The need of the hour:

Stepping-up counter fraud controls in the banking sector

The Gulf Cooperation Council (GCC) countries' economic recovery since the peak of the pandemic in 2020 has been remarkable; it has been so convincing that their economies were projected to have grown at their fastest pace in more than a decade in 2022.[1] The flurry of economic activity also resulted in increased financial fraud (FF), specifically in the financial services sector.

FF has had a dramatic surge in the region in the post-pandemic era. In Q2 of 2022, reported FF cases more than doubled in the region compared to the previous quarter.[2] A recent survey reported 62% of KSA residents have experienced attempts of FF while 14% have been impacted by some form of fraud.[3]

Regional authorities have taken notice of this surge in fraud related incidents and have introduced measures to enhance the controls to counter fraud - key measures such as the below:

- The Central Bank of the UAE, UAE Banks Federation, Abu Dhabi Police, and Dubai Police launched the country's first-ever National Fraud Awareness campaign.[4]
- The Qatar Central Bank spread Counter Fraud (CF) awareness amongst the public via their communication channels.[5]
- The Saudi Central Bank issued a CF Framework for its member organizations to comply with by June 2023.[6]

In tandem with the authorities, banks have a vital role to play in the fight against FF. Governance, technology, and people are 3 key pillars that the banks should be focusing on within their CF program.[7]

Governance

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), a leading issuer of fraud risk[8] management guidance, describes fraud risk governance as an integral component of corporate governance and the internal control environment; it designates the board and executive leadership to be ultimately responsible for the CF program. The governance of fraud risk varies from bank to bank. This is evident when looking at where fraud risk lies at leading global banks. At HSBC, the group risk and compliance function is responsible for fraud risk, at Standard Chartered Bank, the financial crime compliance (FCC) function is responsible for it.[9] In the GCC, governance of fraud risk is usually the responsibility of either the compliance function or the risk management function.

Regardless of where ownership of fraud risk lies within the bank, it is important for the owner of the risk to have sufficient understanding of the current threats/ trends and the mitigating controls' effectiveness to ensure that residual risk is in line with the bank's agreed risk appetite.

Technology

A surge in financial fraud

Increased digitalization and remote-payment of products and services in recent years has also resulted in innovative ways for fraudsters to bypass the banks' controls. For example, fraudster(s) developed fake websites that greatly resembled the domain-name and appearance of a leading recruitment company's website in order to steal customers' online/mobile banking credentials. The stolen credentials were then used to transfer moderate amounts (SAR20,000–70,000) to "money mules" (i.e., associates who receive stolen funds for further money laundering or immediate cash out via ATM). The worrisome matter is that this fraud was conducted in such a way that it out-maneuvered traditional CF controls such as one-time passwords (OTPs) and legacy fraud detection systems.[10]

In another example of FF sophistication, a fraudster was able to successfully transfer out AED9.5 million from a customer's bank account. After obtaining the mobile/ online banking log-in details (via a phishing/ vishing scheme), the fraudster submitted a cancellation and replacement issuance request for the SIM registered with the bank. Following receipt of the replacement SIM, the fraudster conducted forty-six transactions over a month to empty out the bank account.[11]

The ever-evolving modus operandi of fraudsters is increasingly propelling regional banks to look at more proactive technological solutions. Technology, such as the below, is enabling interesting use cases to prevent FF.

- **Artificial intelligence (AI):** AI-powered solutions can be implemented to recognize suspicious behavior in the bank's transactions. Such solutions scan data passage through systems in real-time (e.g., on the basis of geographical location, rhythm of inputting log-in credentials, new device log-in), flag suspicious transactions, and issue alerts for investigation.
- **Machine learning (ML):** Simple rule-based solutions often lead to a high volume of false positive alerts for a bank's limited resources to manually review and close. ML allows banks to automate the ongoing update of their existing technology solutions to adapt and prevent existing and future threats.
- **Biometric data:** The use of biometrics (e.g., fingerprint, retinal scan) to access online banking channels can add an additional layer of protection for a bank's customers, especially against phishing/ vishing.

Banks need to urgently revisit their CF program and ensure that they invest in updated technology for real-time fraud monitoring to ensure proper safeguards are in place against fraudsters. The value of a fraud detection system is highly dependent on the quality and quantity of the data it has access to. Thereby, by using collective intelligence from multiple sources, banks can increase the effectiveness of their dedicated CF solutions. Organizations who have made investments in CF technology (in the post-pandemic era) have experienced a 60% decrease in their fraud cases.[12]

People

No matter how robust the control framework is, the human element continues to be the most important control against FF. A recent study has identified that over 137,000 Arabs visit fraudulent

websites through which they are subjected to various fraud schemes every day.[13]

It is the banks' responsibility to adequately train their internal stakeholders (i.e., employees, executive leadership, board members) and spread awareness amongst internal and external stakeholders (i.e., third-parties, customers). Although most organizations do provide CF-related training and awareness, a recent survey indicated that almost half of the organizations find their CF training and awareness to be inefficient.[13] Banks need to consider how they can optimize the efficiency of their existing CF training and awareness frameworks for each respective audience group.

As technology advances, fraudsters will continue to come up with innovative techniques to exploit the population's limited awareness of FF and take advantage of CF program deficiencies. While banks in the region have made great strides in fighting FF, fraudsters remain a step ahead of the curve; this clearly puts the onus on the bank to protect its customers and itself from FF.[14] It is time for banks to invest in their CF programs, especially with advanced CF technologies, to ensure fraud is prevented, rather than investigated.

By **Saad Qureshi**, Director, Financial Crime and Analytics and **Humaid Hussain**, Senior Associate, Financial Crime and Analytics, Deloitte Middle East

As technology advances, fraudsters will continue to come up with innovative techniques to exploit the population's limited awareness of FF and take advantage of CF program deficiencies

Endnotes

1. "GCC economies set to grow at fastest pace in a decade on higher oil prices," The National, February 3, 2022.
2. "UAE: 3.4 million phishing attacks detected in second quarter of year," Khaleej Times, August 6, 2022.
3. "62% of Saudis exposed to attempts of financial fraud, survey shows," Zawya, April 27, 2022.
4. "UAE's first national fraud awareness campaign begins to curb Covid-19 scams," The National, April 14, 2020.
5. "Qatar Central Bank warns against cyber fraud," Qatar Peninsula, August 18, 2022.
6. Circular 44021528, SAMA, October 2022.
7. Fraud Risk Management Guide-E Summary, COSO, September 2016.
8. Annual Report and Accounts, HSBC Holdings PLC, 2021.
9. Annual Report, Standard Chartered, (2021).
10. "Cybercriminals are targeting financial institutions in the Kingdom of Saudi Arabia," Arabian Business, May 18, 2022.
11. "Dubai court tells bank to pay Dh9.5m to customer that he lost in unauthorized transactions," The National, April 27, 2022.
12. Middle East Fraud Survey, Deloitte, (2021).
13. "Saudi university issues warning over rise in online fraud," Arab News, April 29, 2022.
14. Middle East Fraud Survey, Deloitte, (2021).