The Italian CERTFin – CERT Finanziario Italiano – is a public-private cooperative initiative aimed at increasing the cyber risk management capacity of financial operators and the cyber resilience of the Italian financial sector through operational and strategic support activities for prevention, preparation and response to cyber attacks and security incidents. The CERTFin performs its activities, which are developed on a cooperative basis for the benefit of all participating financial institutions, in line with the national strategy and with other country-wide institutional initiatives relating to cybersecurity and the protection of critical infrastructure, helping to further develop the national and international network of institutional partners and experts.

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?

It would be beneficial to have a unique standard as a reference for the classification, sharing of fraud related information and distinction between fraud and scams. A reference point could be the document Fraud Taxonomy annually updated by a dedicated Expert Group of the European Banking Association.

Regarding the distinction between fraud and scams, we propose the following two definitions:

- **Scams**: all situations in which the customer is manipulated to initiate a payment or to exchange sensible banking data with fraudster should be considered. Mainly, scams involve the sale of goods and/or services that once purchased are either not delivered/provided or turn out to be significantly different from what the scammer advertised. However, in these cases, payment is voluntarily and consciously completed by the victim (consciously means that the money actually goes to whom the customer wants it to go), without any compromise or technical intrusion (i.e. spoofing).
- **Fraud:** The attacker's goal is not to sell something but to access the victim's money through the direct or indirect use of banking channels. Fraud is characterized by unauthorized transactions or authorized transactions without the perception that the money is directed to someone other than the will of the account holder. In fraud there is always compromise or manipulation or both.

The Italian CERTFin believes that the following three categories should fall under the definition of digital fraud:

a. *The unauthorized transaction was carried out thanks to a compromise of confidentiality: the fraudster, using reasonably sophisticated techniques, managed to steal all the information useful to replace the legitimate payer and complete transactions on his behalf.*
b. *The unauthorised transaction was carried out thanks to a compromise of integrity: the fraudster, using reasonably sophisticated techniques, managed to alter the data of the transaction ordered by the payer, for example by replacing the IBAN of the legitimate recipient with his own.*
c. *The unauthorised operation was carried out thanks to a manipulation of the payer: the fraudster, using reasonably sophisticated techniques, convinces the payer to transfer money to accounts controlled by the fraudster himself or his accomplices.*

Furthermore, we propose to include in the scam category and not in the digital frauds the case when customers are manipulated into investing in fake saving products or taking on fake credit products and the customer voluntarily authorizes to transfer money.

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

The increase of digital frauds undermines customers' confidence in the whole financial system. To this aim, among other data sources, data on frauds should also be gathered, analyzed, and made available in an aggregated manner, by subjects such as the Italian CERTFin. Such analysis could contribute to identify the weak points (for example, the Telco sector) and to prepare adequate countermeasures. Given the increasing importance of this topic, in our opinion the Committee may encourage each country to establish entities acting as data source at national level, to allow information sharing with authorities and/or on an international level.

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

In the European Union cross-country information sharing could be promoted more extensively. One obstacle to the info sharing of fraud related data is the presence of different interpretations of the GDPR and for this reason there is the need for further clarification from the European authorities, in particular the Privacy one, even in the light of regulations promoting info sharing (PSR and DORA).

Another mean available for the financial sector to help reducing digital frauds is the blocking of the execution of the payment order / the related funds, which could be pursued as proposed by a recent amendment by the ECON Commission of the European Parliament within the scope of the Payment Service Regulation review.

Last but not least, an initiative that can be further explored is the promotion of inter sectorial collaboration, on the basis of which different sectors cooperate to reduce digital frauds.