Q1. Do you agree with the features and categories of digital fraud?

A: Yes, we overall agree with the features and categories of digital fraud.

However, the definition of digital fraud might fail to address or undervalue some important trends:

- Communications' based identity spoofing[1] to support digital fraudulent operations, namely situations where the scammers are able to fake the Caller Identification Number or other metadata of a telephone call or text message (i.e., when the scammer calls or texts, the Bank's number appears on the person's telephone), therefore leading the Bank customer to believe that it is in legitimate contact with its Bank or with another entity chosen to inspire trust or authority (e.g. a law enforcement agency), and increasing the chances of success of those fraudulent actions/Entity's. This conduct may lead to the authorization of payment transactions by the Bank customer/payment service user (as referred to in point 2 and differently from the categories of fraud referred to in point 1, which lead to unauthorized payment transactions). This subject, the so-called "impersonation fraud", is currently foreseen in the proposal of PSD III/PSR, which is under negotiation.
- Deepfake[2] based identity theft frauds, namely in terms of spoofing customer identities through the creation of fake identity documentation, fake media records and files (photo, video, audio) and fake media live content (impersonating voice). This trend is increasing, based on widely available artificial intelligence techniques belonging to the deep learning type, and contributes to an exponential increase in the overall effectiveness of the digital fraud operations performed.
- Digital fraud perpetrated through employees' credentials of a Bank and/or any other intermediaries, namely in cases where there are email compromise situations through phishing or similar attacks, allowing the creation of fake and fraudulent payment orders by usurping the employees' credentials, or cases where a fraudster impersonates an employee of the Bank[3].
- Fraud in banking products and services other than payment services, namely, and most importantly, considering the rising trend of deposit account overdraft and/or consumer credit[4], whereby fraudulent actors, after gaining access to the account or identity information of banking customers, or by simulating banking relations, get funds from the Bank under some type of personal loan agreement and disappear with the funds.

[1] What is Phone Number Spoofing | Phone Scam (kaspersky.com)
[2] Deepfakes make banks keep it real (ft.com)
[3] Identity theft | CaixaBank
[4] What Is Loan Fraud? How Do I Protect My Financial Assets? (aura.com)

Therefore, we believe that Section 1 could be enhanced with the following changes: i) a more detailed description of the impact of spoofing and deepfakes in the effectiveness and spread in the context of situations of fraud identified in points 1 and 2, ii) a more detailed description of the importance of personal loan services right after payment services in point 3, and iii) a consideration on the fact that the indirect role of Banks might in some cases be actually direct, where the fraudulent scams are targeted at Bank's employees but affect customer accounts though the formers' actions.

Q1. Are there additional financial stability and/or prudential transmission channels from digital fraud to the banking system?

A: No, we understand that there are no additional financial stability and/or prudential transmission channels from digital fraud to the banking system.

However, the indirect transmission channel, regarding reputation, could be better detailed, namely:

- The size, extent, scope and speed of the impact transmitted to the banking system with a potential impact on financial stability is not necessarily dependent on the reimbursements. We consider that a material reputational damage could arise from the news, social media[5] and other communication channels and how the issue is addressed therein, and the tone set on those public communications, together with the reaction, in terms of communication, from Banks and supervisory authorities. A digital fraud scam which is widespread through negative social media and traditional media news, not properly addressed in terms of restoring confidence by the affected Banks and supervisory authorities, might lead to a more structural lack of trust and even to a deposit withdrawal from customers.
- In terms of data, social media and traditional media traffic, and consumer confidence[6] data, could be used to measure the potential imbalances between jurisdictions, and, at the individual level, surveys on brand value and other related metrics[7] could complement fraud related data.
- In conceptual terms, it might be argued that the real novelty of digital fraud for financial stability is related to this notion of confidence. Considering the basic notion of the impact on financial stability from a financial perspective (of the solvency, liquidity and profitability of individual Banks and the overall system), we have evolved to an additional notion, through the Basel Committee on Banking Supervision's Principles on Operational Resilience, which stipulates that, regardless of their financial condition, operational disruptions on Banks might hamper financial stability due to the inability of firms, organizations and persons to perform

[5] Wake up to the dangers of digital bank runs (ft.com)
[6] Leading indicators - Consumer confidence index (CCI) - OECD Data
[7] Basef Banca: Estudos & Serviços (marktest.com)

their basic necessary banking activities, therefore hurting directly economic flows and potentially creating additional volatility (see, as example, a recent ransomware case reported[8]). With digital fraud, however, we might be facing a new, third-way, propagation hypothesis, which is regardless of financial conditions and of operational resilience: confidence[9]. If customers lose confidence in one Bank or in the system, and stop doing business, financial stability is impacted in the same way as in the other hypotheses, e.g., due to digital fraud, simply because the decrease in the use of financial services is equivalent to their disruption. This is not new, conceptually, but has not been addressed through banking laws, regulation or supervisory powers and activities, unlike the financial soundness and operational resilience.

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

A: We understand that the Committee could consider other data sources when assessing the risks of digital fraud.

Although data on payment transactions is already captured and is unquestionably the one with the most quantitative nature, integrity and precision, and direct link with the systemic risk from digital fraud, there could be other data sources that contribute to this assessment in a complimentary way, e.g.:

- One important source of information is cybercrime[10] data collected by cross-sectorial authorities in the context of their activity, specifically if data is available per sector and by crime typology. An increase or other trend or feature of digital fraud related events found in this data could be helpful in complementing the overall digital fraud landscape, together with other sources, with a focus on the criminal implications.
- Customer complaints[11] are another relevant source of information, specifically if data is available per product or service, channel and source of complaint and processes are reliable. An increase or other trend or feature of digital fraud related events found in this data could be helpful in complementing the overall digital fraud landscape, together with other sources, with a focus on the customer impact.
- Another potential source of information is data on major incidents[12] reported by the Banks, specifically if this data covers both operational, security and cybersecurity incidents, and

[8] Ransomware attack on ICBC disrupts trades in US Treasury market (ft.com)
[9] FINANCIAL STABILITY OR INSTABILITY? (researchgate.net)
[10] Report Cybercrime online | Europol (europa.eu)
[11] Guidelines for complaints-handling for the securities (ESMA) and banking (EBA) sectors | (europa.eu)
[12] EUSurvey - Survey (europa.eu)

distinguishes incident root-causes that might be directly or indirectly related to digital fraud. An increase or other trend or feature of digital fraud related events found in this data could be helpful in complementing the overall digital fraud landscape, together with other sources, with a focus on the systemic implications from low frequency high-severity events.

- Finally, data on operational losses, as required by the Basel III and Basel III standards, might also play an important role. However, the standard should be adjusted in order to allow for a better use of the data, as the current list of event types makes the usefulness of External Fraud data indeed very limited. Further granularity could be useful to assess digital fraud.

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

A: Yes, we understand that additional, banking-specific, initiatives on digital fraud could be pursued by the Committee.

We agree with the list of initiatives presented in the discussion paper and we recognize their importance. However, there might be other areas where supervisory attention is warranted to tackle digital fraud:

- Media and social media management requirements applicable to both Banks and Supervisors.

  This could be embedded into Principles, either new or existing, and would aim at establishing the need for Banks and Supervisors, individually, among them and between both categories, to have in place adequate communication management strategies, policies and procedures specifically targeted at limiting the impacts on consumer confidence of ill-founded news regarding digital fraud that might have a potentially systemic impact on the financial system.

- Cooperation framework, requirements, and tools for information sharing among Supervisors.

  Creating the basis for effective cooperation among supervisory functions in Banking (payments, prudential, conduct, anti-money laundering, etc.) and with other authorities (e.g., Crime Police) to foster information sharing that allows for having a complete set of data from all sources, which are put to work to steer supervisory actions.

- Cooperation framework, requirements, and tools for information sharing between Banks.

  In this regard, it is especially important to consider: i) supervisory expectations fostering collaborative approaches among institutions to fight digital fraud as non-competitive area of business; ii) requirements for financial market infrastructures, namely payments, to allow for these initiatives to be effectively implemented in practice; iii) joint initiatives developed by

banks in the areas of mule-accounts[13], synchronized customer fraud online alerts[14] and joint efforts for digital education, using the channels of both public and private entities, with a focus on traditional distribution channels, to tackle the less informed[15].

The Banco de Portugal, through its Forum on Cybersecurity and Operational Resilience[16] is currently working on a long-term plan with initiatives tackling these three areas of action.

Furthermore, within the Payment Systems Forum[17], an advisory structure of the Banco de Portugal that brings together the main national stakeholders involved in the supply and demand of payment services, including General Government representatives, the Banco de Portugal has been involved in several initiatives to tackle digital fraud. The Payment Systems Forum has recently published the National Strategy for Retail Payments 2025[18], with initiatives to be implemented until 2025, several of which are aimed at fraud prevention, as detailed in the Strategy.

Finally, the Banco de Portugal believes that there could be merit in promoting a framework for initiatives based on innovative technologies such as artificial intelligence applied for behavioral analysis, aimed at mitigating digital fraud.

[13] Money Muling | Europol (europa.eu)
[14] How to Recognize and Prevent Bank Fraud to Avoid Becoming a Victim (bankofamerica.com)
[15] esa_thematic_report_on_financial_education.pdf (europa.eu)
[16] Forum on Cybersecurity and Operational Resilience | Banco de Portugal (bportugal.pt)
[17] Payment Systems Forum | Banco de Portugal (bportugal.pt)
[18] National Strategy for Retail Payments 2025 (bportugal.pt)