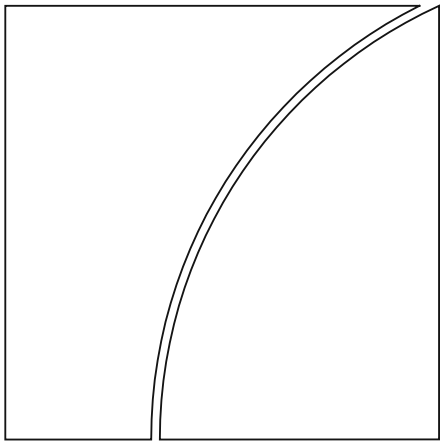
Basel Committee
on Banking Supervision



Discussion paper

Digital fraud and banking: supervisory and financial stability implications

Issued for comment by 16 February 2024

November 2023

BIS

This publication is available on the BIS website (www.bis.org).

ISBN 92-9197- 978-92-9259-709-2 (online)

Contents

Introduction

The ongoing digitalisation of finance can provide benefits to the economy as well as to financial stability. These include greater efficiency in the provision of key banking services (eg lower costs and faster execution), more convenience for customers (eg greater distribution channels and easier user interfaces), enhanced access to banking services for a greater portion of the world's population (ie financial inclusion), increased transparency in financial transactions and faster response to crises (eg faster communication and decision making, helping authorities and institutions to respond more effectively). Examples of such benefits include instant and standardised payment systems, mobile banking platforms and, in principle, applications of distributed ledger technology to finance.

But technological banking advancements can also increase risks to bank soundness and financial stability. One such example is digital fraud: criminals are exploiting digitalisation to commit online fraud at a greater scale and scope than previously – notwithstanding important data caveats and gaps – as digitalisation enables fraudsters to be more agile.[1] The cybercriminal ecosystem is increasingly industrialised and includes ways for non-technical criminals to access/use cyber tools without having technical expertise (also known as crime as a service). There are dedicated marketplaces on the dark web for selling and purchasing payment card data and online banking access. The techniques used by fraudsters/attackers are getting more sophisticated: malicious codes adapted to many banking applications could bypass current security measures (eg two-factor authentication, biometrics).[2]

Fraud risks have also evolved in response to the Covid-19 pandemic. The pandemic has accelerated changes in customers' behaviour, including the increased reliance on remote- and online-financial services. This, in turn, has further increased the scope and nature of fraud risks.

This discussion paper provides a high-level assessment of the supervisory and financial stability implications of digital fraud for the global banking system. It is structured around three broad sets of questions:

(i) What is digital fraud? What are its main defining features? How does digital fraud affect banks and how should policymakers think about it?

(ii) What are the supervisory and financial stability implications? How are supervision and financial stability affected by digital fraud? Why is digital fraud of relevance to the Committee and its mandate? What empirical data are available to assess its magnitude and prevalence?

(iii) What is being done to mitigate digital fraud risks within the banking sector? What initiatives have been pursued, or are planned, at the domestic, regional and global level?

This discussion paper is intended to provide a high-level assessment of these questions. It is not a comprehensive and exhaustive analysis of digital fraud. The empirical analysis included in this discussion paper is based on readily available data.

This discussion paper does not make a formal distinction between retail and wholesale digital fraud. While the majority of the paper is primarily focused on retail, there are also some elements that may have a connection to wholesale digital fraud. It also focuses primarily on external sources of fraud.

[1] For example, LexisNexis (2022) finds that digital fraud increased by 37% on average between 2022 and 2021 across high-growth markets in Latin America, Europe/Middle East/Africa, and Asia-Pacific.

[2] See, for example, Radford, J (2022): "6 methods hackers use to bypass two-factor authentication", Securus Communications, January.

The purpose of this paper is to elicit comments and feedback from a broad range of interested stakeholders. As described in this paper, digital fraud is by nature cross-sectoral and many initiatives to address it involve not only banks and their supervisors, but also other stakeholders such as customers of banks, government agencies, non-profit organisations, technology companies and trade associations. Digital fraud techniques also evolve and can easily spill over beyond the banking system. The Committee therefore considers it important to engage with a broad range of interested stakeholders beyond banks and bank supervisors so as to better understand the status of digital fraud as well as its mitigants.

The Committee welcomes comments from interested stakeholders – including academics, analysts, civil society, market participants, public authorities and the general public – on the different elements covered in this discussion paper by 16 February 2024. All comments may be published on the website of the Bank for International Settlements unless a respondent specifically requests confidential treatment.

Section 1: What is digital fraud? How should we think about it?

Key points:

- *Digital fraud in the context of the banking system encompasses activities that are committed remotely and/or virtually, and relies on deception to achieve its outcome. It is primarily focused on banks' customers, even though banks can play an indirect and involuntary role in facilitating fraud.*
- *For the purpose of this discussion paper digital fraud is grouped into four broad categories: (i) unauthorised retail payment transactions; (ii) manipulating bank customers to issue retail payments; (iii) fraud related to other banking products; and (iv) fraud through customers' data or banks' systems.*
- *A key question for policymakers is how best to harness the benefits of technological banking advancements while identifying, monitoring, managing and mitigating digital fraud risks with appropriately designed and implemented controls.*

Defining digital fraud

Digital fraud can take many different forms and there is no uniform definition across jurisdictions.[3] By its nature, digital fraud spans multiple dimensions (eg consumer protection, conduct, market integrity, anti-money laundering and combatting the financing of terrorism (AML/CFT), financial stability) and is therefore cross-sectoral in nature.

Consistent with the Committee's mandate the focus of this discussion paper is on digital fraud in the context of the banking system. Digital fraud shall therefore be defined as all fraudulent activities perpetrated by external parties through digital means (eg emails, websites, malicious software, etc) with the aim of stealing banking assets or credentials of bank customers. This definition does not capture digital fraud in other parts of the financial system. Digital fraud is related to, but different from, operational risk/resilience, cyber risk and/or social engineering (see Box A).

Box A: Where does digital fraud fit in with other concepts?

Digital fraud, as defined above, is related to other concepts such as operational risk, including cyber risk and social engineering, and operational resilience. There are areas of both overlap and underlap across these terms. More specifically, and using the definitions set out by the Committee and other global forums, one can view the relationship between digital fraud and the following concepts as follows:

- **Operational risk:** Defined as the risk of "loss to a bank resulting from inadequate or failed internal processes, people and systems or from external events" (BCBS, 2023a). In contrast, digital fraud is mainly focused on the losses to banks' customers, although, as noted below, this could eventually result in operational losses to banks.
- **Cyber risk: "**The combination of the probability of cyber incidents occurring and their impact" (FSB, 2023).[4] Cyber risk covers a broader set and scope of incidents that could affect a bank and/or its customers.

[3] In some cases, digital fraud is defined in the Criminal Code/Law of a jurisdiction.

[4] Cyber incident, in turn, is defined as a 'cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not'. (FSB, 2023).

- **Social engineering:** "A general term for trying to deceive people into revealing information or performing certain actions" (FSB, 2023). Some aspects of social engineering are a tool for digital fraud, while other aspects relate to deceptions that are beyond digital fraud.
- **Operational resilience:** The "ability of a bank to deliver critical operations through disruption" (BCBS, 2023b). When applied to digital fraud, operational resilience is therefore about the ability of a bank to withstand fraudulent activities affecting its customers and continue to deliver critical operations.

This definition of digital fraud can be specified to further distinguish it from broader fraudulent activities (eg cyber attack against a bank, any kind of scam of banks' customers). In particular, the following features are relevant to digital fraud:

- **Remote/virtual access:** By its nature, digital fraud is committed remotely and/or virtually. This differs from, say, internal fraud, which requires physical access by a bank employee (eg possession of IT equipment, an access badge to the internal network). As such, internal bank fraud is outside the scope of this discussion paper.
- **Deception or falsification:** Digital fraud relies on deception and/or falsification to achieve its outcome. In this sense, it relies on the inability of a bank or its customers to appropriately distinguish a fraudster from a legitimate counterparty. Digital fraud relies on the inability to verify who is at the origin of the action, due in part to the lack of appropriate authentication technology to identify the legitimacy of counterparties. This differs from financial extortion that relies on violence or coercion.
- **Customer-oriented:** Digital fraudulent activities targeting a bank's information system are limited to those areas related to its customers (eg account managing systems, card processing systems, banking applications).
- **Banks' indirect role:** Even if digital fraud is focused on banks' customers, banks can play an indirect and involuntary role in facilitating their transmission, for instance by being the payment processors of fraudulent transactions, by being targeted to access customers' data or by seeing their logo and other marketing-related visuals usurped by fraudsters.

Building on this definition and features, digital fraud can be grouped into four broad categories.

1. Digital fraud related to online payment instruments: unauthorised payment transactions

This category of activities targets bank customers' payment services (eg cards, credit transfers, direct debits, e-money). It includes unauthorised payment transactions resulting from theft or the misappropriation of a customer's payment data or access to their online banking account. Examples of such fraudulent activities include 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), and

its use by the fraudster to make payments or to sell them on hidden and obscure parts of the Internet (the "dark web"), but also Account Takeover (ATO)[5] and Automatic Transfer Systems (ATS)[6] frauds.

2. Digital fraud related to online payment instruments: manipulation of the payer to issue a payment order

Digital fraud activity under this category comprise fraudulent transactions made as a result of the payer being manipulated by the fraudster to issue a payment order or to give the payment service provider the instruction, in good faith, to a payment account it believes belongs to a legitimate payee. For example, this includes such activity conducted through social engineering techniques (eg phishing emails, text message or phone calls), impersonation of the bank (eg spoofing) or any other trusted third party.

3. Digital fraud related to bank customers' other banking products

A third category includes fraudulent activities on other banking products, for instance when customers are manipulated into investing in fake saving products or taking on fake credit products.

4. Digital fraud related to the bank through customers' data or banks' systems

A fourth category of digital fraud targets the bank itself through misuse of customers' data or banks' systems. For instance, it can be the opening of bank accounts and/or applying for credit cards using stolen identities (eg bought on the dark web) or false identities, and the use of these accounts and/or cards as a relay in money laundering circuits, to receive fraudulent transactions, use associated payment instruments or subscribe to loans, etc. It can also consist of compromising the bank's information system, obtaining the credentials of an administrative user of the mobile banking application portal and using this access to edit the mobile device number of some customers in order to bypass one-time-password authentication, increase the limits of the customer accounts and access them to conduct fraudulent funds transfers.

Harnessing the benefits of digitalisation while mitigating digital fraud risks: a simple analytical framework

An important question for policymakers is how best banks can harness the benefits of technological banking advancements while mitigating digital fraud risks with appropriate safeguards (eg increasing customer awareness, enhancing banks' cybersecurity arrangements and ability to detect, respond and mitigate digital fraud activities, etc) while being subject to robust supervisory and regulatory measures.

As illustrated in Figure 1 there is a positive relationship between the diffusion of digitalisation in banking – and its benefits – and the risk of digital fraud. At one extreme, an unconstrained "maximalist" push towards ever-more digitalisation may result in greater benefits from online banking services, but may come at the expense of material digital fraud risks (point A in Figure 1). At the other extreme, a return to a completely or mainly "analogue" banking system would, by definition, eliminate or significantly reduce

[5] ATO means the theft of a customer's bank account access codes via, for example, social engineering techniques impersonating the bank, the installation of a malicious code on the customer's computer or smartphone (due to a phishing-type social engineering scam), and/or the development of a fake banking application (rogue mobile app) that impersonates its bank. In each of the above cases, the fraudster will be able to access the customer's bank account and perform the operations they wish. This technique involves the fraudster taking manual control once the access codes have been obtained. As bank fraud prevention solutions continue to improve, ATO frauds are becoming more difficult to execute for fraudsters.

[6] ATS means the hacking of a customer's computer or smartphone with the aim of installing malicious code capable of automatically issuing fraudulent transfers from the customer's bank account/online banking application, replacing the recipient of transfers initiated by the customer without the customer's knowledge, or intercepting the validation/two-factor authentication text message. These malicious codes are targeting more and more banking applications and are adapting to technological developments and are bypassing certain anti-fraud security measures implemented by banks.

digital fraud risks (point B in Figure 1). Yet such an outcome would come at the expense of losing out on the financial stability benefits from digital banking. As such, the key question for policymakers is how best to strike the right balance within this spectrum (eg point C as an indicative example in Figure 1), and how best to reduce digital fraud risks for a given level of digitalisation (eg shifting from point C to point D) or how to further reap the benefits of digitalisation for a given level of fraud risks (eg shifting from point C to point D′ in Figure 1), which represent a range of superior outcomes. The latter may call for:

(i) better use of technology to increase the speed and effectiveness of controls;

(ii) increased awareness of bank customers about digital fraud;

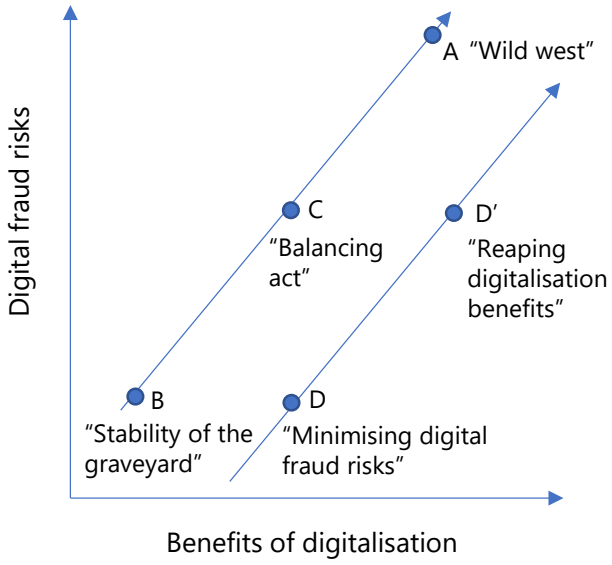
(iii) making better use of technology to enhance security of digital banking services;

(iv) making use of big data, artificial intelligence (including machine learning) etc for regtech and suptech innovations; and

(v) enhanced information and intelligence sharing among the relevant stakeholders.

Accordingly, the left arrow line in Figure 1 represents the current "state of the world". The aim of regulators/supervisors should be to shift this line to the right, so that the benefits of digitalisation can be achieved with fewer digital fraud risks. It must be noted that digital adoption is largely outside the scope of supervisory controls.

Figure 1: Benefits and fraud risks from the digitalisation of finance



Section 2: What are the supervisory and financial stability implications? What have we seen to date?

Key points:

- *There are at least two supervisory and financial stability transmission channels from digital fraud that are of relevance to the Committee's mandate: (i) financial losses to banks resulting from digital fraud; and (ii) reputation risks to banks and supervisors.*
- *Quantifying the materiality of digital fraud activity and losses is not easy due to intra- and cross-jurisdictional data challenges. These include data gaps, a lack of harmonised/comparable definitions and differences in the way in which data are collected across authorities and jurisdictions.*
- *Notwithstanding these important caveats, readily-available public data suggest that the risk of significant impacts on the stability of individual financial intermediaries, or on financial stability, from some dimensions of digital fraud seems at the moment to be limited. Out of the four categories of digital fraud discussed in Section 1, "Category 1"-type fraud (digital fraud on online payment instruments and unauthorised payment transactions) appears to be the most documented in terms of readily available empirical data across many jurisdictions). Any assessment of the materiality of the three other categories of digital fraud remains incomplete due to significant data gaps between jurisdictions and between categories of digital fraud. Nonetheless, absence or scarcity of data does not necessarily mean absence of risks.*

The previous section highlighted the customer-focused dimension of digital fraud risks as well as the trade-off between digitalisation benefits and digital fraud risks. Yet the Committee's primary focus is traditionally on the risks to banks themselves. So why may digital fraud be of relevance to the work of the Committee? There are at least two main supervisory and financial stability transmission channels from digital fraud to banks and the banking system that fall within the mandate of the Committee:

(i) financial losses to banks resulting from digital fraud, suffered by banks themselves directly (eg banks unknowingly sending funds to fraudulent counterparties) or due to the need to refund their clients (eg banks having to compensate customers for losses suffered – be it the banks' fault or not). 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.

(ii) reputational risks to banks and supervisors resulting from high-profile digital fraud incidents (eg enhanced by wide press coverage, public discontent). This could translate to a broader, system-wide loss of trust in the integrity and resilience of banks that could lead to, for example, mass bank deposit withdrawals.

An important factor in the extent to which financial losses or reputational risk could pose supervisory or financial stability concerns is whether banks are required to make payouts to customers, either through legal/regulatory requirements or through industry practices. For example, in jurisdictions where banks reimburse customers (unless customers are liable to gross negligence), the first channel may be more of a concern than the second. Even in jurisdictions where the cost of frauds fall mainly on customers or other subjects, banks may have incentives to avoid fraud and rely on other strategies to mitigate such risks. In addition, other factors, such as supervisory expectations and reputational risk, could incentivise banks to invest in the security of their systems to reduce their losses.

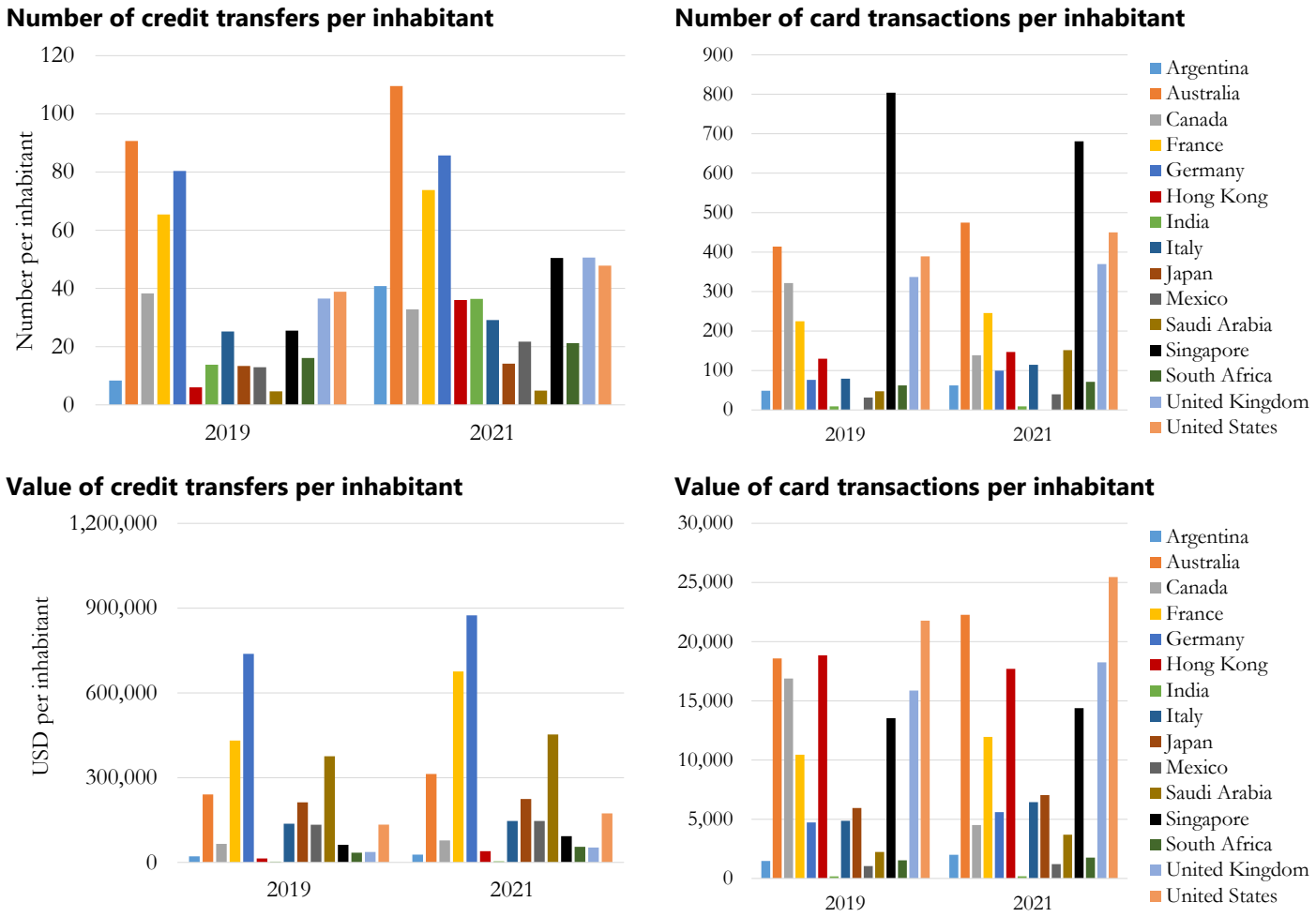
Overall, similar to the common international practice concerning payment cards and other instruments, where the issuer or the financial intermediary bears the loss, information from available jurisdictions (France, Hong Kong, India, Italy, and Japan) shows that intermediaries generally bear the loss, often with the exception of fraudulent or grossly negligent behaviour on the part of the user/client. The

difference in who bears the final cost of digital fraud across jurisdictions might reflect in part differences in practices, in addition to the law or regulation.

Both the Basel II and III standards require banks to collect data on all losses from internal and external fraud, but not specifically from the subset from digital fraud. Thus, quantifying the materiality of losses due to digital fraud is not easy, especially across jurisdictions, due to data limitations. Data challenges mainly stem from a certain degree of cross-jurisdictional heterogeneity in retail payment habits (Figure 2) and regulation, and the lack of harmonised definitions.[7] On the one hand, financial regulation has an impact on the nomenclature of payment services and on the regulatory perimeter, which affects statistical reporting and the availability of data on total and fraudulent payment transactions. On the other hand, heterogeneity in technological development and in the use of digital payments must also be taken into account when it comes to analysing digital fraud risk across jurisdictions, in order to make meaningful comparisons.

[7] Retail payment habits are measured using an indicator based on credit transfer and card transactions per inhabitant from the BIS. In some jurisdictions, the value of credit transfers may include large value or wholesale transactions.

Figure 2: Payment habits vary across jurisdictions[(a)]



Sources: BIS, HKMA and HKICL.

(a) Data on the number of card transactions per inhabitant in Japan are not available. In some jurisdictions, the value of credit transfers may include large value or wholesale transactions. Data for Hong Kong SAR covers Faster Payment System transfers, which may not include all types of credit transfers. The relative increase in the number of transactions per inhabitant in Hong Kong between 2019 and 2021 also reflects the fact that the Faster Payment System was only introduced in 2018.

The development of digital retail payment systems and the rise of e-commerce have fostered the use of digital payments and innovative online payment methods. In turn, this has increased the demand for improved security, especially on remote transactions (Hayashi, 2020; UK Finance, 2022). In the European Union (EU), retail payments digitalisation has been accompanied by regulatory interventions aimed at improving efficiency, security and transparency, including digital fraud reporting by payment service providers.[8]

In many jurisdictions outside the EU, fraud reporting by payment service providers seems to be not formally required by financial authorities as part of their statistical reporting. Retail payments security

[8] See Payment Services Directive 2 (PSD2): DIRECTIVE 2015/2366/EU (PSD2), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

is monitored using alternative data sources, including consumer surveys, information reported by financial intermediaries, or claims filed directly by consumers to a variety of institutions.[9]

To compare digital fraud risks across jurisdictions, Table 1 summarises the information on digital fraud and payments that are publicly available for each of the 15 jurisdictions surveyed, together with the main data sources.[10] National authorities often collect information concerning fraud related to online payments by cards and credit transfers, although information on the number and value of online transactions is not collected. However, for some jurisdictions such information can be retrieved from the payment system statistics computed by national central banks.

Data include the overall value of fraudulent transactions on online card and credit transfers reported by payment service providers, or alternatively the value of the economic losses due to fraud with both online payment methods reported by consumers. Data on the value of remote payments carried out with cards as well as the value of total credit transfers were also collected (total credit transfers were used, since data on the online component is only available for a few jurisdictions, as shown in Table 1). A jurisdiction-level indicator of the incidence of fraud on both types of online payment services can then be calculated as the share of the value of fraud to the value of transactions (Figure 3).

According to this indicator, fraud on online credit transfers has been trending up in some of the surveyed jurisdictions between 2017 and 2021, from a range of 0.01-0.25 basis points to a range of 0.01-0.40 basis points (Figure 3.a). This trend may be worth monitoring, considering that transactions made via online credit transfers are a large share of the total and have a very large total value (Figure 4.a). Another interesting fact emerging from Figure 3.a is that the cross-jurisdiction dispersion of the phenomenon is large; this could warrant an investigation of the determinants of this dispersion. However, a caveat is in order, since – as mentioned above – available data on credit transfers may include wholesale operations, at least for some jurisdictions.

Figure 3.b shows that over the same period fraud rates on online card-based payments have been trending down, and converging across the jurisdictions for which data are available. With the exception of South Africa, fraud rates went from a range of 13-34 basis points in 2018 to a range of 10-18 basis points in 2021. This trend seems due to the improved security of online card transactions brought about by the regulatory interventions on customer authentication.[11] Over the same period the incidence of card-based payments relative to credit transfers has been slightly increasing (Figure 4.b).

Notwithstanding the data caveats outlined above, Figure 5 shows that online banking fraud appears to be small relative to total bank assets, on average well below one basis point.[12]

With important caveats warranted by the data problems just mentioned and by the small sample of jurisdictions that could be analysed, the following tentative observations can be noted:

[9] These include antifraud government agencies like the Canadian Anti-Fraud Center in Canada, consumer protection authorities like the Federal Trade Commission in the United States (US), and industry associations like the Australian Payments Network in Australia, UK Finance in the United Kingdom (UK), and the South African Banking Risk Information Centre in South Africa. In Asian jurisdictions, fraud data is also available from financial authorities like the Hong Kong Monetary Authority, the Reserve Bank of India, and the Japanese Financial Services Agency as well as police reports and official crime statistics to monitor the retail payment security while some data may be collected in the form of fraudulent activities/modus operandi instead of payment means.

[10] For some of the countries reported in Table 1 that collect information on payment fraud (Germany, Hong Kong, India and Singapore), detailed time series data on the value of fraud on online banking services are not publicly available. Therefore, they are not included in the analysis presented here.

[11] See eg Ardizzi et al. 2020; Hayashi, 2020; Cologgi, 2023. At the same time, there is evidence of fraud-related losses borne by payment service users in many jurisdictions due to manipulation of the payer to circumvent or neutralise the use of multi-factor authentication (EBA, 2022; FCA, 2023).

[12] Data on Japan is not included in Figure 5.a, as its fraud rate on the value of online credit transfers is very low (0.003-0.014bp).

(i) The fraud phenomenon seems to have a relatively limited size in monetary terms; hence the risk of significant impacts on the stability of individual financial intermediaries, or on financial stability, seems at the moment to be limited.

(ii) Out of the four categories of digital fraud discussed in Section 1, "Category 1"-type fraud (digital fraud on online payment instruments and unauthorised payment transactions) appears to be the dimension where most readily available empirical data is available across some jurisdictions. Online credit transfers are much larger relative to card payments in terms of value (well above 90 percent of the total), and feature a smaller fraud rate (the latter result may partly reflect the presence of wholesale payments in the denominator of the rate[13]). The fraud rate of online credit transfers seems to be trending upwards in some jurisdictions in recent years, whereas the reverse holds for frauds on card payments.

Any assessment of the materiality of the three other categories of digital fraud remains incomplete due to significant data gaps between jurisdictions and between categories of digital fraud. Nonetheless, absence or scarcity of data does not necessarily mean absence of risks.

With regard to Categories 2 and 3 of digital fraud, the fact that one or more clients are tricked by fraudsters using manipulative techniques (such as stealing credit card data or making fake investments) is generally a matter of negligence and should not be a significant risk to bank soundness or financial stability. However, some instances of Category 2 may not always be attributable to gross negligence from the customer and could lead to reimbursements from banks, depending on the jurisdiction. Moreover, if the fraudsters use the bank's resources (eg its mail server, website or social media accounts) to motivate bank customers to invest in a fake banking product or to grant access to their bank account, the credulity of the customers is no longer in question since the source of this information is legitimate. In view of the credibility of such a fraud, and depending on its scale, the financial loss for the bank could in theory be significant, as well as the impact on the confidence in this bank and potentially the rest of the banking system.

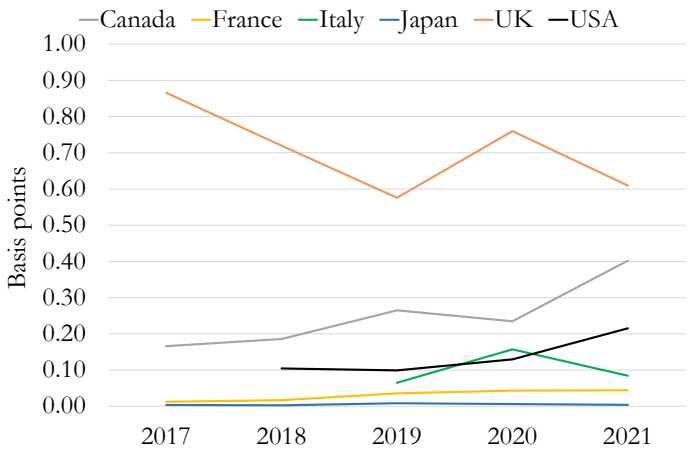
With regard to Category 4 of digital fraud, namely on the bank through customers' data or banks' systems, the existence of data is partly related to the banks' cyber incidents disclosure through compulsory or voluntary incident reporting to their supervisor or media coverage. Since there is no standardisation of cyber data collected from banks by local supervisors, it is hard to assess the supervisory and financial stability implications this category of digital fraud could have. Nevertheless, due to the fact that category 4 digital fraud may involve a compromised bank information system, it encloses additional dimensions of (cyber) risk.

Overall, the available evidence suggests that there is a room for improving data on digital fraud. With better data, authorities could improve their understanding of the phenomenon, whereas intermediaries could improve operational risk management and transparency in the financial services industry, and ultimately market discipline and consumer protection.

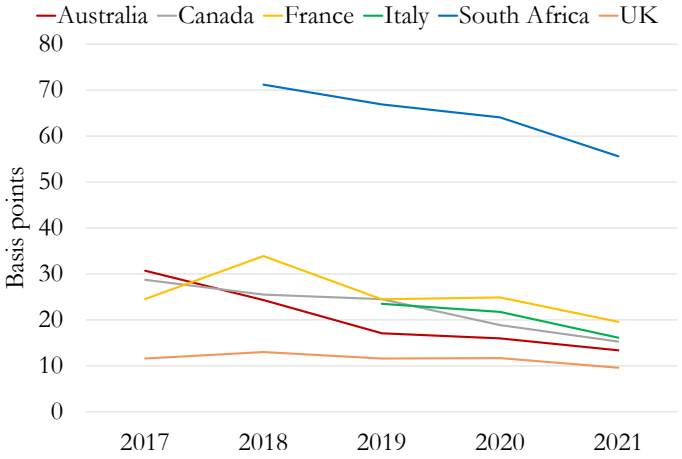
[13] For Japan, total annual value of frauds on online credit transfers (ie numerator) also includes frauds on wholesale payments.

Figure 3: Online banking fraud

(a) Fraud rate on the value of online credit transfers



(b) Fraud rate on the value of online card payments

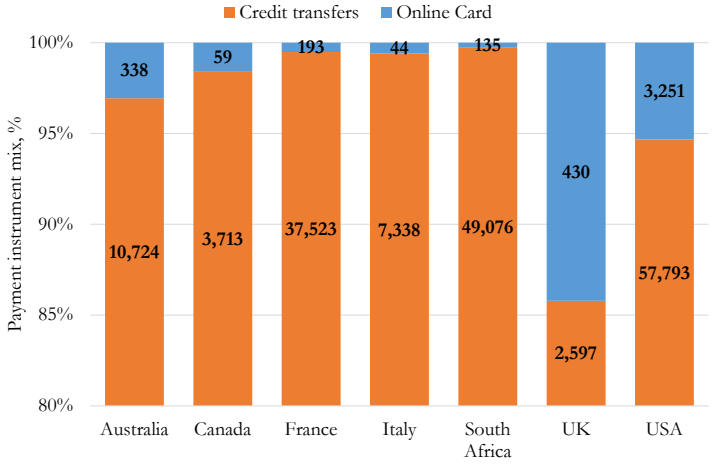


(a) Total annual value of frauds on online credit transfers divided by the total value of credit transfers. (b) Total annual value of frauds on online card payments divided by the total value of online card transactions. Source: Data on online credit transfers fraud come from the Canadian Anti-Fraud Center, Banque de France OSMP, Banca d'Italia, UK Finance, the Federal Trade Commission and the Japan Financial Services Agency. Data on the value of total credit transfers come from the BIS (for the UK we use the value of retail credit transfers processed via BACS). Data on card-not-present fraud come from Hayashi (2020), Cologgi (2023), Banque de France OSMP, Banca d'Italia, Australian Payments Network, UK Finance, the Canadian Anti-Fraud Center, the South African Banking Risk Information Center. Card-not-present (CNP) transactions are calculated based on data on total and card-present transactions from the BIS. For Canada data on CNP transactions come from Payments Canada (2022), while for the UK they are estimated based on data from UK Finance (2022), Hayashi (2020) and the BIS.

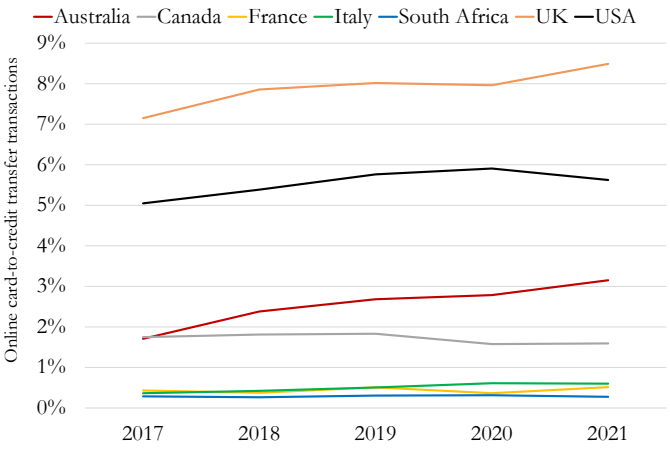
Figure 4: Relative importance of online card and total credit transfers transactions

(a) Value of payments in 2021

(percentage shares and billion of national currency)

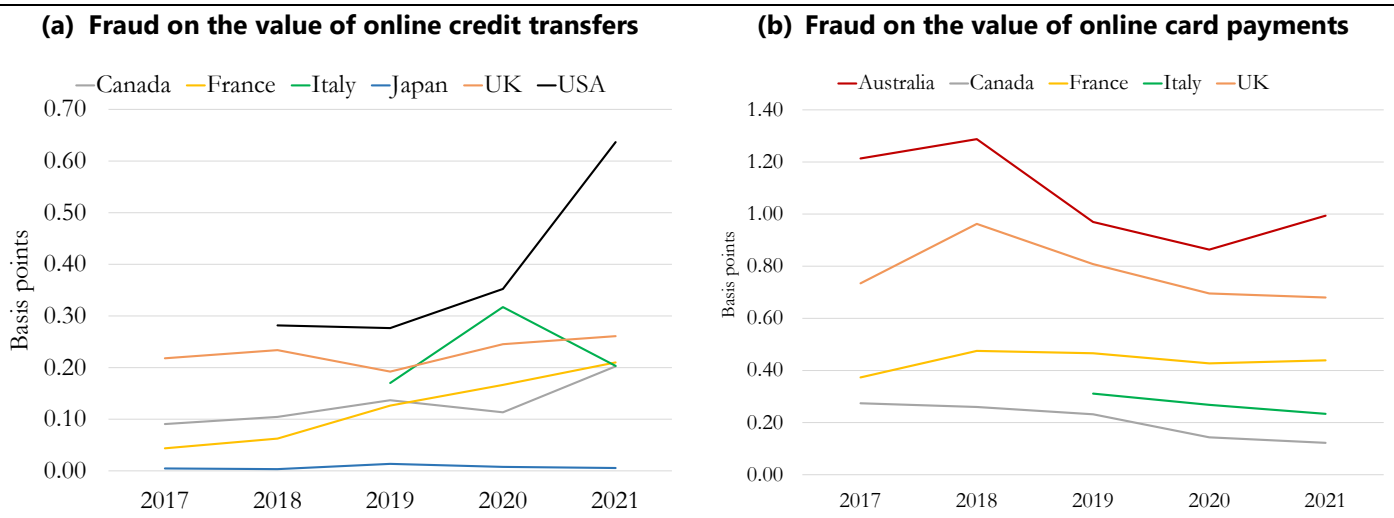


(b) Share of online cards



(a) Payment instrument mix (share of online card payments and total credit transfers). Labels (within the bars) show the value of payments made by card (online) and credit transfers (total) in 2021 expressed in billions of national currency (b) Percentage share of the value of online card payments relative to total credit transfers. Source: see notes to Figure 3.

Figure 5: Online banking fraud relative to bank assets



(a) Total annual value of frauds on online credit transfers divided by the total assets (financial and non-financial) of domestic banks. (b) Total annual value of frauds on online card payments divided by the total assets (financial and non-financial) of domestic banks. Source: data on total assets are from the BIS. For data on fraud with online banking services (cards and credit transfers) see notes to Figure 3.

Table 1: Availability of supervisory data on bank payments and fraudulent transactions

		Credit transfers	Card based payments	Other instruments	Fraud data	Online payments data publicly available	Frequency	Source
		[A]	[B]	[C]	[D]	[E]	[F]	[G]
[1]	Argentina	×	×	×	n/a	Cards	n/a	n/a
[2]	Australia	×	✓	✓	Value/Volume	Cards	Semiannual	Australian Payments Network
[3]	Canada	✓	✓	✓	Value	Cards/CT	Annual	Canadian Antifraud Center
[4]	France	✓	✓	✓	Value/Volume	Cards/CT	Semiannual	OSMP, PSD2 (EBA/ECB)
[5]	Germany	✓	✓	✓	Value/Volume	Cards	Semiannual	BaFin, PSD2 (EBA/ECB)
[6]	Hong Kong SAR	×	✓	×	Value/Volume	n/a	Annual	HKMA, HK Police
[7]	India	✓	✓	✓	Value/Volume	n/a	Monthly	RBI, CPFIR
[8]	Italy	✓	✓	✓	Value/Volume	Cards/CT	Semiannual	Bank of Italy, PSD2 (EBA/ECB)
[9]	Japan	✓	×	✓	Value/Volume	n/a	Quarterly	JFSA, BoJ
[10]	Mexico	×	×	×	n/a	Cards/CT	n/a	n/a
[11]	Saudi Arabia	✓	✓	✓	Value/Volume	n/a	Annual, Quarterly	Saudi Central Bank (SAMA)
[12]	Singapore	✓	✓	✓	Value/Volume	Cards/CT	Annual, Semiannual	Singapore Police, MAS
[13]	South Africa	✓	✓	×	Value	Cards	Annual	SABRIC
[14]	United Kingdom	✓	✓	✓	Value/Volume	Cards/CT	Annual	UK Finance
[15]	United States	✓	✓	✓	Value/Volume	Cards/CT	Annual	Fed Board, FTC

Section 3: What is being done to mitigate risks from digital fraud for banks?

Key points

- *There are a wide range of domestic and regional initiatives aimed at addressing digital fraud, often involving multiple stakeholders. These include initiatives related to: (i) raising public awareness and customer empowerment; (ii) guidance/statements regarding control measures and security protocols; (iii) supervising banks' digital fraud risk management practices; (iv) collaborating with multiple authorities to detect, respond and disrupt fraud activities; and (v) cross-border cooperation.*
- *Two relevant global initiatives that cover digital fraud to a certain extent are Financial Action Task Force (FATF)'s work on cyber-enabled fraud and the Committee on Payments and Market Infrastructures (CPMI)- International Organization of Securities Commissions (IOSCO) Principles for financial market infrastructures.*
- *While digital fraud is not explicitly defined in any existing Committee documents, it is covered by the operational risk standards, the Basel Core Principles and the Risk Management Principles for Electronic Banking.*

This section reviews current/planned initiatives related to mitigating digital fraud risks. It starts by reviewing existing Committee standards and supervisory guidelines that cover digital fraud, before summarising initiatives at the national, regional and global level.

Existing Committee standards and supervisory guidelines

While digital fraud is not explicitly defined in any existing Committee documents, it is covered in different areas of the framework. These include the following:

- **Operational risk capital requirements (Pillar 1):** Financial losses for banks that arise from digital fraud are captured by the operational risk capital standard. Under the revised Basel III operational risk framework, a bank's operational risk Pillar 1 capital requirements is the product of its business indicator component (a proxy for a bank's business volume) and a scalar, the internal loss multiplier, which accounts for a bank's average historical operational risk losses during the previous ten years.[14] Seven categories of losses are identified, including two that are usually of relevance to digital fraud (external fraud, internal fraud). In principle, Pillar 1 capital requirements for operational risk would therefore reflect a bank's losses stemming from digital fraud. In practice, however, this would depend in part on: (i) whether banks are liable to refund any digital fraud losses from customers (ie whether digital fraud exposes banks to financial losses); and (ii) whether supervisors have chosen to include banks' historical losses for the purpose of calculating operational risk capital requirements (ie they have not exercised the national discretion to set the "internal loss multiplier" at one and therefore not include historical losses).[15] Under Basel II, banks that have adopted the Advanced Measurement Approach (AMA) consider losses stemming from digital fraud when calculating their regulatory capital charge for operational risk using internal models. In some jurisdictions – such as Canada and Japan, for example – digital fraud is thus included in banks' AMA operational risk calculations. While the AMA is discontinued under the revised Basel III operational risk framework, the requirements for

[14] The revised operational risk framework is available here.

[15] Even in circumstances when the multiplier is set at one, digital fraud is also "captured" through the income streams of activities that are included in the calculation of the business indicator component of the operational risk framework.

loss data collection are expanded, requiring larger banks to record internal losses and disclose annual loss data, irrespective of the above-mentioned national discretion.

- **Supervisory review process (Pillar 2):** Under the Pillar 2 supervisory review process banks are expected to have adequate capital to support all the risks in their business and to develop and use better risk management techniques in monitoring and managing these risks.[16] Thereby, the focus is on three main areas: (i) risks considered under Pillar 1 that are not fully captured by the Pillar 1 process; (ii) factors not taken into account by the Pillar 1 process; and (iii) factors external to a bank (eg business cycle effects). To the extent that the risks associated with digital fraud (ie financial losses to banks resulting from digital fraud and reputation risks to banks) are a material risk, which are not (fully) captured by Pillar 1 capital requirements, they should be appropriately addressed under Pillar 2. All material risks faced by banks should be addressed in the bank's Internal Capital Assessment Process (ICAAP). This includes bank's management ensuring that the bank has adequate capital to support its risks beyond the minimum requirements. However, increased capital should not be viewed as the only option for addressing risks confronting the bank. Other means for addressing risk, such as strengthening risk management, applying internal limits, strengthening the level of provisions and reserves, and improving internal controls, must also be considered. In addition, supervisors evaluate how well banks manage their risks and take measures, where appropriate.
- **Principles for the sound management of operational risk (PSMOR) and the Principles for Operational Resilience (POR):** The PSMOR aim to promote the effectiveness of operational risk management through the banking system.[17] Sound risk management allows the bank to better understand and manage its risk profile, including those risks associated with digital fraud. Risk management encompasses identifying risks to the bank; measuring and assessing exposures to those risks (where possible); monitoring exposures and corresponding capital needs on an ongoing basis; taking steps to control or mitigate exposures; and reporting to senior management and the board of directors on the bank's risk exposures and capital positions. Closely linked to the PSMOR are the POR. The POR aim to strengthen banks' ability to withstand operational risk-related events that could cause significant operational failures or wide-scale disruptions in financial markets. When applied to digital fraud, operational resilience is therefore about the ability of a bank to withstand fraudulent activities affecting its customers and continue to deliver critical operations. An effective operational risk management system and a robust level of operational resilience work together to reduce the frequency and the impact of operational risk events.
- **Basel Core Principles (BCPs):** Under the BCPs, supervisors should determine that banks have adequate policies and processes to prevent the bank from being used, intentionally or unintentionally, for criminal activities. [18] This includes the prevention and detection of criminal activity, and reporting of such suspected activities to the appropriate authorities (Principle 29). In addition, supervisors should determine that banks have adequate internal control frameworks to establish and maintain a properly controlled operating environment for the conduct of their business taking into account their risk profile, including measures for prevention and early detection and reporting of misuse such as fraud, embezzlement, unauthorised trading and computer intrusion (Principle 26).
- **Risk management principles for electronic banking:** In 2003 the Committee published the Risk Management Principles for Electronic Banking to help banks expand their existing risk oversight

[16] The supervisory review process framework is available here.

[17] The Principles are available here.

[18] The current BCPs are available here.

policies and processes to cover their e-banking activities.[19] Among the fourteen Principles there are three that are also of relevance for digital fraud. More specifically, banks should take appropriate measures to authenticate the identity and authorisation of customers with whom they conduct business over the internet. Failure on the part of the bank to adequately authenticate customers could result in unauthorised individuals gaining access to electronic banking (e-banking) accounts and ultimately financial loss and reputational damage to the bank through fraud, disclosure of confidential information or inadvertent involvement in criminal activity (Principle 4). Furthermore, banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications to reduce the risk of fraud in operational processes and systems (Principle 6). Finally, banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information. The inherent nature of straight-through processes for e-banking may make programming errors or fraudulent activities more difficult to detect at an early stage (Principle 8).

Domestic and regional initiatives

Most Committee member jurisdictions have launched initiatives aimed at addressing digital fraud, often involving multiple stakeholders, including various government departments, law enforcement agencies, market practitioners and regulators of financial, telecommunication and technology sectors as well as members of the public. These initiatives fall broadly into five categories summarised below with selected examples; this section is not intended to be a comprehensive or exhaustive analysis of all relevant initiatives underway by all member jurisdictions. Some of these initiatives form part of overall strategies to tackle an issue spanning multiple government agencies.

(i) Public awareness and empowerment

Consumer and employee education remains one of the most important prevention tools and educated consumers are the first line of defence. Customers using payment and other banking services may be victimised by criminals seeking to commit fraud through digital means, such as social engineering techniques used to obtain personal/account information or deceive victims into transferring funds or authorising payments. Increasingly, these involve real-time payments in which the victim cannot cancel or withdraw the transaction. Many jurisdictions issue warnings or advisories and undertake education campaigns to increase consumer awareness of risks and emerging fraud techniques, and encourage consumers to protect personal information such as credit card details and passwords.

Initiatives often take the form of collaborations among multiple bodies, including from the public and private sector. Many are undertaken by financial authorities[20] while some are pursued in collaboration with law enforcement and other government agencies and private sector bodies.[21] In other cases, initiatives are undertaken by banks and/or by authorities in cooperation with banks and industry associations.[22] While such initiatives are often long-standing, many have been expanded, or new ones introduced, since the onset of the Covid-19 pandemic, particularly with regard to the protection of payment credentials alongside deployment of strengthened authentication measures. Different channels

[19] The Principles are available here.

[20] For example, the Bank of France and ACPR in France, and BaFin in Germany, the Bank of Italy in Italy.

[21] For example, the JFSA, National Police Agency, other government agencies and trade associations in Japan; MAS, Ministry of Home Affairs, Police, other government agencies and industry associations in Singapore

[22] For example, in Canada (by banks), HKMA with banks in Hong Kong SAR, JFSA with Japan Bankers Association in Japan.

are used to deliver these messages, with some initiatives providing consumer helplines.[23] In addition to raising customers' awareness of fraud, some initiatives also focus on raising awareness among bank staff of the need to protect customers' assets by identifying and reporting fraud.[24]

Several initiatives also seek to empower customers, for example by providing them with tools to notify their banks when using different channels, such as mobile applications or web pages or exploring possible flexibility for credit card holders to opt-in or set sub-limits for higher risk situations such as card-not-present transactions.[25]

(ii) Requirements and guidelines with regard to control measures and security protocols

Most regulatory/supervisory authorities issue guidance or policy statements to banks setting out expectations and requirements regarding controls for payments. These may include requiring security protocols such as multi-factor authentication and response to digital fraud. Guidance may be issued at supranational (eg EU Payment Services Directive 2 (PSD2)) or jurisdictional level, and often also covers harmonised security measures for banks, non-bank payment service operators and e-money institutions.[26] Guidance generally covers the need for adequate controls and fraud risk-management frameworks, including preventive measures such as transaction limits and authentication controls, real-time monitoring of transactions for unauthorised activity, detective measures such as fraud surveillance, and corrective controls such as emergency kill switches.

Many jurisdictions emphasise technological and data aspects of payment security. This generally includes requirements on information/data security and transaction monitoring and may also include requirements to report data on payment fraud for analysis of trends and patterns to support supervisory actions.[27] In some jurisdictions there is also a focus on the resilience of the network and information systems of the broader financial sector, including the reporting of major Information and communication technology (ICT) related incidents[28]. Some jurisdictions also promote the use of recognised digital identification systems for customer due diligence in legislation and supervisory guidance.[29] Another area where technology may support efforts to combat digital fraud is the use of digital IDs and digital signatures. Digital fraud often involves the creation or modification of messages to make them appear to come from persons who control accounts or other persons entitled to make payments. Some jurisdictions that have introduced legal frameworks supporting digital ID and digital signatures are exploring their use to make payments more secure.[30]

(iii) Supervision of banks' digital fraud risk management practices

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

Fraud (including digital fraud) may fall under different parts of authorities' supervisory regimes, such as operational risk, technology risk (including cyber-security), money laundering and terrorist

[23] For example, in India and the UK.

[24] For example, in South Africa, Hong Kong SAR and Japan.

[25] For example, in Mexico and Hong Kong SAR.

[26] For example, EU PSD2, HKMA, MAS and the Saudi Central Bank.

[27] For example, the EU, Japan and Saudi Arabia.

[28] For example, EU DORA (Digital Operational Resilience Act).

[29] For example, Hong Kong SAR and Saudi Arabia.

[30] For example, Mexico.

financing (ML/TF) risk (eg the risk of mule accounts used to launder proceeds of fraud), reputation risk or conduct risk.

Some supervisory authorities have increased collection and analysis of data to understand evolving fraud risks and prioritise high-risk areas including money mule networks or use techniques such as phishing simulation and cyber reconnaissance to assess the cyber-security of regulated entities to address cyber-crime/digital fraud risks.[31] Others promote measures to strengthen security of e-banking and online credit card transactions, such as tokenisation of credit card data and allowing customers to set sub-limits for higher risk credit card transactions.[32]

Supervisory authorities also promote the use of advanced techniques by banks. These include the deployment of graph analytics in retail banks to support bespoke thematic intelligence capabilities to strengthen the response to fraud, and organising forums for banks to work with data experts to explore the use of tools such as network analytics to identify mule account networks often used in fraud.[33] Many supervisory authorities have issued updated fraud risk-management principles or guidelines which take into account increased technology and cyber risks and growing use of cloud technologies, application programming interfaces and rapid software development.[34]

(iv) Collaboration among stakeholders for an ecosystem response

Some jurisdictions adopt collaborative and structured methods for monitoring and handling of transactions affected by digital fraud to improve detection, response and disruption of often rapid fund flows. These include an ecosystem approach, regulatory reporting, common data repositories and facilitating information sharing among financial and other authorities and banks. Specific measures may include mandating harmonised security measures among banks, payment and e-money institutions and requiring regular reporting of information on fraud.[35]

Information sharing on fraud or related money mules has been increasing among authorities and banks and the public under an eco-system approach.[36] Other initiatives involve collaboration with the banking sector on prompt bank-to-bank sharing of financial crime information and multi-agency task-force approaches to anti-fraud work.[37] Several jurisdictions have also introduced or are exploring facilities, such as mobile apps, that allow the public to check information, such as bank account and telephone numbers, against a database of information previously linked to scams or help to block fraudulent calls, detect fraudulent SMS and facilitate reporting of scams.[38]

Many jurisdictions adopt collaboration among regulatory authorities, law enforcement, government and non-profit bodies and different industry sectors (eg telcos). Together, they aim to adapt controls in response to changes in fraudster tactics and protect customers by blocking scam calls, text messages or websites; or providing the tools and / or data to customers to identify genuine transactions from scams (eg white list approach).[39] Cooperation and collaboration with the payment industry is also an

[31] For example, the HKMA and the RBI.

[32] For example, the HKMA.

[33] For example, the HKMA.

[34] For example, the MAS, JFSA and HKMA.

[35] For example, the EU, JFSA and RBI.

[36] For example, the National Economic Crime Centre in UK, Fraud and Money Laundering Intelligence Taskforce in Hong Kong SAR, Bank of Italy and National Cyber Security Agency in Italy, and the Joint Operations Centre in Saudi Arabia.

[37] For example, the HKMA, Hong Kong Police and Hong Kong Association of Banks in Hong Kong, National Police Agency and Financials ISAC Japan in Japan.

[38] For example, Hong Kong SAR and Singapore.

[39] For example, Canada, Singapore, Japan, and Hong Kong SAR.

important aspect of many jurisdictions' responses, as awareness has grown of the need to "design out" fraud at source and engage sectors which create vulnerabilities.[40]

(v) Cross-border cooperation

Digital fraud, being largely internet-based, has a clear international element. There are many well-documented cases of digital fraud, and related laundering of proceeds, occurring across borders, indicating that there is therefore a role for international cooperation to play in addressing the problem.[41]

There are existing channels for cooperation among law enforcement agencies through Mutual Legal Assistance requests for individual cases. More general information, for example on money laundering typologies, related to fraud is shared through the FATF and its network of regional bodies. There are also bilateral channels for sharing relevant information under memoranda of understanding (MOU) between financial regulators and other authorities.

Sharing of customer information among banks and other financial institutions in cases involving, or suspected to involve, digital fraud is often constrained by legal barriers such as those related to data privacy. Some jurisdictions have introduced, or are considering, provisions allowing banks and other financial institutions to share information in cases where there is reason to suspect crime. However, to date, most of these appear to be limited to domestic sharing.

Global initiatives

There are two sets of global initiatives by other global standard setters and forums related to digital fraud (directly or indirectly) that may be of relevance to banks and bank supervisors.

FATF work on cyber-enabled fraud

The FATF is undertaking a project, due to conclude in 2023, focusing on transnational financial flows and ML/TF related to cyber-enabled fraud, building on the work and expertise of the Egmont Group of Financial Intelligence Units and INTERPOL (FATF, 2023). There will be a public report on ML/TF risks and trends of cyber-enabled fraud, risk indicators, the impact and vulnerabilities of digitalisation and new technologies, the role of data analytics, digital tools and industry and public-private partnerships in combating financial flows linked to cyber-enabled fraud, and challenges and best practices. While the project is primarily law enforcement focused, some areas including the identification of strategies and partnerships for disruption and response, and improving domestic and international information sharing, may be relevant to the work of the Committee.

CPMI-IOSCO Principles for financial market infrastructures

The Principles for financial market infrastructures (FMI)[42] require FMIs to have "robust management and control systems to identify, monitor and manage general business risk" including fraud. The Principles require FMIs to have "appropriate human resources and risk-management policies to address fraud prevention". Entities holding securities in custody are also required to apply safekeeping procedures that "fully protect" customers' securities, including from fraud.

[40] For example, the Observatory for the Security of Payment Means in France.

[41] See, for example, PaymentsJournal (2023).

[42] The Principles are available here.

Feedback on the discussion paper

The purpose of this paper is to elicit comments and feedback from a broad range of interested stakeholders. The Committee welcomes comments from interested stakeholders – including academics, analysts, civil society, market participants, public authorities and the general public – on the different elements covered in this discussion paper by 16 February 2024. The Committee particularly welcomes feedback on the following questions:

Q1. Do you agree with the features and categories of digital fraud? Are there additional financial stability and/or prudential transmission channels from digital fraud to the banking system?

Q2. What other data sources could the Committee consider when assessing the risks of digital fraud?

Q3 Are there any additional, banking-specific, initiatives on digital fraud that could be pursued by the Committee?

References

Radford, A (2022): "6 Methods Hackers Use to Bypass Two-Factor Authentication" https://securuscomms.co.uk/how-hackers-bypass-two-factor-authentication/.

Ardizzi, G., E Bonifacio and L Painelli (2020): "Payment card fraud: global trends and empirical evidence on online fraud in Italy", Bank of Italy, Occasional Papers, n. 562 (in Italian).

Australian Payments Network: https://www.auspaynet.com.au/resources/fraud-statistics

Basel Committee on Banking Supervision (2023a): "Revisions to the principles for the sound management of operational risk", March.

——— (2023b): "Principles for operational resilience", March.

Banque de France, Observatory for the Security of Payment Means (2021): "Annual Report 2021 – Statistical Appendix".

BIS, payments and financial market infrastructure statistics https://www.bis.org/statistics/payment_stats/commentary2301.htm

Canadian Anti-Fraud Center: https://www.antifraudcentre-centreantifraude.ca/index-eng.htm.

Cologgi, M (2023): "The impact of regulation on retail payments security: evidence from Italian supervisory data", Finance Research Letters, Volume 54, June 2023, 103799.

European Banking Authority (2022): "Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry".

Financial Action Task Force (2023): "FATF-INTERPOL Partnership: Igniting global change to take the profit out of crime", September.

Federal Trade Commission Consumer Sentinel Network: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

Feedzai (2022): "The RiskOps Age: Q2 2022 Financial Crime Report" https://feedzai.com/blog/q2-2022-financial-crime-report-the-riskops-age/#:~:text=Over%205%20million%20cards%20were,engineering%20attacks%20in%2010%20days.

Financial Conduct Authority (2023): "Unauthorised payments from your account". https://www.fca.org.uk/consumers/unauthorised-payments-account.

Financial Stability Board (2023): "Cyber Lexicon", April.

Hayashi, F (2020): "Remote Card Payment Fraud: Trends and Measures Taken in Australia, France, and the United Kingdom", Federal Reserve Bank of Kansas City, Payments System Research Briefing.

Hong Kong Monetary Authority and Hong Kong Police press releases: https://www.info.gov.hk/gia/general/202212/07/P2022120600325p.htm.

Japan Financial Services Agency (2020): Survey on payment fraud, https://www.fsa.go.jp/news/r2/ginkou/20201225.html.

LexisNexis (2022): "Digital payment fraud in high-growth markets", October.

Payments Canada (2022): Canadian Payment Methods and Trends Report 2022.

PaymentsJournal (2023): Cross-border payments: fighting e-commerce fraud using data, March

Payment Systems Directive 2 (2015): Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

South African Banking Risk Information Center: Annual Crime Statistics 2019 and 2021.

Singapore Police: Annual crime statistics https://www.police.gov.sg/media-room/statistics

UK Finance (2022): Annual fraud report 2021.

Saudi Central Bank Counter fraud framework: https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Counter_Fraud_Framework.pdf.