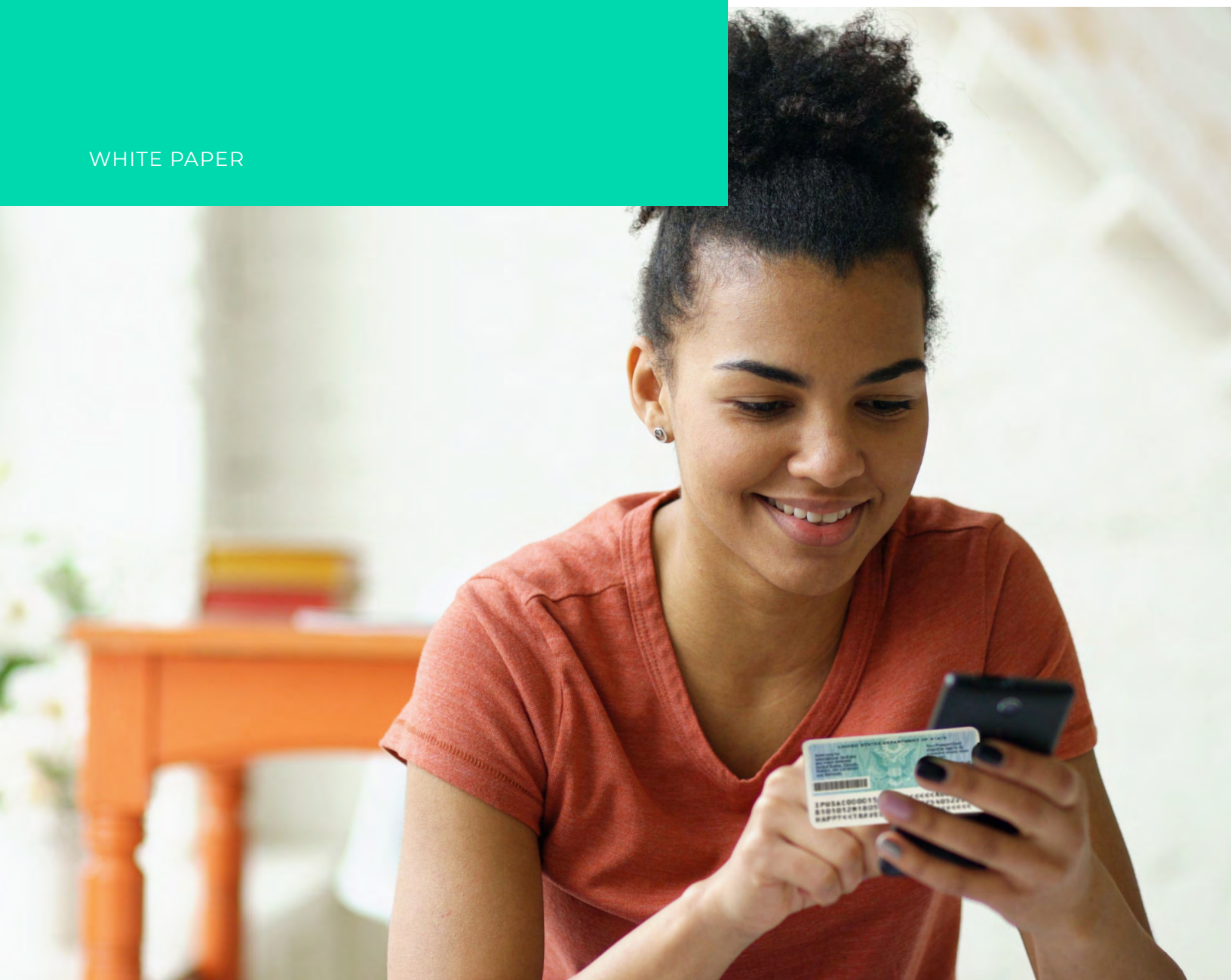
OneSpan
Be bold. Be secure.

# DIGITAL ACCOUNT OPENING

## HOW TO TRANSFORM & PROTECT THE ACCOUNT OPENING JOURNEY

WHITE PAPER





## EXECUTIVE SUMMARY

Customers expect a fully digital account opening process – available online and on mobile. Banks, credit unions, and other financial institutions (FIs) need to offer customer-centric, mobile-first account opening and customer agreement experiences to convert customers and drive growth.

### Remote digital identity verification is a challenge

The account opening process has the potential to impact long-term customer loyalty, profitability, retention, and share of wallet. Despite this, customer identity verification during account opening remains one of the most challenging processes for FIs to digitize. While traditional FIs are making progress, high application abandonment rates, increasing levels of identity fraud, and intensifying competition from challenger banks have all increased the urgency to modernize.

### Technologies and trends to transform account opening and identity verification

Based on extensive interviews and consultations with our customer base and analysts from Gartner and Aite Group, this white paper highlights key technologies, trends, and considerations when digitizing and protecting the account opening experience.

Line of business owners and senior leaders in digital experience, digital transformation, and fraud prevention will benefit from these recommendations on how to transform this strategic area of the business. By supplementing core systems with capabilities such as digital identity verification, agreement automation, e-signature, and machine learning-based risk analytics, FIs can overcome the challenges they have faced in digitizing account opening.

## TABLE OF CONTENTS

## INTRODUCTION

New customers expect to be able to open an account online. As a result, banks and other FIs need to offer digital account opening through online and mobile channels. Despite customer demand for fully digital account opening services, many banks do not offer fully digital account opening experiences – with some aspect of the onboarding process, such as identity verification, requiring the applicant to come into the branch. The prospective customer starts the account opening process online, but is subsequently required to sign paper agreements or present ID documents in-person. These manual steps slow down the account opening process and frustrate applicants, often causing them to abandon the account opening process.

### Poor customer experiences lead to high abandonment rates

The failure to deliver a fully digital account opening process means that banks, credit unions, and other financial institutions (FIs) are losing out to competitors and challenger banks that offer users the ability to open accounts entirely remotely. According Senior Analyst, Tiffani Montez at Aite Group, "application abandonment rates are still between 65% and 95%, depending on the product."[1] If the online customer experience is poor, applicants may turn to financial providers that enable them to complete the account opening process in a single sitting.

Verifying the identity of a remote applicant digitally, while also protecting the account opening process against fraud, has been a challenge for FIs. Advances in digital identity verification methods, such as ID document verification and facial comparison, are changing this.

### Fully digital customer experiences drive growth

The unmet need for fully digital account opening experiences presents tremendous opportunity for growth. In order to provide exceptional user experiences while also protecting the user and FI from fraud, FIs need to prioritize technologies that:

- ✓ Digitize key parts of the account opening process, such as digital identity verification methods and electronic signature
- ✓ Provide a platform for integration with existing and third party solutions
- ✓ Leverage workflow
- ✓ Detect and mitigate fraud in real time

User experience and security are intrinsically linked and the best remote account opening processes will deliver the convenience consumers demand, while offering the security and anti-fraud measures that FIs rely on.

> A good customer experience correlates strongly to customer willingness to make another purchase, and it builds brand loyalty. Every poor online authentication experience increases the risk of customer attrition and lost sales. Creating a consistent, memorable, and enjoyable omnichannel customer experience (CX) must be an obsession for your company. "
>
> **Forrester, The Identity And Access Management Playbook, 2018**

> FIs should replace manual customer authentication processes in the branch, call center, and operations team with facial recognition instead of asking knowledge-based authentication questions.[3]

**Tiffani Montez**
**Retail Banking Senior Analyst**
**Aite Group**

## KEY TRENDS IN DIGITAL IDENTITY VERIFICATION

Digital identity verification is a key step in the remote account opening process as it fulfills Know Your Customer (KYC) requirements that FIs must adhere to when onboarding new customers. KYC is an important step in the fight against fraud. By verifying the identity of an applicant, FIs can run checks to ensure that the applicant is not a criminal or bad actor.

**In a 2018 Aite Group survey of account opening processes at large financial institutions, 63% of respondents indicated that they were likely to implement mobile data capture and identity document verification for checking, savings, and credit card accounts within 1-2 years.[2]**

The financial services industry invests massive amounts of money every year to attract and acquire new customers. Unfortunately, much of this is wasted once the applicant hits a barrier during the account opening process. This friction point is often the upfront identity verification step, where the FI needs to carry out KYC checks to ensure the applicant is who they say they are and that they are not attempting to commit fraud.

Today, identity verification approaches in the financial services industry fall into two camps:

1. **Manual, in-person verification:** Online and mobile applicants are forced to come into a branch to verify their identity and sign documents. This introduces a high level of friction and keeps applicants from completing the process in a single sitting.
2. **Unreliable, high-friction online verification methods:** A commonly used digital identity verification method in the UK and North America is knowledge-based authentication (KBA). KBA involves the applicant answering a series of questions that are verified using queries to credit bureaus and third-party databases. Unfortunately, KBA is viewed as a high-friction process requiring applicants to remember and answer personal questions based on public data. Further, KBA has become less reliable due to large-scale data breaches that have occurred in recent years.

Manual, in-person verification and high-friction methods are unacceptable for consumers who demand a simple, convenient, and friction-free digital account opening experience.

Current identity verification methods are:

| HIGH FRICTION | TOO LONG | NOT SECURE |
|---|---|---|
| 65-95% of users abandon the account opening process due to high-friction steps such as the requirement to go into a branch or answer KBA questions.[4] | In-person identity checks deny the applicant the ability to complete the account opening process in a single sitting.<br>When the account opening process is extended due to mandatory in-person ID verification, abandonment rates increase. | Based on "something you know", KBA has always been high friction, but historically was known to deter fraud.<br>Multiple, large-scale data breaches have now rendered standalone KBA models less effective. |

## TREND 1: USERS ARE WILLING TO PERFORM ACTIONS THAT ESTABLISH TRUST

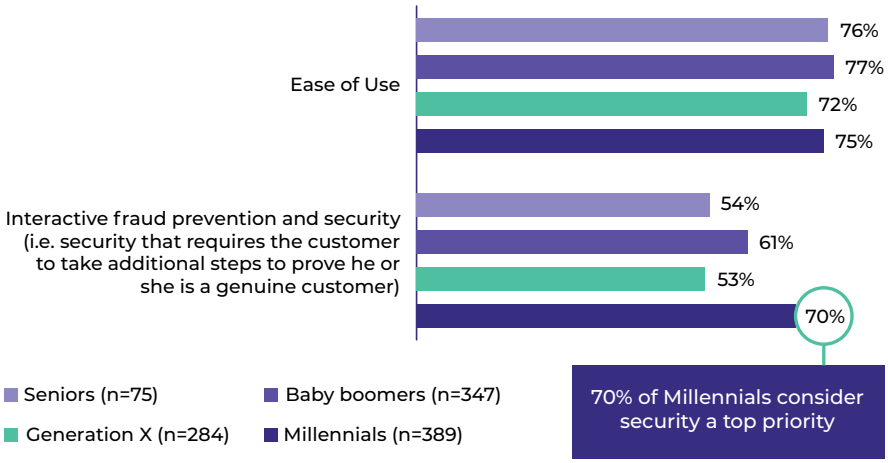
Ease of use is very important to users when opening an account remotely, but so is security. Applicants want to be sure that their data is secure and that their account cannot be breached. Applicants are therefore willing to accept some security steps during the account opening process. These trust-moments build a stronger relationship between the user and the bank.

In a consumer survey by Aite group, researchers found that 70% of millennials considered security a top priority when transacting with financial institutions online.[5]

This would suggest there is a clear difference between 'good' friction (friction that protects the user and establishes trust) and 'bad' friction (friction that frustrates and disrupts ease of use). Today's consumers, especially future generations, are more aware of the need for trust-establishing actions that protect their account and help to prevent fraud.

The point at which friction is introduced into the customer journey is also often as important as how it is introduced. Gartner refers to this process of establishing trust as 'progressive intimacy'. At the beginning of a relationship between a customer and an FI, the FI has not yet earned the customer's trust. Once trust is established, however, the user will accept more friction to keep their account secure.

Consumers' Priorities for Online Banking Capabilities




Source: Aite Group

## TREND 2: MULTI-LAYERED DIGITAL IDENTITY VERIFICATION ACHIEVES OPTIMAL CUSTOMER EXPERIENCE & PROTECTS AGAINST FRAUD

Digital account opening presents a two-fold challenge: FIs must achieve their risk and compliance objectives, while ensuring a seamless customer experience.

Multi-layered digital identity verification through a single platform allows FIs to access a wide range of third-party identity and verification services. This way, FIs can select the best verification types for their use case and channel, to improve customer experience and minimize risk.

A platform-based approach results in higher pass rates and enables failover in the event of a verification failure or provider unavailability. This in turn eliminates the need for manual intervention and reduces customer abandonment. All of which enables FIs to provide an optimal customer experience and safeguard against application fraud – second only to account takeover fraud as the biggest fraud challenge for financial institutions.[6]

Benefits of a multi-layered digital identity approach:

1. **Scalable:** Ability to select the best verification types to optimize adoption rates and access new check types as they come to market.
2. **Flexible:** Ability to access multiple verification providers through a single platform.
3. **Auditable & Enforceable:** Ability to capture a complete audit trail of the identity verification process.
4. **Configurable:** FIs can select multiple verification types and build a workflow of verification types based on a rule-set or identity workflow (e.g. risk or geography).

Multi-layered approach enables FIs to gain a 360° view of the applicant

> Automated identity document capture and verification is relatively new in the market and is gaining traction in many economic sectors. [..] Overall, 90% of FIs indicate plans to implement within the next two years.[7]
>
> **Aite Group**

## BEST-IN-CLASS DIGITAL IDENTITY VERIFICATION METHODS

### ID DOCUMENT VERIFICATION

Document verification is a digital identity verification method used to check whether an applicant's ID document (e.g. passport, ID card, driver's license, etc.) is legitimate.

Using the in-built camera on a mobile or hand-held device, the technology captures an image of the applicant's ID document. Artificial intelligence and advanced authenticity algorithms are then used to analyze the image to produce an authenticity score to determine whether the ID document is fraudulent or genuine.

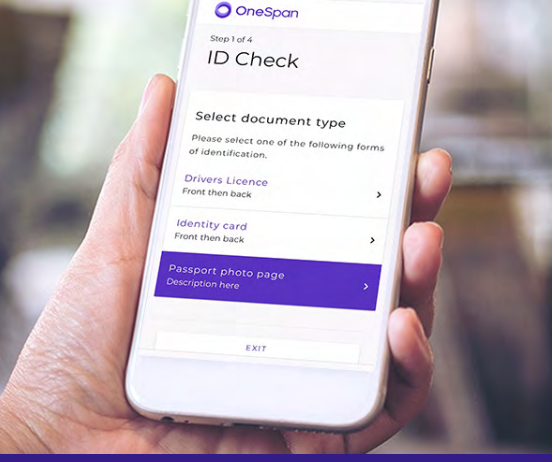
Advanced authenticators include:

1. **Visible Security Features:** Embedded security features such as watermarks or holograms can be detected and their positioning and appearance analyzed.
2. **Font Usage and Consistency:** Fonts are analyzed and compared to standard fonts for a particular document template. The spacing, shape, and consistency of letters is used to analyze authenticity.
3. **Rounded Corner Detection:** Rounded corners can be checked to ensure they are aligned with templates.

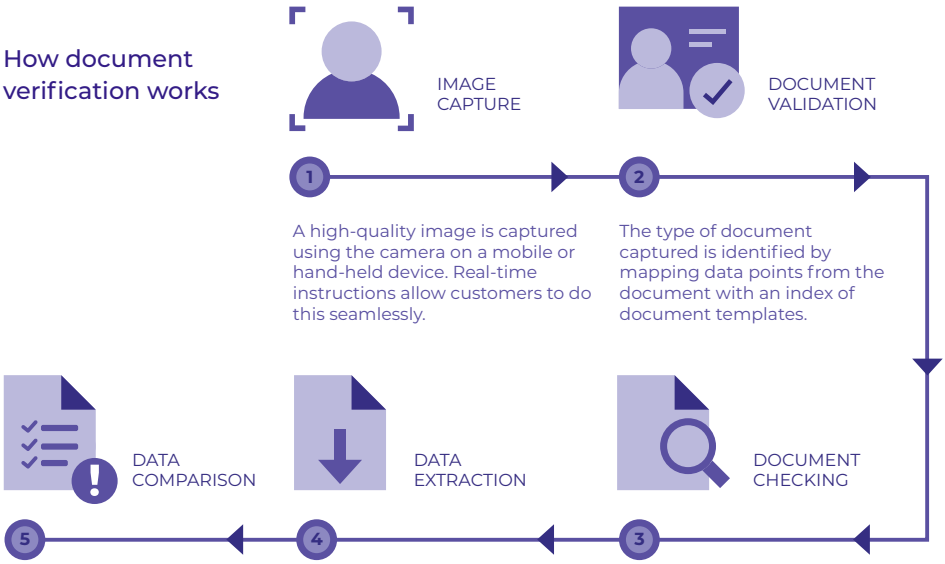
Once the authenticity check is complete, ID document verification technology extracts data such as name and date of birth from the authenticated ID document. This data reduces the need for manual data entry and can be compared with previously captured data (such as data provided during an application process) to prove that the owner of the ID document is the person applying for the account.

ID document verification enables a customer's ID documents to be authenticated digitally and in real-time, whether the user is in-branch or remote. For the consumer, the experience is quick and simple. For FIs, automated ID document verification speeds up account opening, removes a manual step, eliminates the need to train staff to manually verify ID documents, and ensures that identity verification processes are consistent and compliant – all while protecting against fraud.

> Capturing the data from an identity document enables an FI to use that data to prefill another document, such as a credit card or DDA application. This is much more customer-friendly than having to type all this data via a small mobile keyboard, and it also eliminates many keying errors that normally lead to additional back-office work, thus improving operational efficiency. [...] Know Your Customer requirements can be met through this process as well, improving compliance." [8]
>
> **Aite Group**

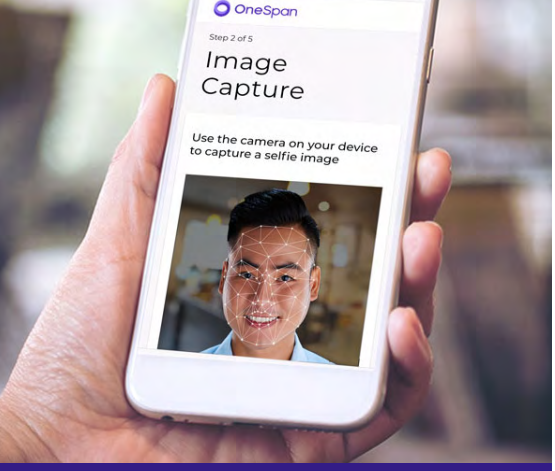



## How document verification works




Benefits of ID document verification:

- ✓ Assists in meeting anti-money laundering (AML) and KYC requirements
- ✓ Uses facial comparison features to establish that the person presenting the ID matches the individual on the ID document
- ✓ A fully digital process delivers an excellent user experience; mobile image capture is usable and accessible for everyone
- ✓ Data extraction straight from the document removes manual data entry
- ✓ Documents can be verified in seconds (from <5 minutes to <10 seconds , depending on the provider)




## FACIAL COMPARISON

The ability to prove that a user is genuine and physically present during remote account opening is a critical component in the fight against application fraud. In 2017, there were 16.7 million victims of identity theft in the US alone – a record high.[9] With such high levels of identity theft, it is essential that FIs verify that a user is genuine during the account opening process.

Due to data breaches and SMS security vulnerabilities, traditional methods of identity verification such as KBA and two-factor SMS authentication can no longer be relied on to verify users during remote account opening. This is driving FIs to turn to ID document verification and facial comparison to verify prospective customers securely.

Here's how facial comparison is used to prove that an applicant is present during the transaction:

1. **Document Verification:** Document verification is used to verify the authenticity of an applicant's passport, ID card, or driver's license.
2. **Selfie:** Once the authenticity of that ID document is confirmed, the applicant is asked to take a selfie using their handheld device.
3. **Biometric Comparison:** Facial comparison technology compares the selfie image with the image from the verified ID document to prove that the verified person is present during the account opening process.

Facial comparison technologies use advanced algorithms to extract biometric data from a person's features, distilling an image into a standardized dataset. For example, the position and size of a person's eyes relative to each other can be used as a data point extracted from an image. Comparing two datasets can determine whether two images are from the same individual.

If one image is from a pre-verified source (e.g. a passport or ID card verified using document verification) and the second image is a real-time image taken from the applicant at the time of their application, facial comparison can be used to prove their presence.

### Facial Comparison Technology Considerations

**Liveness detection:** Before a captured image or selfie is used for facial recognition, liveness detection can be applied to the image to prove genuine human presence and that a static image of the person has not been fraudulently used. Liveness detection helps to prove that an image has not been fraudulently created using methods such as high-resolution print-outs or pre-recorded videos.

**Verified source image:** A verified source image of the customer must be available to compare against. To solve this, use facial comparison in conjunction with a document verification feature that can extract a source image from a valid identity document.

> Digital fulfillment presents the opportunity to implement e-signatures for loans, which eliminates the need to sign in a branch or with a notary, and provides user-friendly methods for funding a checking account that do not rely on a consumer going into a branch to make their first deposit.
>
> **Aite Group**
> **Transforming the Digital Account-Opening and Onboarding Experience**

## THE ROLE OF ELECTRONIC SIGNATURES

Once a new applicant's identity has been verified and KYC requirements met, the next hurdle in keeping the account opening process digital is obtaining the customer's signature. Depending on the account type and applicable laws and regulations, a signature may be required to agree to the terms of the account, agree to receive documents electronically, or acknowledge receipt of digital disclosures.

For financial institutions and other organizations implementing electronic signatures and records, questions often arise regarding the legal requirements and implications of e-signing. Today, more than 90 countries have enacted laws enabling electronic signatures and records.

In Europe there are three forms of electronic signature: Basic, Advanced, and Qualified E-Signature. While the first two do not require third-party identity validation in the form of a digital certificate, the latter requires that a Certification Authority (CA) provide a personal digital certificate to the signer and in certain countries it is mandatory to use the local CA. Therefore, to support compliance with legal and regulatory requirements in any jurisdiction, it is important that a solution provide the flexibility to implement any of these forms of e-signature as part of an online or mobile process.

Implementing e-signatures as a 'click-to-sign' ensures the easiest user experience for remote use cases. According to a 2018 Celent report comparing top banks' mobile account opening experiences, "within the context of mobile, checking a box to accept the terms and provide a signature was all that was required."[10]

Electronic signing can take place on any device (e.g., through a mobile app, or a web or mobile browser) and can be fully integrated for an automated hand-off between back-end systems. Digital data captured throughout the account opening process can flow into core systems and be used to automatically trigger downstream processes.

Financial institutions report that paperless account opening workflows dramatically improve the first experience with the customer by removing any need to wait while documents are printed or errors corrected. And if done remotely, there is the added benefit of enabling customers to choose when and where they transact with the bank.

To evolve an FI's omni-channel strategy, electronic signatures can be used by FIs across multiple channels. For the customer, imagine having the ability to start the account opening process online, pause it, save your progress, and resume in another channel – such as mobile – without having to rekey any information already entered. For the financial institution, maintaining a consistent omni-channel process helps avoid the delays, costs, and errors that happen when using paper and manual processes.

BMO Bank of Montreal implemented e-signatures to simplify and streamline the remote onboarding and account opening process. Today, new applicants and existing customers can open a new account on their phone in less than eight minutes.[11]

BMO Bank of Montreal

## THE COST OF FRAUD

- 13 billion data breaches since 2013 [18]
- 2.41% of FI revenue lost to fraud [19]
- US$5.1 billion of identity fraud losses in 2018 [20]
- US$599 million projected US FI spend to combat application fraud by 2020 [21]

## SECURITY & COMPLIANCE CONSIDERATIONS

Cyberattacks on banks and FIs are growing in volume, complexity, and speed. According to Forbes, cyberattacks target financial services 300 times more often than other industries.[12] Attackers target FIs to access sensitive customer data that can then be used to commit fraudulent activities.

In addition to causing victims anxiety, fraud costs FIs and their insurance companies significant amounts of money. LexisNexis estimates that in 2018, the cost of fraud for mid to large financial service companies operating internationally was 2.41% of revenue.[13]

Given the scale and impact of fraud, it is vital that FIs can detect fraud during the account opening process. As fraudsters use increasingly sophisticated methods, a rules-based fraud prevention system alone can no longer keep up. To stay ahead, FIs need an identity verification and risk-based fraud solution that leverages AI through supervised and unsupervised machine learning. Machine learning allows organizations to analyze data with context across devices, applications, and transactions, and requires very little manual input.

Machine learning algorithms analyze transaction data and only flag suspicious transactions with higher risk scores. By detecting complex patterns that are difficult for humans and older rules-based methods to identify, this risk-based analytics approach is more effective in detecting new and emerging fraud.

### Common attacks during and after the account opening process

| During Account Opening | After Account Opening |
|---|---|
| **APPLICATION FRAUD**<br>Fraudsters use customer data stolen through data breaches, account takeover, social engineering, phishing or multiple other methods, to fraudulently open a new account.<br><br>In 2018, data breaches exposed 447 million records globally across banking, business, education, government, and healthcare.[15] Data breaches that expose personally identifiable information (PII) make identity theft and application fraud easier to perpetrate.<br><br>In addition to application fraud, the use of manipulated, synthetic, or manufactured identities is also on the rise. Fraudsters nurture synthetic identities so that they have credit bureau files and mobile numbers before using them to commit fraud. [16] | **ACCOUNT TAKEOVER (ATO)**<br>According to Javelin Research, 16.7 million US consumers had their identity stolen in 2017, an increase of over 1 million from the previous year. Much of this was driven by ATO attacks, with losses from identity theft reaching $5.1 billion.[17]<br><br>Common attacks that lead to ATO include:<br>• **Phishing Attacks:** Fraudsters send emails or SMS messages engineered to encourage the user to click a link redirecting to a fake banking portal or to open an attachment that will install a piece of credential-harvesting malware.<br>• **Mobile Banking Trojans & Overlay Attacks:** Fraudsters leverage vulnerabilities in operating systems to install malicious Trojan software on the victim's device. This overlays fake screens on legitimate mobile banking apps to collect banking credentials.<br>• **Malware:** Fraudsters harvest data through key-logging or man-in-the-middle malware which intercepts data via the victim's browser. |

## USING DIGITAL IDENTITY VERIFICATION TO COMBAT APPLICATION FRAUD

Financial institutions have traditionally depended on credit bureaus for identity verification. One challenge with this approach is the static nature of personal information. If the PII has been stolen or compromised, fraudsters will be able to use it to open a new account.

When an applicant is attempting to open a new account, FIs can no longer depend on verifying a user's identity based on static data from credit bureaus. By combining risk analytics with multi-layered digital identity verification methods, FIs should look to verify a potential customer using a context-aware approach.

A context-aware approach enables real-time security decisions based on the total risk associated with a new customer to better manage their risk of fraud – especially for remote transactions. With a context-aware identity verification solution, FIs can dramatically reduce fraud and drive top-line growth, while providing the best user experience possible for new digital account openings.

## SECURING A CUSTOMER'S ACCOUNT ONCE THE CUSTOMER HAS BEEN ONBOARDED

After a customer has been onboarded and the account opened, FIs need to ensure that access to the customer's account is secure. Each time a customer attempts to access the account, FIs need to authenticate the identity of the user to ensure that the access attempt is genuine and not initiated by attackers trying to access the account. In an Aite Group survey, 27% of consumers reported accessing their online or mobile banking accounts daily, with a further 47% accessing their account at least once a week.[14] With such high frequency of use, FIs must continuously authenticate users.

Existing customers can be authenticated through a variety of digital authentication methods such as one-time passcodes, multi-factor authentication, SMS authentication, and biometric authentication.

Adaptive authentication technology can also be used to further improve the user experience, while providing the optimal level of security for each transaction. Intelligent Adaptive Authentication uses machine learning to analyze the risk of a transaction based on data such as the user's behavior, location, device integrity, and recent transactions. Scoring these data elements allows the technology to apply a risk score to each transaction and adapt the security and required authentication accordingly throughout the customer's digital journey. This ensures the best possible customer experience, while safeguarding transactions and sensitive customer data.

## DIGITAL AUDIT TRAILS

To prove that a compliant account opening process was followed, financial institutions should capture a full audit trail of exactly what the applicant saw and did during an account opening process – including the identity verification and signing steps.

Digital audit trails prove that the FI carried out all necessary KYC checks and that the applicant intented to be bound by the terms of the agreement. Audit trails provide a complete record of the account opening process and can protect FIs against legal or compliance disputes.

## HOW ONESPAN CAN HELP

At OneSpan, our mission is to transform and protect the digital customer journey – from an applicant's first interaction to securing their accounts throughout the entire customer lifecycle. Our solutions have been designed to help FIs deliver a differentiated customer experience, while safeguarding customers' financial transactions and helping protect against fraud. To learn more, visit OneSpan.com or contact us to discuss your unique requirements.


1 Aite Group, AI: Transforming the Digital Account-Opening and Onboarding Experience, 2018

2, 3, 4 Ibid

5 Aite Group, Digital Banking Customer Engagement: Adoption, Usage, and Satisfaction Impact Report, 2017

6, 7, 8, 18, 21 Aite Group, Application Fraud: Fighting an Uphill Battle, December 2018

9 Javelin Strategy & Research, Identity Fraud Study, 2018

10 Celent Research, The US Open: Looking at Mobile Account Opening at US Banks

11 Celent Research, BMO Digital Transformation in Personal Banking, 2017: http://bit.ly/2oUTDyW

12 Forbes, https://bit.ly/2INLaLI

13, 19 Lexis Nexis, 2018 True Cost of Fraud Study for the Financial Services Sector

14 Aite Group, AI: Transforming the Digital Account-Opening and Onboarding Experience, 2018

15 Identity Theft Resource Center, End-of-Year Data Breach Report, 2018

16 Aite Group, Synthetic Identity Fraud: The Elephant in the Room, 2018

17, 20 Javelin Strategy & Research, Identity Fraud Study, 2018

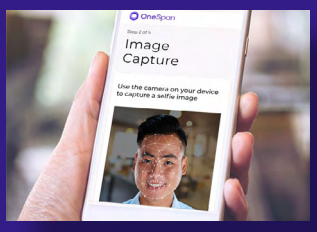

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.




Last Update March 2019.


**FIND OUT MORE ABOUT DIGITAL ACCOUNT OPENING**




**CONTACT US**


**info@OneSpan.com**
**OneSpan.com**