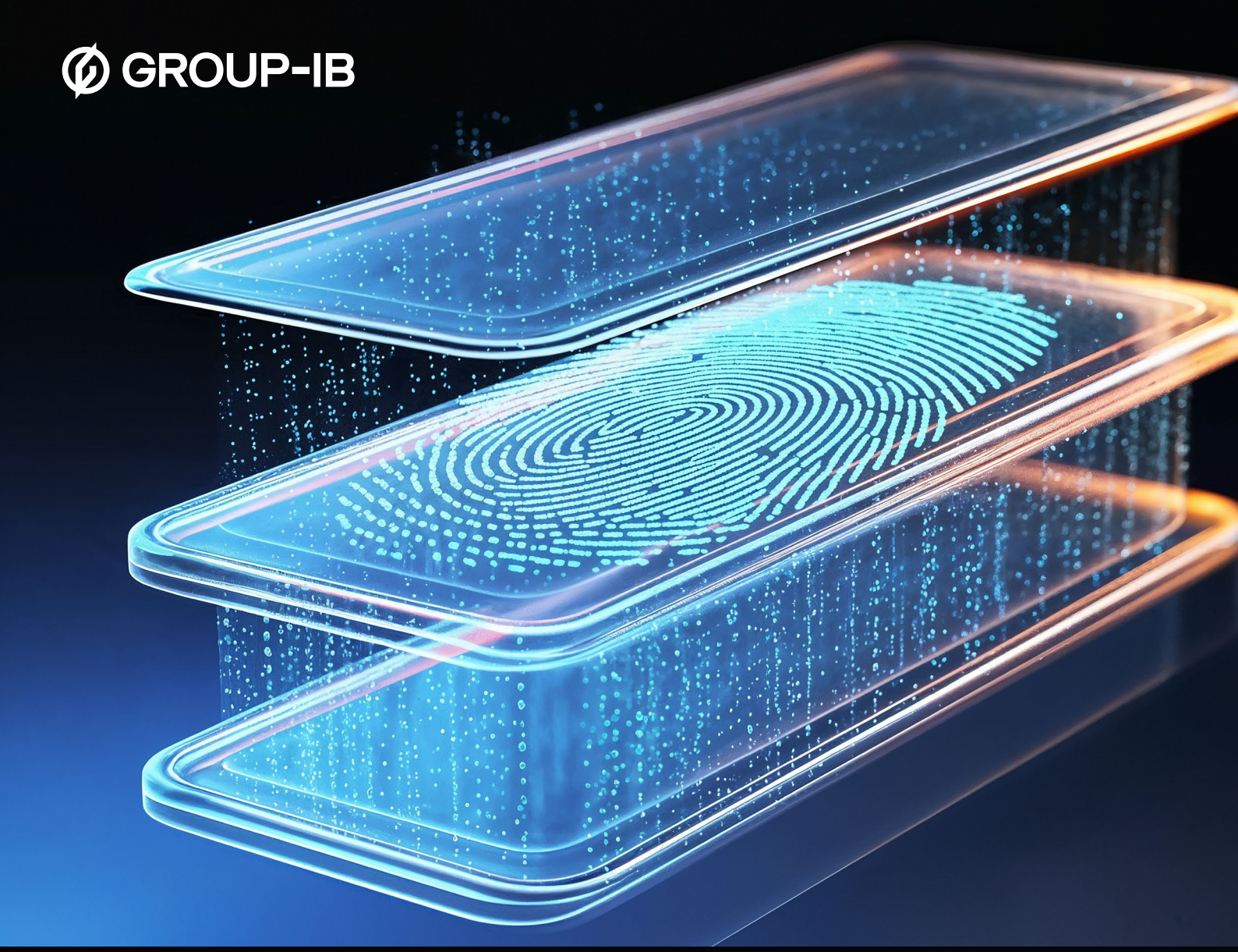
GROUP-IB



End of OTP: UAE banks' fast-track guide to CBUAE Consumer Protection Regulation

OTP-based transaction authentication is being phased out in the UAE, giving the region an opportunity to move towards upgraded fraud resilience. While the regulatory shift is already in motion, here's what the UAE banks must do to meet the March 2026 deadline.

Table of contents

01 Executive Summary

At the start of 2025, the Central Bank of the UAE (CBUAE) updated its Consumer Protection Regulation, a comprehensive framework designed to strengthen digital banking security and reduce fraud.

The updated regulation sets out a clear expectation: by March 2026, Licensed Financial Institutions (LFIs) must eliminate weak authentication methods and adopt modern, customer-centric approaches to strengthen the protection of digital transactions.

The transition is far more than a technical upgrade. It represents a paradigm shift in how banks approach authentication, fraud monitoring, and customer empowerment. **Failure to comply may expose institutions to supervisory actions, higher regulatory risk ratings, and reputational damage.**

This guide explores CBUAE's updated regulatory context, including new rules for the adoption of modern authentication methods, such as biometrics and cryptographic tokens, along with continuous, real-time fraud monitoring, prevention, and enhanced customer controls. It also addresses the challenges faced by Licensed Financial Institutions (LFIs) in adopting these new regulations, as well as other relevant topics.

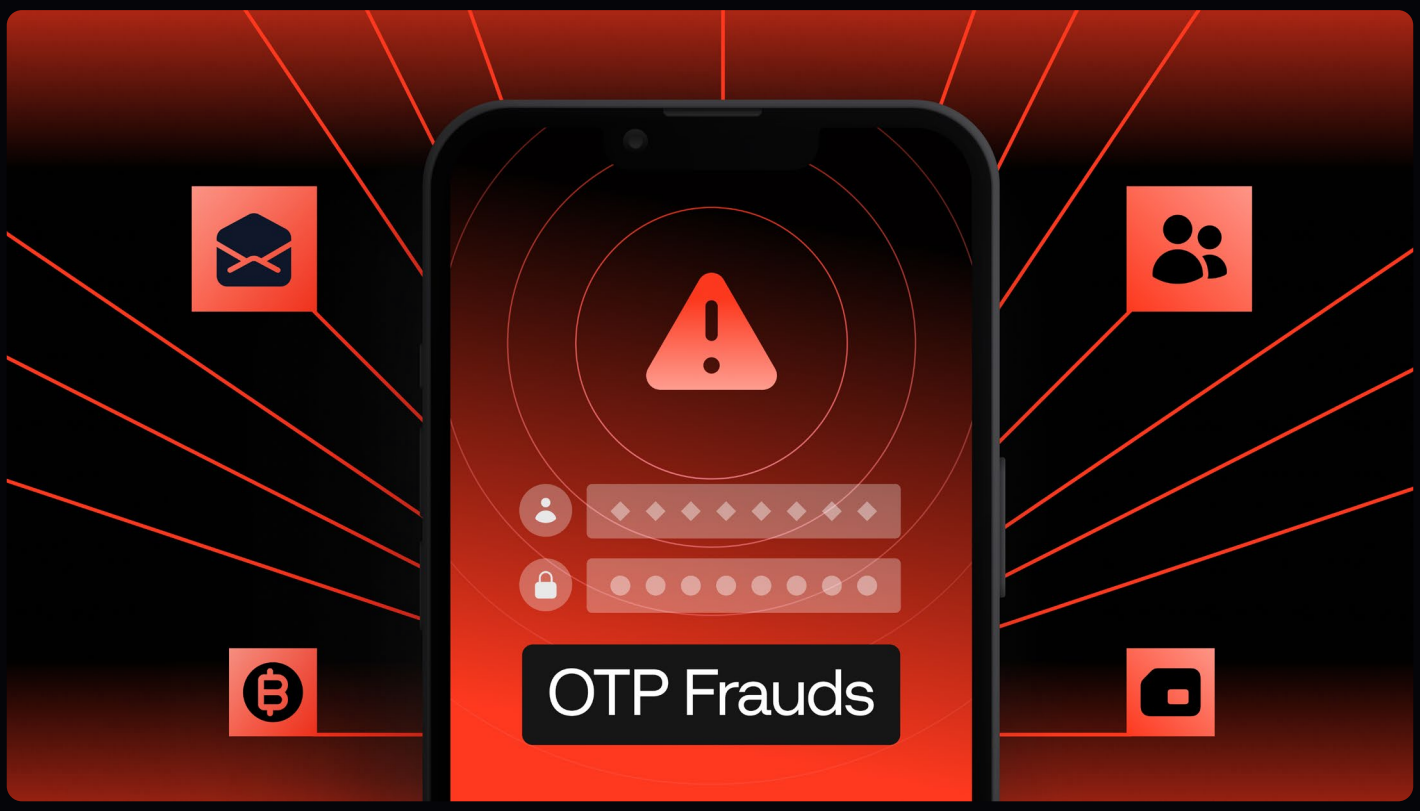
The guide also presents a detailed, four-stage roadmap for LFIs to transition from outdated authentication and security protocols and legacy architecture to risk-based, biometric verification systems and unified, intelligence-driven fraud protection, recommending advanced, integrated solutions like Group-IB Fraud Protection and BioConfirm to achieve both compliance and long-term resilience.

02 Introduction

Banks handle thousands of transactions daily, and behind every transaction is a critical responsibility: ensuring safety, legitimacy, and secure exchange. SMS- and email-based OTP verification has long been a standard method for transaction authentication, providing a familiar and convenient experience without obstructing the customer journey. **However, the growing risk of fraud associated with these conventional but convenient methods has forced authorities worldwide to rethink how they secure banking transactions.**

While widely adopted and consumer-friendly, SMS and email passcodes are frequently compromised through phishing, SIM-swap attacks, and malware, allowing fraudsters to hijack sessions, authorize APP transactions, take over accounts, and route stolen funds through mule networks that support investment and impersonation schemes.

Recognizing these weaknesses, the CBUAE has drawn a firm line under legacy authentication methods.



Digital fraud shows escalating numbers in the UAE

42%

of the UAE organisations reported an increase in fraud year-on-year
PwC

56%

of the UAE residents report facing at least one financial fraud attempt per month
Gulf News

1.6B+ AED

is the estimated financial loss due to fraud incurred by UAE banks in recent years
Gulf News

$160,000+

is the reported loss from extreme SIM-swap cases in the Middle East
Group-IB

What does the Consumer Protection Regulation say?

The Consumer Protection Regulation prohibits weak stand-alone methods such as SMS OTPs and instead requires institutions to adopt strong, risk-based, or multi-factor approaches such as biometrics, in-app verification, or secure tokens. Why? Because OTP alone does not authenticate:

- The device
- The identity
- The user's intent

The regulation also obligates Licensed Financial Institutions (LFIs) to introduce measures that give customers more transparency and control over their transactions, implement continuous real-time fraud monitoring, and conduct regular assessments of emerging typologies.

Sensitive activities like changing limits or adding new payment instruments now require additional layers of security. The consequences of failing to comply are significant. Institutions that fall short of the March 2026 deadline risk:

- Being flagged with higher risk ratings in the CBUAE's supervisory dashboards
- In more severe cases, direct intervention or referral to the Enforcement Department

Compliance is therefore not optional; it is a defining requirement for maintaining both regulatory approval and customer trust in the years ahead.

03

UAE banking authentication: Learning from regional success and building for the future

Digital payments in the UAE continue to grow, with real-time payment transactions value expected to reach $132 billion (Dh 484.4 billion) in 2028.

One thing is for certain — digital payments aren't slowing down anytime soon, but security systems are. As banks work to operationalize these new rules, the current authentication systems in the UAE reveal transformation challenges that require strategic, integrated solutions.

There are systemic gaps in pre-regulation protocols. Changing authentication will not be an overnight overhaul, especially for banks that lack real-time intelligence to detect and stop sophisticated fraud.

Current authentication and session integrity weaknesses include:

- Lack of device-binding standards
- Absence of biometric, tokenized verification for high-risk transactions
- Lack of RAT/screen-sharing detection
- Weak controls around 3DS (liability shifts)
- No real-time behavioral analytics

These are exactly the gaps CBUAE cited in discussions with banks.

To effectively shut down regulation challenges and financial fraud, banks and users need real-time, reliable risk-based (evaluation of fraud signals and device) biometric authentication as an essential line of defense. **For Licensed Financial Institutions, the path to modern authentication involves navigating both technical integration requirements and broader operational transformation.**

The most immediate challenge lies in technology integration: ensuring that new authentication mechanisms, risk engines, and monitoring tools can operate seamlessly with existing infrastructure.

Authentication flows in banking architecture pass through multiple layers (OTP, mobile banking, 3DS, fraud monitoring, core access, device management systems). This means new authentication controls must be integrated end-to-end across channels, risk engines, and backend systems to function correctly and consistently.

Many Licensed Financial Institutions (LFIs) still operate on legacy architecture that cannot easily integrate modern authentication tools. These systems face significant constraints: data lacks standardization, no real-time connectivity across transactions, customer profiles, and channels, and immediate fraud response capabilities are absent. Compounding

this challenge, authentication solutions from different vendors often lack native compatibility with each other or with existing banking infrastructure. This means adoption cannot simply be 'plug-and-play.' Introducing device- binding, tokenized, and behavior-driven authentication will require comprehensive re-engineering of digital channels, backend APIs, and mobile applications.

Beyond technology, the regulation imposes new operational obligations: continuous fraud monitoring, enhanced reporting, and customer-facing controls that give individuals direct authority over their security settings. These requirements place additional demands on systems infrastructure, governance frameworks, and fraud prevention and cyber intelligence teams - resources that remain limited.

Customer expectations are shifting rapidly: consumers demand both security and convenience, and they are quick to abandon services that feel interrupted or cumbersome. This makes the balancing act between compliance and user experience especially delicate.

Learnings from Saudi Arabia's authentication evolution

A regional study

The Saudi Central Bank (SAMA) officially released the Counter Fraud Framework (CFF) in 2022, which forced banks to modernize their controls within tight deadlines.

The objective was to implement standardized fraud-prevention controls across Saudi banks, including real-time fraud detection and monitoring; revised authentication journeys, improved governance, fraud reporting, and management processes.

Like many financial institutions in the UAE today, banks in Saudi Arabia faced similar challenges, including legacy architectures, limited expertise, and the need to meet strict compliance requirements without compromising customer experience.

How did the transformation succeed?

Banks that used the CFF as an opportunity to strengthen defenses did so by integrating customer journey–oriented fraud controls.

How did they approach the transformation?

- Adopting integrated solutions that fused fraud prevention with broader cyber intelligence
- Enforcing real-time behavioural and device monitoring
- Revising their digital channel operations under CFF deadlines

UAE banks are now facing a similar inflection point, but with less time to replicate that transformation.

04

Four stages to meet the March 2026 deadline + long-term security

STAGE 1

Immediate Actions (1 Quarter, 2026)

Objective	Priority Actions	Key Takeaway
Establish strong authentication and secure high-risk journeys before the March 2026 deadline	• Freeze the expansion of SMS and email OTP across all channels. • Identify and secure all high-risk transaction journeys. • Replace OTP with in-app biometric or cryptographic authentication for sensitive actions. • Enforce device binding for payments, enrolment, and account changes. • Activate real-time session monitoring (malware, overlays, remote access, emulators). • Apply dynamic, risk-based step-up authentication for suspected APP scams, social-engineering attempts, and account takeover (ATO) scenarios. • Ensure secure in-app authentication for 3DS and card-not-present transactions. • Validate controls, evidence, and dashboards for compliance readiness. • Continuously monitor customer experience and tune authentication friction based on real-time risk signals. • Plan post-compliance API re-engineering for core authentication journeys.	Banks must have full visibility into their existing authentication security and what must be replaced first.

STAGE 2

Ensure Continuous Resilience (Post-Compliance)

Objective	Priority Actions	Key Takeaway
Maintain an evolving, intelligence-driven fraud defense	• Re-engineer APIs for modern authentication flows (including 3DS, instant payments, and device enrolment) to streamline long-term operations and scalability. • Progressively enrich the risk engine with cyber-fraud fused intelligence to improve correlation, accuracy, and automation. • Continuously update behavioural, device, and anomaly detection models. • Maintain global and regional fraud intelligence feeds. Conduct quarterly typology assessments. • Automate fraud response workflows. • Strengthen Customer Experience (CX) with seamless, low friction authentication.	Compliance is just the starting point; the regulations will continue to evolve. Banks must be ready with future-proof, intelligence-driven platforms and proven regional experience to stay ahead of regulatory requirements and fraud risks.

With Group-IB, organizations can make this shift effectively and confidently through our comprehensive security assessment to establish gaps and control modifications, enabling unified cyber-fraud monitoring and intelligence sharing into a single ecosystem. The converged, real-time intelligence on suspicious transactions, mule networks, coordinated scam campaigns, and emerging TTPs can help Licensed Financial Institutions (LFIs) identify, correlate, and block emerging fraud schemes before they escalate.

For organizations looking to modernize and strengthen fraud posture and authentication, Group-IB's BioConfirm addresses the need with its modern fraud prevention, device-binding, biometric verification that ensures only the right user consents to the transaction.

05

Mapping Group-IB Fraud Protection and BioConfirm to modern authentication and fraud risk controls

Requirement	Group-IB Alignment
Provide customers with easy-to-follow guided instructions and alerts prior to executing transactions	While customer-facing guidance is owned by the bank's digital channels, Group-IB Fraud Protection (FP) generates real-time risk signals that can be translated into contextual alerts, confirmations, or preventive actions. By correlating behavioral biometrics, device intelligence, environmental risk, and fraud intelligence, Fraud Protection enables precise, risk-based customer guidance and proportionate step-up actions such as additional confirmation or biometric verification.
Reduce reliance on SMS-based OTP by implementing in-app push authentication	Group-IB enables the elimination of SMS OTP by combining FP's real-time risk assessment with BioConfirm in-app authentication, allowing banks to replace OTP with risk-based biometric verification, secure push approvals, and cryptographically bound device confirmation, aligned with CBUAE guidance.
Send secure push notifications for high-risk or high-value transactions and account changes	Fraud Protection continuously evaluates device trust, user behavior, environment, and transaction context. When defined risk thresholds are exceeded, BioConfirm triggers secure in-app push notifications requiring biometric approval from the registered, trusted device.
Prohibit SMS OTP, email OTP, or static passcodes as stand-alone authentication	Group-IB supports strong authentication using inherence factors (biometrics), possession factors (trusted, cryptographically bound devices), cross-channel transaction signing, and contextual fraud intelligence, enabling LFIs to avoid weak stand-alone authentication methods fully.
Use strong authentication for 3DS transactions and avoid weak second-factor methods	Fraud Protection delivers unified real-time risk scoring across device, behavior, network, and fraud intelligence to support confident 3DS decisioning. BioConfirm enables in-app biometric authentication and transaction signing, replacing SMS OTP and supporting liability management and dispute resolution.
Apply strong authentication for instant payment enrolment	Fraud Protection secures instant-payment enrolment by validating session integrity, detecting remote access or deepfake-assisted attempts, and ensuring enrolment originates from a trusted device. BioConfirm enables strong in-app confirmation without reliance on SMS OTP.
Secure card provisioning and wallet enrolment without SMS or email OTP	Fraud Protection assesses device integrity, environment risk, behavioral patterns, and prior account activity during wallet provisioning. BioConfirm enforces in-app biometric confirmation and trusted-device binding, ensuring compliant enrolment without SMS or email OTP.

Apply strong authentication for first-time access or new devices	While Emirates Face Recognition is performed by the LFI, FP protects the surrounding context by validating device posture, environment integrity, behavioral consistency, and cyber-fraud indicators, mitigating deepfake-assisted or manipulated enrolment attempts while preserving e-KYC compliance.
Allow lighter authentication for recurring logins from trusted devices	Fraud Protection continuously validates that recurring logins originate from previously bound, low-risk devices operating in safe environments, enabling LFIs to rely on passcodes or device-native biometrics where appropriate.
Require cross-channel confirmation for internet banking logins	Fraud Protection enforces cross-channel confirmation via approvals through the mobile banking app. BioConfirm ensures approvals are device-bound and biometric, while FP applies real-time fraud checks to prevent replay or proxy attacks.
Apply step-up authentication for sensitive account actions (limits, security settings, personal data, new card requests)	Fraud Protection monitors sensitive actions in real time across channels. When elevated risk is detected, preventive action is taken, or BioConfirm enforces biometric or trusted-device step-up authentication, ensuring only legitimate customers can approve changes.
Perform periodic fraud risk and typology assessments	Fraud Protection enables periodic fraud-risk and typology assessments using real-time analytics, historical data, behavioral profiling, cross-channel correlation, and threat intelligence. Dashboards and expert intelligence reports support continuous control refinement.
Suspend sessions when malware, screen sharing, VPN, or remote access is detected	Fraud Protection detects malware, screen sharing, VPN usage, remote-access tools, and active call states. It evaluates overall session trust and enables session suspension, blocking, or step-up authentication, alongside real-time user warnings where appropriate.
Avoid clickable links in email or SMS	Group-IB enables LFIs to shift sensitive approvals from email or SMS links to secure in-app flows using FP signals and BioConfirm, ensuring approvals occur only within trusted, device-bound environments.
Enhance cross-channel fraud detection and intelligence sharing	Fraud Protection correlates fraud intelligence across web, mobile, and 3DS channels to detect coordinated fraud patterns. Integration with Threat Intelligence (TI) and Digital Risk Protection (DRP) enables full-cycle, intelligence-driven fraud detection and response.
Use advanced fraud detection methodologies (behavioral analysis and digital biometrics)	Fraud Protection natively supports behavioral analysis and digital biometrics, continuously profiling interactions and detecting environment risk indicators such as emulators, malware, VPNs, and device tampering across all digital channels.

06

Beyond compliance: A real opportunity to achieve fraud resilience

Many UAE banking systems face foundational challenges: fragmented data across platforms, legacy architecture, incomplete threat visibility, limited operational orchestration, and constrained resources. These constraints make comprehensive, real-time fraud prevention difficult to achieve with current infrastructure alone. However, as the CBUAE regulations urge banks to establish stronger standards for fraud monitoring, compliance, and prevention, this transformation provides a critical window for institutions in the region to fraud-proof their operations and build overall resilience against cyber attacks.

Institutions can close these gaps rapidly by adopting integrated solutions that unify fraud monitoring intelligence and authentication into a single ecosystem - exactly what Group-IB's platform delivers.

Build unified fraud intelligence: End-to-end visibility in real time

Group-IB's Fraud Protection delivers constant, end-to-end visibility and classifies signals across mobile and web environments through continuous analysis of:

- **Device behaviour:** integrity checks, rooting/emulator detection, RAT presence
- **Session anomalies:** overlay detection, remote access signals, unusual navigation
- **Geolocation signals:** impossible travel, risky IP ranges, velocity anomalies
- **Payment patterns:** beneficiary risk, transaction velocity, mule indicators
- **User behaviour:** hesitation patterns, behavioural biometrics, interaction anomalies

These signals give you a complete context of the network activity and help identify **pre-fraud indicators**, allowing banks to intervene way before fraud is concluded. Today, such capabilities aren't as prolifically implemented in UAE banks as needed, but they are essential for meeting CBUAE mandates and achieving true fraud prevention.

Enable intelligent risk assessment: Real-time scoring and correlation

These signals feed directly into your existing risk engine, enriching modern fraud systems with a **unified, correlated, real-time picture of risk:**

- The scope of emerging threats
- Blended attack vectors
- High-risk sessions
- Anomalous interactions
- Indicators of compromise

This is the point where the system “thinks” and “acts” adaptively rather than relying on passive alerts.

Do not give fraud consent: Authenticate true user intent with Bioconfirm

Group-IB Bioconfirm is one of the strongest modern authentication solutions.

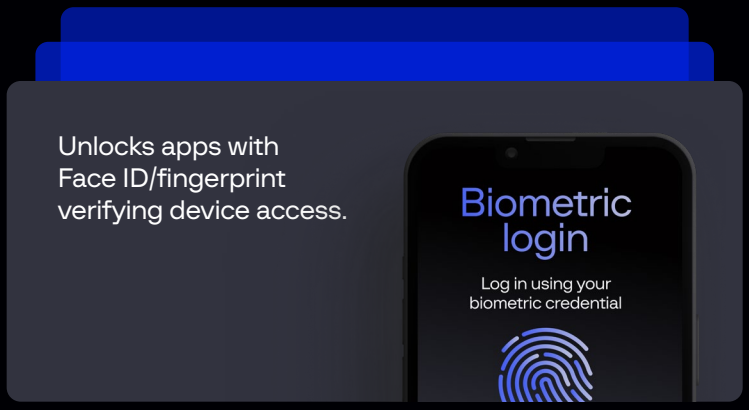
- One-tap Face/Fingerprint user consent on their trusted device
- Cryptographic tokens that no fraudster can see, spoof, or intercept
- Highest-level security for real users, with zero extra effort
- Desktop emulators, phishing, and SIM-swaps? Blocked by design
- Malware-resistant protection for mobile banking apps
- Easily integrates with your risk engine + PSD2 / RBI compliance

Using real-time, token-based technology, it is only visible and actionable by the true account holder. **Maximum security, zero friction — no added steps ensure the customer experience stays intact, and authentication becomes proactive and unspoofable, unlike easily exploitable OTPs**.

How it works

Standard biometric login

What it does



Bridging the gap in current authentication controls

Only confirms device access, not the account holder’s intent for specific actions (e.g. transfers). Vulnerable to malware, stolen credentials, spoofing; Sends “Login OK” flag, without proof of user consent.

BioConfirm and Fraud Protection also feed authentication outcomes (success or failure) and fraud signals into your fraud detection logic and digital identity verification systems. These signals enhance your banking security risk engines with device-bound authentication and sessional insights, improving detection of anomalous behavior and fraudulent activity.

Make your systems adaptive and intelligent: Build unified intelligence through continuous feedback

The integrated insights from BioConfirm and Fraud Protection enable banks to achieve unified visibility, early detection, improved accuracy, and the **ability to understand complex, multi-step attack chains - while maintaining CBUAE compliance. This level of comprehensive defense is simply not possible with siloed systems.**

Through Group-IB's Threat Intelligence **(the industry's largest global and regional presence among cybersecurity technology providers),** regional hubs with localized expert presence, advanced technology platform, banks gain an always-on defense ecosystem that continuously evolves to maintain the highest level of resilience and defense posture.

07

The path forward: Preparing for the March 31st, 2026, deadline (and beyond)

The CBUAE has established a clear mandate: by 31st March 2026, weak authentication methods must be eliminated and replaced with strong, adaptive, customer-centric security.

For banks, this deadline is more than a regulatory compliance exercise; it's an opportunity to modernize digital channels, strengthen customer trust, and significantly reduce fraud losses. The transformation requires strategic planning, integrated technology, and experienced partners who understand both the regulatory landscape and the technical complexities involved.

Group-IB partners with LFIs throughout this journey. Start with our compromise assessment to identify gaps and priorities specific to your institution, then discover how Group-IB's integrated fraud defense platform enables you to meet CBUAE requirements while building comprehensive protection that evolves with emerging threats.

GROUP-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,550+
Successful investigations of high-tech crime cases

500+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor
*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- Forrester
- datos INSIGHTS
- kuppingercole ANALYSTS
- Gartner
- IDC
- Frost & Sullivan

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785