Financial Stability Institute | BIS

Digital fraud – Executive Summary

The ongoing digitalisation of finance brings numerous benefits, such as increased efficiency, convenience, financial inclusion, transparency and quicker responses to crises. However, it also introduces significant risks to bank soundness and financial stability. One such risk is digital fraud.

To provide a high-level assessment of digital fraud, its supervisory and financial stability implications, and the initiatives to mitigate digital fraud in the banking sector, the Basel Committee on Banking Supervision (BCBS) issued a discussion paper in November 2023 – *Digital fraud and banking: supervisory and financial stability implications*.

What is digital fraud?

Digital fraud is defined as fraudulent activities conducted through digital means to steal banking assets or customer credentials. It targets primarily bank customers and relies on deception. Banks can play an indirect and involuntary role in digital fraud's transmission. The BCBS paper categorises digital fraud into four main types.

Unauthorised payment transactions

This includes the theft of a customer's payment card data through the installation of malicious scripts on e-commerce sites or social engineering techniques (eg phishing emails or SMS). The fraudster then uses the data to make payments or sells the data on hidden and obscure parts of the internet.

Manipulation of payers to issue payment

This involves fraudulent transactions made as a result of the payer being manipulated by the fraudster, eg through social engineering techniques, impersonation of the bank or any other trusted third party. The payer is directed to issue a payment order or to give the payment service provider the instruction, in good faith, to issue a payment to an account the payer believes belongs to a legitimate payee.

Fraud related to other banking products

Such fraud involves other banking products beyond payments, such as when customers are manipulated into investing in fake saving products or taking on fake credit products.

Fraud related to the bank through customer data or bank systems

This type of fraud targets the bank itself through misuse of customer data or bank systems. Examples include opening bank accounts or applying for credit cards using stolen or false identities, and the use of these accounts/cards for fraudulent transactions. It can also involve compromising the bank's information system, obtaining an administrative user's credentials for the mobile banking portal and using this access to edit customers' mobile numbers to bypass one-time password authentication, increase account limits and conduct fraudulent fund transfers.

What are the supervisory and financial stability implications of digital fraud?

The supervisory and financial stability implications of digital fraud can be significant. There are two main transmission channels: financial losses to banks and reputation risks to banks and supervisors.

Banks may suffer financial losses if they unknowingly send funds to fraudulent counterparties or if they need to refund customers for losses. In extreme cases, such financial losses could reduce banks' capital resources and shock-absorbing capacity, which may have spillover effects to other banks or market participants.

Reputation risks to banks and supervisors may result from high-profile digital fraud incidents that could erode public trust and lead to mass withdrawals of deposits.

Quantifying the extent of digital fraud is challenging due to data gaps, lack of harmonised definitions and differences in data collection across jurisdictions. Despite these challenges, available data suggest that the current risk to financial stability from digital fraud is limited. The first type of digital fraud (unauthorised payment transactions) is the most documented, while documentation of the other three types is still limited due to the aforementioned challenges. Nonetheless, absence or scarcity of data does not necessarily mean absence of risks.

What is being done to mitigate risks from digital fraud?

There is a wide range of domestic and regional initiatives to address digital fraud.

Public awareness and empowerment

Many jurisdictions issue warnings or advisories and undertake education campaigns to increase consumer awareness of risks and emerging fraud techniques. Educated customers are the first line of defence, making customer education one of the most important prevention tools. Initiatives also seek to empower customers by providing them with tools to notify their banks when using different channels, such as mobile applications or web pages, and by offering flexibility for credit card holders to opt in or set sub-limits for higher risk situations, such as transactions not requiring presentation of the card.

Requirements and guidelines with regard to control measures and security protocols

Authorities in most jurisdictions issue guidance or policy statements setting out requirements or expectations regarding security protocols, such as multifactor authentication, information/data security and transaction monitoring, as well as reporting data on payment fraud for trend and pattern analysis to support supervisory actions. Some jurisdictions also promote the use of recognised digital identification systems for customer due diligence.

Supervision of banks' digital fraud risk management practices

Many jurisdictions include aspects of fraud-related controls in their supervisory regimes, including on-site inspections, collection and analysis of fraud-related data and encouragement of the use of technology to address fraud risks.

Collaboration among stakeholders for an ecosystem response

Some jurisdictions adopt collaborative and structured methods for monitoring and handling transactions affected by digital fraud to improve detection, response and disruption of fraudulent fund flows. Specific

measures may include mandating harmonised security measures, information sharing and regulatory reporting.

Cross-border cooperation

Digital fraud can occur across borders, indicating a role for international cooperation. At present, channels for cooperation among law enforcement agencies exist through mutual legal assistance requests for individual cases. There are also bilateral channels for sharing relevant information under memoranda of understanding between financial regulators and other authorities.

At the global level, initiatives by global standard-setting bodies, such as the Financial Action Task Force (FATF) and the Committee on Payments and Market Infrastructures (CPMI)-International Organization of Securities Commissions (IOSCO) further support efforts to combat digital fraud. The FATF's work on cyber-enabled fraud and the CPMI-IOSCO *Principles for financial market infrastructures* provide valuable frameworks for managing fraud risks and enhancing the resilience of financial systems. In the case of the BCBS, digital fraud, while not explicitly defined, is covered in the Basel Core Principles, the operational risk and operational resilience standards and the *Risk management principles for electronic banking*.

This Executive Summary and related tutorials are also available in FSI Connect, the online learning tool of the Bank for International Settlements.