CENTRAL BANK OF EGYPT
Egyptian Banking Institute

البنــك المركــزى المصــرى
المعهــد المصرفــى المصــرى

CURRENT TRENDS

November 2021

Fraud in Digital Banking

MOVING FORWARD WITH CONFIDENCE...

Introduction

As banking evolves and changes across the globe due to advanced technologies, fraudsters found new sophisticated ways of attacking banking systems with technologically-advanced tools that make fighting fraud the main challenge for financial institutions & represent a major threat to the banking structure and the entire economy if not managed & controlled efficiently.

The banking industry has always been under tremendous pressure to accelerate digital transformation, combat all sorts of financial frauds, and meet customer demand for immediacy and personalized experience. In addition to arming themselves with efficient financial crime and fraud management solutions in a widely digitized world.

Consequently, the emergence of advanced technologies is a double-edged sword, as it is not only reshaping the banking industry but is also making it vulnerable to severe financial frauds, which make fraud management nowadays a persistent challenge and a key concern for banks, as advanced technologies have widened the threat landscape related to financial crime, as it increases cybercriminals' opportunities to prey on every digital consumer.

Therefore, such threats require financial institutions, to adopt robust technology-based fraud prevention tools, re-think their traditional approach to fraud, and understand how the fraud lifecycle unfolds, while at the same time, offering a seamless user digital experience, in order not to lose its credibility and associated business.

How and where Digital Fraud happens?

- **Cybercrime**: Online theft committed on a financial institution's internet or computer networks.

- **Phishing/Smishing/ Vishing Scams**: Refers to a method for gathering personally identifiable information (PII), using deceptive e-mails and fake websites that can be used to access customer accounts. For instance, sending links via emails to direct customers to fake online banking web pages.

- **Malware**: Refers to a computer program that, when installed on a device, can collect data or information for financial transactions. This malware can automatically perform transactions on behalf of customers after hacking into a legitimate session or stealing credentials, including second-factor authentication.

- **Porting**: This is the transfer of a user's mobile phone number from one service provider to another & once the fraudster has access to the user's messages, they can retrieve one-time passwords and make payments via the user's online banking.

- **Identity takeover**: Stealing an individual's personal and/or financial information to access their banking accounts. This usually involves obtaining a full name, date of birth, and address and passing identity verification over the phone.

- **Mobile Banking Fraud**: Smartphones and mobile banking applications are increasingly becoming targets for fraudsters. Hackers target the information on the device, as well as the information the device can access and the messages it receives.

- **Card Not Present (CNP) or Remote Purchase Fraud**: Involves the fraudulent use of card details obtained through: digital attacks, spam e-mails or calls to make purchases over the Internet that do not require a physical card for payments.

- **Counterfeit Card**: Refers to a fake card created using compromised details from a magnetic strip of a genuine card.

- **New Account Fraud**: Creation of a new banking account by an unauthorized person using the customer's personal information.

- **Account Take Over (ATO)**: Gaining illegal access to an existing user's account in order to steal funds and make unauthorized transactions.

- **Debit or credit card Fraud**: It is the unlawful use of a credit/debit card to falsely obtain money or belongings without the awareness of the credit/debit card owner.

- **Point of Sale (POS) Attack**: The hackers used malware that transmits card information automatically to them when a card is swiped at the point of sale (POS).

- **Investment and online shopping scams**: Presenting fake online offers to make customers believe in a smart investment that seems of great benefit.

- **ATM scams**: Through the incorporation of devices within ATMs that can record and steal confidential information from the customer's card.

How can financial institutions combat fraud & secure digital transactions?

- Developing a technology-based anti-fraud system:

The effectiveness of technology-based anti-fraud systems depends crucially on their ability to detect possible instances of fraud in real-time, so that suspicious activity can be flagged & identified immediately which is an impossible feat for humans.

Accordingly, a technology-based anti-fraud system must employ big data technologies, allowing it to apply advanced analytical techniques to huge volumes of transactions once occurred, besides incorporating machine-learning techniques to improve its systems' sensitivity and ability to differentiate between legitimate transactions and frauds.

Such practices ultimately contribute to strengthening the most important asset that banks have which is the customers' trust in their brand.

- Implement multi-factor authentication controls:

Multiple authentication controls such as biometrics (e.g., fingerprints, voice & facial recognition), E-signatures to securely enable digital transactions, & text message verification proves its effectiveness over one-time passwords alone (OTPs) at reducing various types of fraud. Such precautions make it difficult for fraudsters to impersonate account holders. Additionally, behavioral authentication should be implemented which uses algorithms to detect abnormal behavior like unusual IP addresses and multiple failed login attempts.

- Educating customers:

One of the most important steps in educating the customer is continually engaging with them to raise their awareness about different types of fraud, & how to proactively protect themselves, by publishing some useful tips on the bank's official website on how to secure themselves, to avoid becoming a victim of fraud, or through a guidance pamphlet available at the branch.

- Make employees fraud awareness and training a requirement:

All employees, especially front-line employees and customer service specialists, should be knowledgeable about fraud threats and & how to detect red flags. Employees must also know which steps they should take when a fraud attack occurs, and how to contain it.

- Effective communication with customers:

Digital banking, although convenient, reduces human interactions a bank has with its customers. But fraud is a major issue, and customers need an easy way to reach out to their banks, report a suspected case of fraud, and be taken seriously when they do. Therefore, banks should find the right communication tools that assure they are actively preventing fraud while not causing unnecessary anxiety to their customers.

- Beware of Internal Fraud:

Although financial frauds that occur today are due to outside factors, there's still a possibility of fraud being committed by someone employed at the institution. Accordingly, financial institutions should adopt a zero-tolerance culture for internal fraud, to maintain a culture of accountability among employees of the consequences of committing fraud, besides using careful hiring practices & checking the backgrounds of each potential employee.

Fraud Prevention Challenges in Digital Banking

- Keeping anti- fraud systems up to date:

Despite having multiple fraud systems in place, some banks and financial institutions still have gaps in their fraud protection systems, because their multiple fraud detection technologies weren't designed to work together to combat & detect potential frauds.

keeping a regularly updated anti-fraud system is a must to monitor all of the activities that users perform through their digital journey such as: (logged in used devices, any change in user's profile details, any updates in account's access permissions, adding a payee, submitting a financial transaction, comparing the customer's current behavior with their previous behavior through online and mobile banking sessions, etc.).

By monitoring all of these activities & avoiding one size fits all approach, the bank's anti-fraud system could identify, detect suspicious actions & predict the probability of fraud before taking place.

- Optimizing the customer's experience:

To optimize the customer's experience, financial institutions must proactively deploy intelligent systems that can detect fraud, while ensuring these systems don't dampen or put any obstacles to the customer's digital experience besides injecting additional security measures only when necessary.

- Meeting regulatory requirements:

The regulatory environment seems to become more complex & volatile every year, and financial institutions must have anti-fraud solutions that are in line with the diverse regulatory rules & are constantly updated based on the newly issued regulations by central banks.

- Minimizing costs related to fraud through:

- Maintaining a well-trained internal fraud team
- Keeping the cost of upgrading to advanced anti-fraud technology under control, while ensuring the ability to detect emerging attack scenarios using the current anti-fraud systems.
- Avoiding incurring fines for non-compliance; and indirect costs related to poor user experience & abandonment; lack of customer's trust, and reputational damage.

Examples from global financial institutions adopting anti-fraud practices

- The central bank of Malaysia, the Hong Kong Monetary Authority, and the Monetary Authority of Singapore (MAS): Have released technology risk management guidelines for financial institutions (FIs) to address the security gaps. The MAS guidelines comprised a set of key technology and cyber risk management principles and best practices, which FIs can adopt to prevent fraud, given certain conditions such as the nature, size, and complexity of its business.

- Bank of America: Having a sustainable cybersecurity program built on accountability, consistency, and measurements to assess potential frauds. In addition to a strict code of ethics for all employees that require confidential treatment of client information. Furthermore, providing all employees with information protection training annually, and making the completion of this training a must to all employees. In addition to regularly updating various security pages on their official website, for example, online banking security, credit & debit card security, as a guide for customers on how to protect themselves against suspicious activities.

- Bank of Scotland: Adopting an approach to fraud risk management that seeks to balance the demands of minimizing losses resulting from fraud, whilst being sensitive to the impact on the customer's digital experience. The bank utilizes various advanced tools such as device identification of the phones & tablets used by customers, in conjunction with biometric behavioral technologies through adopting voice ID, which allows customers to use their voice instead of writing their passwords for accessing their accounts, and Fingerprints ID, to verify themselves when using mobile banking Apps.

- **Barclays:** Having a dedicated team available 24/7 if customers need advice or help in addition to, an advanced Fraud detection system that monitors transactions and payments on a real-time basis. The bank also deploys Biometric systems helping in tracking users' normal behavior when viewing their account details online, in order to identify if a fraudster has accessed personal users' accounts, such tools are strictly used in compliance with the bank's internet banking terms and conditions, to protect customer's privacy and information.
- **Starling Bank:** A digital bank in London, their expert fraud team puts in place a series of sophisticated, automated fraud controls such as Identity and verification checks, including video verification and anti-impersonation measures during the customer's onboarding process. The bank also incorporates In-app card controls features, allowing customers to take control of their card functionality themselves. For example, freezing their card in case it's lost to restrict unauthorized transactions. Also, applying Real-time fraud prevention solutions that monitor all digital payments 24/7, besides multi-factor authentication tools.

HOTLINE

15200

One number to better serve you!

Headquarters – Nasr City
22 A, Dr. Anwar El Mofty St., Tiba 2000
P.O.Box: 8164 Nasr City, Cairo, Egypt

www.ebi.gov.eg

Like us on
facebook.com/EgyptianBankingInstitute

Follow us on
instagram.com/egyptianbankinginstitute

Join us on
linkedin.com/company/egyptian-banking-institute

Watch us on
YouTube Channel: Egyptian Banking Institute (EBI)