INSTITUTE OF INTERNATIONAL FINANCE

February 16, 2024

Pablo Hernández de Cos, Chairman
Basel Committee on Banking Supervision
Centralbahnplatz 2
4051 Basel, Switzerland

RE: Basel Committee on Banking Supervision Consultative Paper "Digital fraud and banking: supervisory and financial stability implications"

Dear Mr. Hernández de Cos:

The Institute of International Finance ("IIF")[1] welcomes the opportunity to comment on the Basel Committee on Banking Supervision ("BCBS" or "the Committee") Consultative Paper "Digital fraud and banking: supervisory and financial stability implications."[2]

We commend the BCBS for undertaking work on the important subject of digital fraud which, as underscored in the discussion paper, is being committed at a greater scale and scope than ever before.[3] This is in large part due to the rapid advancement of digitalization and new technologies which provide both benefits and risks to financial institutions and the provision of financial products and services more broadly. At the same time, digital fraud should be seen as fraud enabled by digital means, rather than as a wholly new phenomenon.

While digital fraud is overall an extensive category of activities, we understand and support the Committee's decision to focus primarily in this discussion paper on retail (as opposed to wholesale) and external fraudsters (as opposed to employee fraud.) Retail clients and households are the most vulnerable, and most likely to be taken advantage of by fraudsters using the latest technologies, as they are likely to be less able to manage their security than larger organizations and businesses. Small- and medium-sized enterprises are also relatively vulnerable, however, and thus should most likely receive more emphasis in the discussion paper analysis going forward.

For all these reasons, it is important that banks work closely together with law enforcement agencies, government authorities, regulators, and cross-sectoral partners, especially telecommunications firms, to help make customers and individuals aware of how to detect and

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks, and development banks.

[2] Basel Committee on Banking Supervision 2023. Digital fraud and banking: supervisory and financial stability implications November 2023

[3] This article for example finds that payment fraud in the US grew by 73% over 2023.

protect themselves against digital fraud. It is also important not to view these issues in isolation or strictly through the prism of prudential policy. Fraud is a multifaceted, global problem which requires an integrated approach to solutions throughout its lifecycle. This should critically include prioritizing the prevention of fraud whilst also improving efforts to deprive criminals of their illicit resources through more effective asset recovery measures. The BCBS should be aligned in this work across the international standard setting bodies, and in particular with the Financial Action Task Force (FATF) and the Committee on Payments and Market Infrastructures (CPMI).

Before responding directly to the three broad sets of questions posed in the discussion paper, we would first like to draw your attention to a number of over-arching considerations on the development of digital fraud and also scams in the banking sector, and the financial services sector more broadly.

1. *Fraud is a complex, cross-sectoral phenomenon, and the chain of fraud comprises many other relevant stakeholders.*

Fraud is a complex phenomenon. It is a chain that involves actors from different sectors. There needs to be a clear distinction between unauthorized transactions and authorized transactions (scams) within the industry. Subsequently any liability structure that may be considered by the BCBS or other international standard setters should be with these separate definitions in mind.

Typically, app scams take place in a different context prior to their final stage in the financial domain when the payment is ordered, where payment services are provided in strict compliance with regulation. As such, app scams are different than unauthorized digital fraud.

The chain of fraud comprises many other stakeholders beyond banks, especially telecommunications and internet technology firms, which both customers and fraudsters overwhelmingly use to access and undertake financial services.

According to the UK Finance 2023 Half Year Annual Fraud Report, for example, 77% of the volume of fraud, accounting for 32% of total losses, originated from online sources, which includes lower-value scams such as purchase fraud.[4] Another 17% of fraud incidents, representing 45% by overall losses, was conducted through telecommunications, which includes impersonation. This on average results in larger value fraud. (In the UK Finance Report, authorized fraud, including scams, are part of digital fraud.)

Although fraud ultimately impacts the accounts of the victims, it originates on their telephones, tablets, or computers, through social media, online dating platforms, search engines, or apps. Payments fraud affects banks, but also other types of payment service providers ("PSP"). In order to address and mitigate fraud more effectively, we support the development holistic approaches which include greater cross-sector, cross-border, and public-private cooperation in order to work together to thwart fraudulent activity well before bank and other payment accounts are impacted.

For all these reasons, it is important that banks are enabled to work closely together with law enforcement agencies, government authorities, regulators, and cross-sectoral partners, including

[4] UK Finance 2023. 2023 Half Year Annual Fraud Report. Oct. 24, 2023.

telecommunications firms and social media platforms, to help make customers and individuals aware of how to detect and protect themselves against digital fraud.

2. The fight against digital fraud and scams requires coordinated cross-sectoral effort.

Given that fraud and scams almost always originate outside the banking system, we support a more targeted approach to studying the issue. With so many victims being taken advantage of through text messages, phone calls, emails, and social media platforms, it is important that the other actors involved are required to play a much more active role in preventing and minimizing fraud and scams. Without such action, the many efforts the banking sector is undertaking to reduce or prevent and detect fraud and scams, both in its clients' interests and arising from compliance with financial crime and terrorist financing monitoring obligations, lack fundamental enablers.

As one corollary, while bank regulators and supervisors may not have direct oversight over telecommunications, IT, technology, and social media firms, they need to coordinate much more closely with regulators or authorities in those sectors to reduce the volume of frauds and deceptive messages, including impersonations of financial institutions, governments, and utilities. As an example, those firms could alert authorities when there is detectable uptick in direct messages targeting older users.

While the IIF does not want to endorse a specific approach, there are many examples of voluntary efforts already being developed in different countries around the world to reduce the incidence and severity of scams and fraud. For example,

- In the UK, for example, the Fraud Sector Charter is a noncompulsory commitment from telecommunications providers to reduce fraud.[5] Another welcome initiative is Stop Scams UK, which is an industry-led collaboration of responsible businesses from across the banking, telecoms and technology sectors who have come together to help stop scams at source. It was created to enable and facilitate the development of technical solutions that will help prevent the harm and loss caused by scams, and to work closely with the UK authorities, including Ofcom and the Financial Conduct Authority.[6]

- In Australia there are similar initiatives, including the establishment of a national Anti-Scam Centre to share intelligence on scam trends and coordinate action to combat specific types of scams, changes to the Australian Banking Association's (ABA) Banking Code of Practice, a Scam-Safe Accord that envisages a new confirmation of payee system and enhances sharing of information on scams between banks. The Australian Treasury recently consulted on mandatory industry codes to stop scams.[7] There are separate initiatives by major digital platforms (e.g. the Digital Industry Group's Scams Action Plan) and the media regulator ACMA to combat scams. In Spain, banks and telecoms providers

[5] More information can be found here: https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter
[6] Please see https://stopscamsuk.org.uk/about-stop-scams-uk for more information
[7] See Australian Treasury Scams – mandatory industry codes

are likewise working together to develop a plan to stop the rise of digital fraud through phone scams.[8]

In the case of scams, we believe that the best protection would be to ensure that consumers won't be targeted again by scammers. If we want to stop scams, it is necessary to adopt a more balanced legal regime and a cross-sectoral focus on systems and controls to tackle scam prevention in a pro-active manner.

There is a cost to fraud and scams and the responsibility, and the liability framework are important topics that are best placed to be discussed with the wider industry and global standard setters in terms of approaches and models that could work well and help reduce moral hazard. This could include reviewing existing practices and considering where these could be improved further.

3. *Liability should be more appropriately distributed and should consider all parties involved in the chain*

While banking supervisors are not (generally) directly responsible for policy settings around liability for fraud and scams, they are important players in policy discussions at a time when governments are seeking answers to this growing problem. As such, we support Basel Committee members working closely with other global standard-setters and relevant national authorities to address the issue of distributing liability, depending on the kind of transaction and the parties involved.

In many jurisdictions, the liability for losses occasioned by APP scams rests with the consumer, unless the bank has been negligent or acted in bad faith.[9] However we are seeing some jurisdictions move away from this model by shifting full or partial liability for consumer losses on banks. In Singapore regulators are already considering a proposed shared responsibility framework where both firms and customers take on part of the responsibility for phishing scams[10], while in the UK the Payment System Regulator has recently confirmed a mandatory full reimbursement regime for APP fraud resulting in payments in faster payments and CHAPS will come into effect in 2024.[11] The paying and sending PSP will be required to share the cost equally, except where the customer has acted fraudulently, or with gross negligence. There is a high cap on liability of GBP 415,000. Proving that a customer acted fraudulently might also require a complex burden of proof.

The IIF is not supportive of moves to shift liability from consumers to banks, in the case of scams including APP scams.

Consumers should be incentivized to remain vigilant about fraud and scams, and to educate themselves on the means by which fraudsters and scammers operate. Because of the increases in retail digital fraud and scams, it is important to also promote and incentivize responsible

[8] More on the plans can be found here: https://intereconomia.com/noticia/finanzas/la-banca-y-las-telecos-negocian-un-plan-para-frenar-las-estafas-telefonicas-20240115-1702/

[9] See, for example at the UK Supreme Court: Philipp (Respondent) v Barclays Bank UK PLC (Appellant)

[10] Monetary Authority of Singapore 2023. "Consultation Paper on Proposed Shared Responsibility Framework" Oct. 25, 2023

[11] Farrer & Co. 2024 Authorised push payment fraud and mandatory reimbursement January 2, 2024.

behaviors among customers when it comes to their online identities, security, and financial accounts.

A lack of accountability for consumers, where they are reimbursed for transactions – particularly where they authorized the transaction themselves as in the case of scams – is likely to make customers less vigilant and perhaps even careless in some cases, given they know they will be reimbursed. This has the potential to create significant moral hazard.

Such a situation would also incentivize fraudsters and scammers to continue and increase their fraud and scam attempts, knowing that their rates of success could increase with retail customers, who are relying on the banking sector (or other sectors) to compensate them for any fraud from which they may become a victim.

In addition, any liability framework for digital fraud and scams should consider all parties involved in the chain of transactions, not just banks.

A liability regime placing significant burdens on the banking sector could also strongly encourage "first person" fraud, where consumers conspire with third parties in account takeovers and the like. In this case the third party might share some of its profits with the consumer in exchange for participating in this scheme. Any such conspiracy would be very hard to detect, absent a full investigation including forensic analysis of a consumer's devices.

4. Recognizing that "Digital Fraud" can occur across borders.

As acknowledged, fraud and scams are are an issue of growing significance and is ultimately linked to a criminal enterprise with increasing complexity and reach. In some cases, fraud and scams can be of a global nature as well. Recognition of this issue has evolved in discussions at the FATF, with the focus on the lifecycle of financial crime being a critical component to success in building a consistent and holistic cross-border anti-financial crime framework.

The work that the FATF is undertaking around "cyber enabled fraud" ("CEF"), and in particular the publication of the 2023 FATF/Interpol/Egmont Group report on illicit financial flows from CEF[12] is both important and relevant to the digital fraud work of the Basel Committee, and also the cybersecurity focus of the Financial Stability Board ("FSB") and other standard-setters. Given the overlap of so many of these concepts, it is important that the Basel Committee and other standard-setters seek to be consistent in their terminology in order to avoid creating additional fragmentation and possible divergences around concepts, terminologies, and taxonomies.

5. The importance of relevant public-private information sharing and coordination.

As noted by the FATF and discussed in the Committee's consultation document, information sharing between relevant stakeholders on a domestic and cross-border basis in relation to fraud can enable more effective outcomes. At the same time, enhancing coordination across the public and private sectors will significantly assist in tackling these complex, multijurisdictional issues.

[12] FATF Interpol Egmont Group 2023. Illicit Financial Flows from Cyber-Enabled Fraud November 2023

Information sharing should be enabled through public/private coordination mechanisms that bring together stakeholders to tackle fraud and the laundering of related proceeds. Coordination across Financial Intelligence Units ("FIU"), law enforcement, regulators, cybercrime experts and financial crime risk management professionals - alongside a wider set of ecosystem stakeholders including social media platforms, telecoms, and internet service providers – should be encouraged. Leveraging and enhancing existing financial crime public/private partnerships ("PPP") in various jurisdictions should also be prioritized in relation to fraud.

For example, the Europol Financial Intelligence Public Private Partnership ("EFIPPP"), which was created in 2017 as a partnership between Europol and the IIF and has become the first multilateral PPP, has an established Threats and Typologies Working Group dedicated to sharing strategic information on topics related to CEF and investment fraud, mule accounts, and virtual IBANs.[13] Such cooperation across countries and collaboration with domestic information sharing mechanisms is highly useful in identifying and dismantling cross-border fraud schemes and concomitant financial crime networks. The Australian Scam-Safe Accord mentioned above also includes a major expansion of intelligence sharing across the sector with all banks acting on scams intelligence from the Australian Financial Crimes Exchange by mid-2024 and joining the Fraud Reporting Exchange.[14]

However, in order to make such data exchange and coordination/cooperation truly effective, fundamental work remains to be done on enabling and/or clarifying legal gateways for operational as well as strategic information sharing and addressing the negative consequences of data localization. We recommend the BCBS work with international standard setters and industry to discuss these obstacles and best approaches.

6. Closer collaboration and coordination between jurisdictions, and with standard-setters.

Supporting multilateral/international/jurisdictional collaboration and strengthening the detection and prevention of fraud is key. It is important that governments and FIUs continue to commit sufficient resources (human and technological), to the collective analysis of Suspicious Activity Reports and Suspicious Transaction Reports (SARs/STRs), with a specific focus on enhancing the speed, volume, and quality of feedback on threats and typologies provided to suspicious activity reporters, *i.e.*, financial institutions. Enhanced and timely feedback should be specific, focused, and actionable. For example, identifying common payment patterns of concern that are identified by multiple reporters to help the reporting sector refine the focus of its compliance controls will help the system as a whole prevent, detect, and respond to fraud activity more efficiently and effectively.

It is also vital to enhance the collective ability to track and trace assets globally in an expeditious manner. In addition to cooperation through PPPs (as noted above), jurisdictions should work together to intercept fraud proceeds and improve asset recovery rates. The FATF is already considering recommendations aimed at strengthening collaboration with the Asset Recovery

[13] Please see Europol Financial Intelligence Public Private Partnership for more information

[14] Australian Banking Association 2023. Australian banks have joined forces to launch a new Scam-Safe Accord to deliver a higher standard of protection for customers and put scammers out of business in Australia Nov. 24, 2023

Networks ("ARINs") and encouraging cross-border collaboration through the FATF-INTERPOL Roundtable Engagements ("FIRE")[15].

Collaboration via multilateral mechanisms such as these - and others through the Egmont Group, Europol, and Interpol - will allow jurisdictions to collectively address fraud and related criminal issues. However, consideration could also be given, for instance, to exploration of how current processes to request information and flag risk may be automated to help jurisdictions collaborate at pace to trace the proceeds of crime cross-border. Existing data flows, including cross-border payments' messaging services and correspondent wires, could be important enablers in this context, potentially helping to track the movement of a criminal asset through multiple steps to the point where it has come to rest and could be frozen far more quicky than is currently possible.

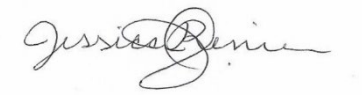
7. Developing guidance around all aspects of fraud.

As there is consensus that tackling fraud and scams at a global level is important, guidance or sound practices which build expectations around all aspects of the fight against fraud discussed herein could be considered. Such an effort would be ambitious but would ultimately help raise and standardize the response globally, creating a more hostile environment for criminals and preventing the risk of regulatory arbitrage where one country pushes further and faster than others.

Ultimately, there also needs to be increased focus on fraud and scam prevention. As recommended by the FATF and others, jurisdictions should promote awareness and vigilance against fraud and scams through public education and financial/cyber literacy. Collaboration with the private sector on prevention strategies is also an important area that will build capacity in the system by developing a more coherent front-end response to fraud and scam deterrence.

Thank you for your consideration of these points. In the Appendix below, we provide more details on the three broad questions posed in the discussion paper. We hope that you will find our comments useful and constructive. If you have any questions or would like to discuss our comments in greater detail, please do not hesitate to contact the undersigned, as well as Martin Boer at mboer@iif.com, Matthew Ekberg at mekberg@iif.com, Gloria Sanchez Soriano at gsanchezsoriano@iif.com or Laurence White at lwhite-advisor@iif.com.

Yours sincerely,



Andrés Portilla
Managing Director
Regulatory Affairs

Jessica Renier
Managing Director
Digital Finance

[15] FATF 2023. Outcomes FATF Plenary Oct. 25-27, 2023

APPENDIX: IIF Responses to the BCBS Discussion Paper on Digital Fraud and Banking

Question 1:

Do you agree with the features and categories of digital fraud?

Given that in most countries banking products and services are rapidly moving into the digital space, we are seeing more instances of digital fraud and scams. We see value in focusing specifically on retail customers, and on external fraud, as this paper does, as there is an important consumer safety, and consumer protection element here. Institutional investors are also more likely to be better resourced and protected against fraud and scams than those in the retail space. As such, we believe consumer education is a big part of the solution, by FI's, telcos, social media platforms, and law enforcement. Information exchange, cross-sectoral, public-private, across borders, is also very helpful in identifying and scam fraud patterns, adversaries, and methods.

When defining "digital fraud" it is important that the Basel Committee coordinate closely with the FSB, CPMI, and other global standard-setters for consistency.

Generally, the categories of digital fraud appear to align with discussions we have read and contributed to. That said, if the proposal of four broad categories comes from any international organization, it would be beneficial to cite the source.

A category of fraud which is of growing importance, and which is not mentioned in the BCBS paper is so-called "friendly fraud" or "first-person fraud". This can include where a cardholder tries to fraudulently charge-back. Any consumer reimbursement schemes connected with APP losses can be expected to experience significant levels of this type of fraud.

We agree with Categories 1, 2 and 3. Scams should be in a separate category to underline its fundamental difference with non-authorized payment fraud. Category 3 should be included in Category 2 because it is the customer who authorizes the payment to transfer the funds; the examples given for this category would be an investment scam or other type of app scam

Category 4 comprises in first place what banks call "admission fraud" - the opening of bank accounts and/or applying for credit cards using stolen identities (e.g., 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 also comprises the cases where the bank's IT systems are compromised. We believe this category could be split into two because these two types are completely different from the point of view of how fraud is committed and the potential mitigating measures that can be taken for each type.

A new category should be added – Customer fraud. There are cases where the investigation carried out by the bank/PSP doesn't find evidence of third parties being involved in the fraudulent transaction other than the customer.

As mentioned in our cover letter, it is important that there be common definitions, and taxonomies, around various types of digital fraud to avoid fragmentation, especially if banks have to report on digital fraud cases across different jurisdictions.

Additional Facts and Figures for consideration:

Statistic	Source
One in every five global consumers fell victim to payments fraud in the last four years. 27% of these victims were the subject of an APP scam.	ACI Worldwide (2023), Prime Time for Real-Time Global Payments Report
Payment fraud is expected to continue increasing and is projected to cost $40.62 billion globally in 2027. Payment fraud cases and skimming attacks spiked 164-174% from mid-2021 to mid- 2022. The cost of digital crime more broadly is projected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015.	Visa (2023), Visa Payment Fraud Disruption Biannual Threats Report December 2022, page 28; Cybersecurity Ventures (2022), 2022 Official Cybercrime Report, page 2
For major European banks, nearly half (47%) of sanctions alerts were reported in 2019 to take longer than a day to process, with almost 100% processed after 5 days.	Oracle (2019), Disrupting Status Quo in AML Compliance, page 4
False positive rates produced by legacy screening systems can reach upward of 95%. EY's experience working with banks across the globe has shown that deploying secondary screening analytics can reduce false positives by up to 70%, allowing investigators to focus on the smaller percentage of payments that truly warrant human review. As importantly, analytics tools in that study identified additional risks in more than 2% of alerts that an investigator had (incorrectly) marked as false positives.	EY (2021), Now payments are in real-time, how can Australian banks continue to conduct effective sanctions screening?
Visa Advanced Authorization prevented $27 billion in fraud during 2022	IIF (2023), Data Policy Impacts Fraud Prevention
CNP card sales reached 19% in 2020 of total card sales, up from 15% in 2019.	IIF (2023), Data Policy Impacts Fraud Prevention
The cumulative effect of fraud losses could reach an additional $108bn of fraud up to 2030 if 30% of machine learning fraud data is lost and up to an additional $180bn up to 2030 if 50% of machine learning fraud data is lost.	IIF (2023), Data Policy Impacts Fraud Prevention; IIF staff estimates based on analysis by SAS, Gerhard Svolba, "Quantifying the Effect of Missing Values on Model Accuracy in Supervised Machine Learning Models
In 2018, $278 billion in card-not-present transactions were declined globally, representing a 27% year-over-year growth.	Visa AI Security (2019), Transforming Payment Security Through Artificial Intelligence
Scams are a growing threat to Australian consumers and businesses, with financial losses to scams of at least $3.1 billion in 2022 (an 80 per cent increase on losses recorded in 2021).1 In 2022, 65 per cent of Australians were exposed to a scam attempt.2	Australian Treasury, Scams – mandatory industry codes, page 4
Digital Twins of Financial Crime Analysts are deployed into banks providing unlimited capacity to more efficiently and effectively manage alert volumes, absorb alert spikes, and reduce the risk of non-compliance. (An [AML] alert decision engine (ADE) was deployed as a "virtual" level 1 analyst to screen all alerts for false positives prior to a manual Level 2 analyst review for detailed investigation. The chosen technology provider's claimed outcomes included decision accuracy of 99%, and reduced decision times from 30 minutes to less than 3 seconds. The FI reported significantly reduced time spent in assessing alerts and re-invested this time in high value risk management	Merlynn, Digital Twins in Financial Crime Alert Management, cited in IIF (2023) Data Policy Impacts – AML and Regtech Solutions

activities, enabling the FI to add plug-ins based on data analytics, derived from behavior, refining the system's ability to flag potential financial crime.	
A study by McKinsey & Co. and the Global LEI Foundation (GLEIF) estimated that on an annual basis, banks could potentially collectively save between $250 million to $500 million per annum if LEIs were used to identify international entities and to automate the tracing of their history for the issuance of letters of credit, including by reducing the incidence of false positives based on AML and other compliance lists.	McKinsey & Company and GLEIF: Creating Business Value with the LEI - Solutions – GLEIF
Card fraud in 2021 continued its downward trend, falling to its lowest level since data collection began. It constituted 0.028% of the total value of card payments made using cards issued in the Single Euro Payments Area (SEPA), amounting to €1.53 billion from a total value of €5.40 trillion. Card-not-present fraud, which accounted for approximately 84% of the total value of card fraud in 2021, declined by 12% from 2020 following the market-wide implementation of strong customer authentication under the revised EU Payment Services Directive (PSD2). Card-present fraud fell by 6% in 2021 from its 2020 level, owing to the continued global roll-out of industry standards, which have been effective in reducing opportunities to commit magnetic stripe counterfeit fraud. Most of the card fraud in both 2020 and 2021 involved cross-border transactions.	The European Central Bank: Card Fraud

Are there additional financial stability and/or prudential transmission channels from digital fraud to the banking system?

It is important that the prudential and financial stability implications are taken into consideration when assessing digital fraud. But it is also the case that there are already Operational Risk requirements for banks that take into account Digital Fraud. There are also relevant risk management requirements as well. Banks should only be liable and register the operational risk losses for which they are responsible.

When it comes to "scam" payments authorized by clients it is important that there is appropriate regulation to address liability framework for these payments so that banks are not forced to bear and register operational risk losses for which they are not responsible, which has the following negative consequences from a prudential and financial stability perspective, including on P&L, capital management, and bank reputation.

From a financial stability perspective, it is necessary that the prudential framework ensures that banks are not responsible and are not liable for authorized "scam" payments.

The discussion paper discusses bank apps and websites, but obviously a lot of fraud is conducted through creating fake portals and websites and scraping customer details from legitimate (and illegitimate) websites. Given the increases in number, scope, and sophistication of spoofing, and deepfakes, and also the fact that generative AI and quantum computing will make the adversaries even stronger (as well as bank/law enforcement defenses), more attention could be

paid to the creation of layers between the customers and the banks, as channels of attempted fraud. That would include Fintech aggregators, and other forms of "open banking," and how their intermediation can create new channels of risk. International standard setters and the BCBS should consider an operational risk management framework that should apply to these non-bank participants to help incentivize anti-fraud efforts.

For example, just recently, a deepfake fraudster in Hong Kong reportedly stole HK$200 million (US$25.6 million) from a multinational company's offices in Hong Kong using deepfake technology.[16] Technological advancements impact the role of trust and security in payments, and it is important the private and public sector work together to make customers aware of these types of deepfakes.[17]

To address some of these issues consideration could be given to regular testing by firms and their supervisors for extreme scenarios. Scenarios could include fraudsters accessing payment systems and undertaking significant damage. That also connects to the importance of digital trust and initiatives around this area.

[16] ARS Technica 2024. "Deepfake scammer walks off with $25 million in first-of-its-kind AI heist" Feb. 5, 2024
[17] See IIF 2023 "Payments Security and Trust" (Sept. 29, 2023) for a discussion around security, trust and opportunities for public-private cooperation.

Question 2:

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

In its Consumer Trends Report 2022/23, the European Banking Authority (EBA) identified the growth in the use of payment services, both in numbers and value of electronic transactions, as one of the main trends in retail banking products and services. At the same time, the EBA points out that the most relevant issue concerning this trend is fraud.

Regarding statistics, at European level the EBA publishes every year data on fraud in payments:

- **The EBA Retail Risk Indicators report** provides two types of data; the latest available ones are for 2021. The first one is the share of fraudulent card payments over all card payments: it was 0.0228% in terms of volume and 0.0385% in terms of value in the EU. The second one is the share of fraudulent credit transfer payments over all transfer payments: it was 0.0025% in terms of volume and 0.0004% in terms of value in the EU.
- **The EBA report on payment fraud data under PSD2, based on data from all Payment Services Providers (PSPs):** The latest available data are for H2 2020. The report offers data for four payment instruments – Cards as reported by issuers, Cards as reported by acquirers, Credit transfers and Cash withdrawals. For each of them, a breakout is provided according to three different types of fraud: the manipulation of the payer by the fraudster, the modification of a payment order by the fraudster, and the issuance of a payment order by the fraudster.

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1054879/Consumer%20Trends%20

As mentioned in the first part of our IIF response, UK Finance, the British banking, and finance industry association, produces a comprehensive report on fraud every year, with half-year updates. In the first half of 2023, UK Finance found that:

- Overall fraud losses totaled GBP 580 million, down 2.4% year on year; of which unauthorized fraud fell 10%, and authorized push scams rose 22%, while Impersonation Police/Bank fell 35%.
- In terms of the origin of this fraud and scams, 77% took place online, 17% over telecommunications, 1% over email, and 5% through other channels.

www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf

On September 2023, the FSB published a document "Stocktake of International Data Standards Relevant to Cross-Border Payments" explaining how the transfer feasibility of data across borders is essential for the well-functioning of the cross-border payments system. It also pays lot of attention to the effect of data localization on anti-fraud measures:

Localization policies can have a number of negative effects, sometimes in ways that would be in conflict with their intended purposes. Industry stakeholders argued that data restrictive policies could:

- increase cyber and operational risks by preventing firms from using regionally situated experts to manage operational risks on an enterprise-wide basis and often require patchwork changes to existing data architecture, thus increasing the possible scope for vulnerabilities.
- prevent financial institutions from pooling data from different sources, thereby weakening internal capabilities to effectively manage risk, detect fraud or identify suspicious activities for AML/CFT compliance purposes.
- prevent financial institutions from complying with cross-border regulatory requirements, including AML/CFT compliance, prudential supervision, and investor protection requirements.
- increase fixed and variable costs to deliver payments, by often requiring new data centers and systems to accommodate such policies. This acts as a barrier to entry for smaller or new players. They also have potential environmental implications associated with the requirement to establish and maintain additional data centers.

Additional papers, reports, and data sources:

ACFE Insights (2023), AI Fraud: The Hidden Dangers of Machine Learning-Based Scams

Cybersecurity Ventures (2022), 2022 Official Cybercrime Report

Financial Action Task Force (2021), Cross-Border Payments - Survey Results on Implementation of the FATF Standards

FATF Interpol Egmont Group 2023. Illicit Financial Flows from Cyber-Enabled Fraud November 2023

IIF/Deloitte: Global financial crime prevention, detection and mitigation Building on progress, addressing evolving priorities and achieving effective outcomes

IIF (2022), IIF Response to the FSB on Data Frameworks Affecting Cross-Border Payments

IIF (2023), IIF submission to FSB: case studies of data frameworks' impact on cross-border payments

IIF and EY (2024), 13th Annual EY-IIF Bank Risk Management Survey

IIF (2023), IIF Staff Paper: Payments Security and Trust

IIF (2023), Data Policy Impacts Fraud Prevention

IIF (2023) Data Policy Impacts – AML and Regtech Solutions

Mastercard (2023), Mastercard leverages its AI capabilities to fight real-time payment scams

McKinsey & Co (2022), Cybersecurity trends: Looking over the horizon

ORX (2023), Annual Banking Loss Data Report 2023

Sift (2023), Q2 2023 Digital Trust & Safety Index: Fighting fraud in the age of AI

Sift (2023), Growing AI-powered fraud highlights the need for advanced fraud detection

South African Banking Risk Information Centre (2022), Annual Crime Statistics 2022

SWIFT (2023), Small payments. Big opportunity.

SWIFT (2021), Guiding principles for screening ISO 20022 payments

Visa (2023), Visa Payment Fraud Disruption Biannual Threats Report December 2022

World Economic Forum (2023), Global Risks Report 2023

Question 3:

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

It may be helpful for BCBS, working with other international standard setters including the FSB and CPMI, to undertake joint work on the prevalence and prevention of chargeback fraud and other areas of first-person or friendly fraud. This may become particularly prevalent in those jurisdictions that choose to adopt a reimbursement policy for APP scam consumer losses. Given the role played by various parties in this space international standard setters should engage non-FIs institutions such as Telecoms and Law enforcement agencies in this work to ensure there are holistic recommendations for a cross-sectoral issue.

The international standard setters are also encouraged to consider how to operationalize better digital trust and identity tools, by which consumers would gain added certainty that bank representatives are who they claim to be. Digital verifiable credentials that could reliably identify communications, websites, and apps, among other things, originating from banks would go a long way to reduce APP scams for example.

It may also be helpful for BCBS to work with international standard setters to undertake activities such as workshops designed to raise awareness of the need for machine learning and advanced techniques to be deployed to detect and prevent fraud, and also to highlight the link with data policy (or data frameworks) that we have attempted to draw in our work, and which has also resonated with the FSB in the cross-border payments space.

In an IIF submission to the Financial Stability Board (FSB) on Case studies of data frameworks' impact on cross-border payments dated October 30, 2023, we presented a number of case studies of the impact of data frameworks (including data barriers) on cross-border payments that are relevant in the fraud context, including:

- Impacts of cross-border personal information transfer requirements
    - EU-US data sharing arrangements
    - Restrictions on personal information export – China and South Korea
    - Personal information transfers in B2B context
    - Intra-group personal information transfers
- AML/CFT, sanctions screening and fraud prevention
    - Impacts of data frameworks on advanced cross-border solutions
    - Impacts of national AML/CFT data localization measures
- Data localization of payments-specific data
- Data localization and operational and cyber risk

The letter proposed a series of priority actions to address these issues, including:

- Address data localization
- Data gateways
- Data access
- Privacy law interoperability
- Binding Corporate Rules

- Data standards

Finally, we believe a cross-sectoral solution is needed to address digital fraud. We encourage cooperation among the global standard-setters, including the Basel Committee and the FSB, in order to consider fraud in its full context so that the weaknesses and responsibilities are appropriately identified and allocated in order to effectively fight fraud, so that there is also a consistent approach across jurisdictions.