pwc

Closing the fraud gap: How banks and telcos can join forces in the Middle East

Ever wondered how digital fraud schemes really work? This report examines the critical link between banks and telecom operators — and why a unified, cross-sector strategy is essential to shutting down today's most sophisticated scams.

Over the past decade, digital banking has redefined the financial landscape across the Middle East. Customers now expect seamless, mobile-first services and financial institutions have delivered. As banks and their regulators race to innovate, fraudsters are evolving just as quickly. Many of today's most damaging scams such as SIM swaps, phishing and account takeovers, rely not only on weaknesses in financial systems but also on vulnerabilities in telecom infrastructure. Combating these threats requires more than sector-specific solutions; it calls for a coordinated, cross-industry response.

Digital fraud trends and the case for collaboration

While digital transformation in banking has significantly enhanced customer experience, it has also introduced new risks. **A recent Lexis Nexis report**[1] revealed that 42% of UAE organisations have experienced an increase in online fraud year-on-year. Across Europe, the Middle East and Africa (EMEA), digital channel fraud now accounts for over half of total fraud losses. These figures highlight the urgent need to revisit and enhance fraud prevention strategies – moving beyond internal investments to encourage industry-wide collaboration.

Banks and telecom providers rely on personal data for onboarding and monitoring customers, yet the lack of integration between these industries creates exploitable gaps. Fraudsters use these weaknesses to deceive customers and bypass controls. To effectively shut down these fraud schemes, banks and telecom providers must combine their strengths, linking identity systems, sharing threat intelligence and coordinating fraud response protocols. Collaboration is no longer a competitive advantage, it's a necessity.

[1] https://risk.lexisnexis.com/global/en/about-us/press-room/press-release/20240417-true-cost-of-fraud-uae

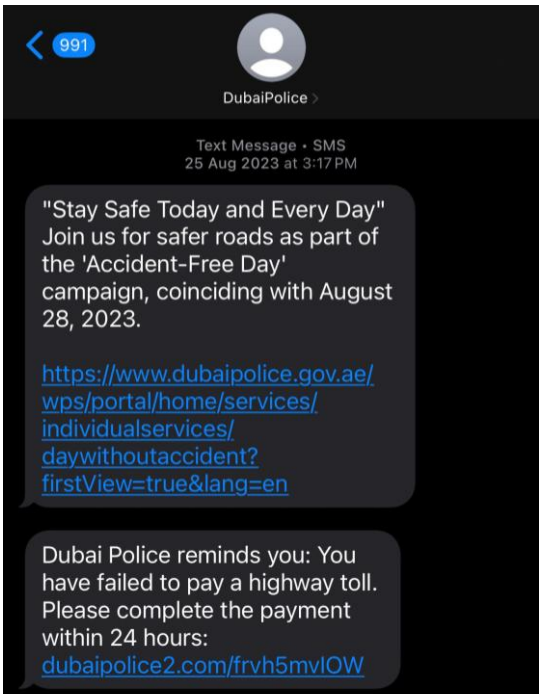
Fraud trends and the role of convergence in combating them

Anti-fraud efforts across banking and telecom often remain fragmented and fraudsters exploit the gaps. For instance, a SIM swap may allow a criminal to intercept one-time passwords and drain a victim's bank account before anyone notices. Without real-time data sharing, these attacks often slip through undetected and telecom companies may be unaware that a customer has been blacklisted by a bank.

Below, we explore some of the prevalent digital fraud trends and how better integration between sectors could close these gaps.

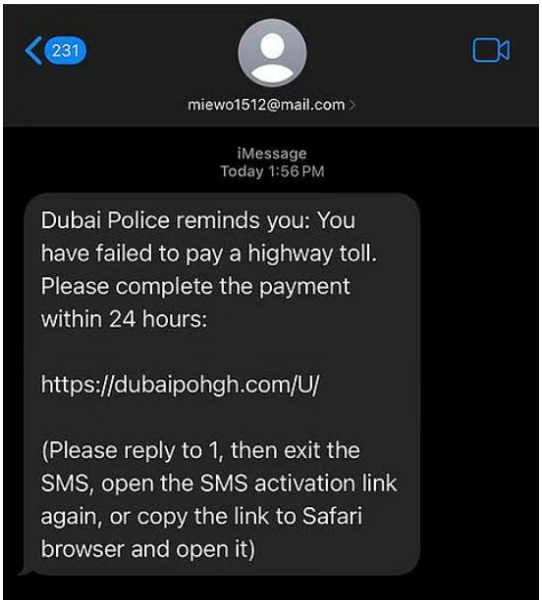
SIM swap fraud:

SIM swap attacks involve fraudsters persuading telecom operators to transfer a victim's phone number to a new SIM card. Once completed, the fraudster can intercept all calls and text messages, including one-time passwords (OTPs) used for banking transactions. This allows fraudsters access to all the calls and texts meant for the original owner, including one-time passwords (OTPs). The OTPs give them access to sensitive accounts like banking, email, or social media, often before the victim even notices anything is wrong. This global fraud type has risen over 1,000%+ in countries such as the UK [1]. Better coordination between banks and telcos, such as real-time SIM swap alerts, would, therefore, allow financial institutions to flag and halt suspicious account activity immediately.



Social engineering, job offer and investment scams:

Scammers trick victims into providing confidential information by impersonating as government officials or bank employees. This allows them to access personal accounts through the OTPs and web meetings [2]. Social engineering scams have risen by over 2,000% (assisted using AI and deepfake technologies). Job offer scams are on a similar trajectory [3] "pig butchering" investment scams continue to command large loss sizes (US [4], often facilitated by crypto and human trafficking). Better integration could help here as well – a telco-run blacklist of numbers linked to fraud complaints, shared with banks, could trigger heightened monitoring of accounts linked to those numbers.



[1] https://www.cifas.org.uk/newsroom/huge-surge-see-sim-swaps-hit-telco-and-mobile
[2] https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year?utm_source=chatgpt.com
[3] https://www.pbs.org/newshour/show/how-human-trafficking-victims-are-forced-to-run-pig-butchering-investment-scams
[4] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

Mule account networks:

Criminals frequently use ‘money mules’ or individuals who allow their accounts to be used to receive and transfer stolen funds. Some are complicit, others are unaware. These mule accounts often appear legitimate on the surface, making detection difficult. Joint analytics between the banks and telecom companies would allow for the speedy detection of unusual mobile communication patterns tied to suspicious financial transfers, enabling quick freezing of the accounts and SIMs involved. Sudden SIM swaps, changes in location, or other changes to the user’s activity pattern can be notified by the telecom companies to the banks through a joint working committee set up between the two, with oversight from regulatory authorities, enabling real-time communication exchange that could assist in identifying mule accounts.

KYC manipulation and account takeovers:

Advances in AI tools have made it easier to forge highly convincing ID documents and bypass Know Your Customer (KYC) checks.
Stolen KYC documents or forged KYC documents can be used by fraudsters to recover/reset accounts, thereby changing the profile details of the customer, including email address, phone numbers and passwords. By synchronising KYC and eKYC processes across banks and telecoms, organisations can cross-validate identity information, flag discrepancies and reduce onboarding risk.
Shared data and AI tools can also be used to detect signs of document tampering or unusual registration behaviour. This would not only mitigate the use of falsified KYC documentation but would also crack down on account takeover and identity theft fraud, which have impacted the telecom and banking industries.

Modus operandi of a fraudster for siphoning funds

Account takeover occurs through techniques like phishing and social engineering whereby the fraudster gains unauthorized access to a legitimate user's online banking / mobile banking account.

Legitimate bank account ✕
Mule account ✓

The fraudster now sets up the legitimate banking account as their mule: disabling notifications, changing the mobile number so that they receive the notification instead, and thereby gaining control of the account.

Legitimate bank account ✕
Mule account ✓

Now, the siphoning begins. The fraudster deposits stolen funds from other victims or fraudulent sources into the victim's now-turned-mule account

Outflow of cash

Once all the funds are transferred to the mule account, the fraudster now initiates large outflows to quickly get the money.
This could be through international transfers or buying cryptocurrencies or simply withdrawing the cash.

At the end of it all, the victim of the account takeover is scrutinized and maybe even penalized because it looks like all the stolen funds were siphoned through their account and no one can trace the fraudster.

“

Global identity theft losses reached US$15.6bn in 2024, a trend expected to rise without integrated KYC systems[1]”

[1] https://javelinstrategy.com/research/2025-identity-fraud-study-breaking-barriers-innovation

Unlocking the power of collaboration

While fraudsters often stay one step ahead, banks and telecom providers must respond with an equally agile, collaborative approach. Below are the key areas where convergence can drive meaningful impact:

All-in-one identity verification:

Telecom operators leverage customer data through mandatory SIM registration processes, including government-issued ID verification. Banks can leverage this verified data to strengthen their onboarding processes. For example, matching SIM registration details with account creation records can prevent impersonation and fraudulent account openings. Additionally, real-time alerts from telecom companies when a SIM swap occurs can enable banks to automatically hold or flag transactions until further authentication is completed.

Unified customer awareness campaigns:

Customer education remains a frontline defence against digital fraud. While financial institutions have made significant strides in this area, a coordinated effort with telecom providers can expand reach and effectiveness. Joint awareness initiatives using SMS, email and applications can help customers recognise red flags, avoid scams and maintain digital hygiene. Tailoring these messages to specific customer segments ensures relevance and resonance. In the Middle East, several regulators have already issued directives and frameworks requiring financial institutions to implement fraud awareness campaigns and a unified approach between banks and telecoms could amplify their impact
and reach even further.

Shared risk intelligence platform:

A shared platform for real-time threat intelligence would allow banks and telecom operators to exchange signals such as backlisted phone numbers, fake or compromised IDs and behavioural indicators, which include frequent SIM swaps among others. A recent introduction of shared intelligence can be seen in India, where the Department of Telecommunication (DoT) introduced India's Financial Risk Indicator (FRI), where telecom providers send risk signals to financial institutions based on analytics and cybercrime inputs.

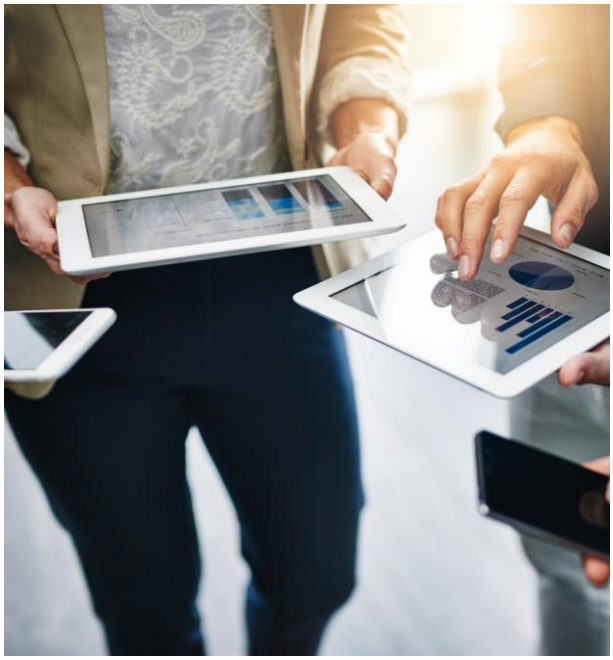
These risk insights allow banks and fintech companies to apply additional safeguards before processing high-risk transactions. The FRI is a risk-based model that classifies a mobile number to have been associated with medium, high or very high risk of financial fraud by leveraging inputs from cybercrime agencies. Fintech companies in India have already started integrating FRI alerts in their systems, configuring multi-step authentications if such mobile numbers are involved in a financial transaction.

Considerations for the convergence: Navigating the fine line

While collaboration between banks and telecom operators presents a powerful opportunity to combat digital fraud, it also presents important challenges. The following considerations are critical to ensuring that any collaboration is both effective and sustainable, while meeting regulatory, operational and cybersecurity standards.

Data protection and privacy issues:

Sharing customer information for fraud prevention purposes raises valid concerns from consent and data sovereignty to regulatory compliance. With growing cyber threats and the proposed exchange of information between banks and telecom companies, responsible data sharing is essential. To make convergence sustainable, both industries must align on privacy standards, cybersecurity protocols and third-party risk frameworks. Regulators in both sectors should establish a baseline security framework for any shared platforms or databases, ensuring consistent compliance across the board.



Establishing accountability:

Defining clear roles and responsibilities is essential to ensure that no fraud case falls through the cracks. A success story in establishing this framework can be seen in Southeast Asia – Singapore. The Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority of Singapore (IMDA) had come out with a Shared Responsibility Framework (SRF) last year to tackle phishing scams[1].

The SRF calls out the individual responsibilities of both telecom companies and financial institutions to determine accountability for fraud cases. The entity that fails to fulfil its duty as per SRF will be held accountable and will have to compensate the customers for the fraud loss incurred. Similarly, regulators across the region will have to draft a framework that details clear accountability and escalation protocols to ensure a successful partnership.

Interoperability between sectors:

Both industries operate based on separate regulations, organizational culture and technological systems. Ensuring convergence across these elements not just requires support and frameworks from regulators, but also collaboration from policy makers, board members & C-suite executives as well as regulatory bodies across both the telcos and banks to tackle the risks they face today.

[1] https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework

A shared vision for a safer digital ecosystem

While innovation fuels growth and convenience, it also expands the attack surface. Fraudsters continue to exploit gaps between siloed systems, institutions and industries. The best way forward is one of integration, combining insights, infrastructure and intelligence across banking and telecom to protect the digital ecosystem.

Fraud is an ever-evolving, ever-changing concept. The future of fraud prevention is not just about reacting to yesterday's scams; it's about anticipating the threats of tomorrow, adapting to them in real time and building a unified defence strong enough to dismantle them.

Key contacts

Rana Shashaa

Middle East Forensic Leader, PwC Middle East

rana.shashaa@pwc.com

+971 56 661 3444

Collin Keeney

Partner, Forensic Services, PwC Middle East

collin.keeney@pwc.com

+ 971 50 650 1829

Prabodh Newar

Director, Forensic Services, PwC Middle East

prabodh.newar@pwc.com

+971 55 802 1365

Gaurav Malhotra

Senior Manager, Forensic Services, PwC Middle East

g.malhotra@pwc.com

+971 58 662 3037

Contributors

Ashok Babu

Manager, Forensic Services, PwC Middle East

ashok.b.babu@pwc.com

+971 54 734 9960

Junaid Sabri Khan

Senior Associate, Forensic Services, PwC Middle East

junaid.sabrikhan@pwc.com

+971 54 581 5185

pwc.com