OneSpan

UAE's Central Bank boosts consumer protection against rising fraud

WHITE PAPER JULY 2025

Introduction

On 23 May 2025 the Central Bank of the United Arab Emirates (CBUAE) issued a new regulatory notice, referred to as "Notice No. CBUAE/FCMCP/2025/3057". Through this notice, CBUAE aims to address the significant increase in fraud impacting customers of financial institutions across the UAE.

In this article we share the key highlights from the CBUAE's directive related to strong authentication of users and transactions, as well as fraud detection and prevention.

Strengthening user and transaction authentication mechanisms

First of all, CBUAE aims to strengthen the authentication mechanisms used to perform financial transactions via digital banking accounts and electronic wallets. To combat weak authentication methods, the notice prohibits financial institutions from using SMS OTP, email OTP, or static credentials (e.g., passwords) as the sole authentication method for financial transactions or account provisioning. As such, CBUAE follows in the footsteps of the Monetary Authority of Singapore (MAS) and the Reserve Bank of India (RBI), which took similar initiatives to ban SMS OTP.

When accessing mobile banking applications for the first time or from a new device, financial institutions must utilize strong identity verification technology like Emirates Face Recognition. For recurring logins to mobile banking apps from trusted devices, static PINs or device-native biometrics may be used. For access to web-based banking applications, the consumer must approve a confirmation from a separate secure channel, such as the mobile banking app or a soft token.

Furthermore, financial institutions must implement step-up authentication in the mobile banking or web banking application for sensitive actions, such as modification of transaction limits, initiation of payments, and modification of personal data (e.g. address details).

Finally, for 3-D Secure e-commerce transactions, SMS OTP, email OTP, and static credentials are disallowed even when used as a second authentication factor. Instead, financial institutions must adopt stronger authentication methods such as in-app verification, soft tokens, tap to authenticate, or biometrics. Financial institutions are held liable and consumers are entitled to a full refund for reported fraud on 3-D Secure transactions authenticated with SMS OTP, and this as of the date of issuance of the notice.

Bolstering fraud detection and prevention

CBUAE also introduces a significant number of requirements to enhance the fraud detection and prevention capabilities of financial institutions in the context of digital banking.

First of all, financial institutions must present the payee's name, account number, bank details, and account type to the consumer before confirming domestic (and whenever possible, international) fund transfers. In addition, financial institutions must implement a "Confirmation of Payee" mechanism for instant payments, allowing a consumer to check whether the bank account number and name of the beneficiary correspond to each other. Similar mechanisms are also required in various other countries and regions, such as the UK, EU, and Australia.

New device

When accessing mobile banking applications for the first time or from a new device, financial institutions must utilize strong identity verification technology like Emirates Face Recognition.

Trusted device

For recurring logins to mobile banking apps from trusted devices, static PINs or device-native biometrics may be used.

Web-based app

For access to web-based banking applications, the consumer must approve a confirmation from a separate secure channel, such as the mobile banking app or a soft token.

In addition, financial institutions must equip their mobile banking apps with controls to detect screen sharing (e.g., by remote access tools), malware, and active phone calls from the mobile device, and suspend mobile banking sessions upon detection. For web banking, financial institutions must ensure that no screen sharing application is active during the session. The usage of VPN from the user's laptop or desktop PC should be taken into account as a risk evaluation criterion.

The CBUAE is also pushing for more sophisticated fraud detection. Financial institutions must implement systems capable of real-time transaction analysis (24/7, 365 days a year) to identify unusual consumer activity and stop suspicious transactions immediately. These systems should incorporate risk scoring mechanisms and analyze consumer account activity for suspicious behaviours like sudden large withdrawals or activity from unusual locations. Financial institutions are also encouraged to use advanced fraud detection methodologies like behavioural analysis and biometrics.

Finally, customer notifications for completed transactions and modifications to personal data, limits, security parameters, and new cards are now required. Financial institutions are also encouraged to avoid clickable links in emails or SMS messages, suggesting push notifications as an alternative.

Empowering consumers

Under the CBUAE's notice, consumers will have easier ways to report suspicious activities. Financial institutions must provide self-service options through mobile applications or online portals for consumers to report fraud and manage their accounts securely. Manual and time-consuming methods like filling out forms via email or visiting a branch for complaints can be avoided in this way.

Financial institutions are also required to provide tools for consumers to control their accounts and enhance protection, including options to modify transfer and payment limits, block or enable accounts, cards, and channels, and use geofencing. Consumers must also be able to view and manage their recurring payment subscriptions.

Financial institutions must equip their mobile banking apps with controls to detect screen sharing, malware, and active phone calls.

Compliance and enforcement

Financial institutions are required to comply with these new requirements by 31 March 2026, with the exception of prompt refunds for fraud cases on 3-D Secure transactions authenticated with SMS OTP, which are effective immediately. Failure to comply may result in higher risk ratings for financial institutions in CBUAE's assessment tools and the CBUAE may take supervisory action.

Conclusion

This comprehensive notice from the CBUAE is a significant step towards creating a more secure financial environment for consumers in the UAE, putting greater responsibility on financial institutions to implement strong user authentication and robust fraud prevention and detection in the fight against fraud.

Financial institutions in the UAE can benefit from OneSpan's strong authentication and threat protection solutions to curb fraud and comply with the CBUAE's new requirements.

About the author

Frederik Mennes is Director of Product Management & Business Strategy at OneSpan. In this role, he is responsible for defining and implementing OneSpan's business strategy for specific industry verticals, and to determine how OneSpan responds to security and regulatory market trends. Previously, Frederik led OneSpan's Security Competence Center, where he was responsible for the security aspects of OneSpan's products and infrastructure. He has an in-depth knowledge of authentication, identity management, and security technology in general.

For more information or to discuss regulatory developments and compliance in more detail for your business, contact the author at frederik.mennes@onespan.com.

About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world's 100 largest banks—to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Learn more at
OneSpan.com/security

Contact us at
OneSpan.com/contact-us