ABI Associazione Bancaria Italiana CERTFin

Position Paper concerning questions raised in *Discussion Paper* EBA/DP/2022/01 on the «EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry»

31 March 2022

1 Introduction

This contribution is jointly provided by the Italian Banking Association (ABI) and the Computer Emergency Response Team of the Italian Financial Sector (CERTFin).

ABI is a voluntary non-profit organization. Its purpose is to represent, defend and promote the interests of its member banks and financial intermediaries. It works, in this framework, for the development of the awareness in society and within the banking and financial system of the social and behavioral values that follow from entrepreneurial principles and from the formation of open and competitive markets. Specifically, ABI undertakes initiatives for the orderly, stable and efficient growth of the banking and financial system, in a competitive outlook consistent with Italian and European Union law.

The CERTFin is a public-private cooperation initiative born in 2017 with the objective to raise the ability to manage cyber risk of financial operators and the cyber resilience of the Italian Financial System as a whole, through operational and strategic support on prevention, preparation and response activities and security incident. CERTFin's chairmanship is shared by Bank of Italy and the Italian Banking Association; the Operational Directorate is entrusted to the ABILab Consortium – Banking Research and Innovation Centre.

CERTFin conducts an annual survey, addressed to the financial industry, regarding ICT security, cyber attacks and linked risks as well as the increasingly widespread frauds in the italian banking sector. More specifically, this survey allows to have an estimate of the number of blocked or actual fraudolent transactions, carried out through internet and mobile channels, and a detailed overview of the main tecniques used by fraudsters, the most common fraud patterns (at the expense of both corporate and retail customers). On average, 20-25 financial institutions fill out the survey, reaching a representativity of the Italian financial industry which exceeds 70% in terms of number of employees.

This contribution is therefore sent in accordance with ABI and CERTFin's institutional purposes.

2 General remarks

- Overall, the data collected reflect a very low level of incidence of frauds and show that the security measures taken by European PSPs are adequate. We would like to note that the PSD2 SCA framework has only been in force for a short time and, as EBA reported, several countries had not started yet reporting the corresponding data related to the period considered in the analysis (2019/2020). Therefore, we assume that it would still be too early to draw definite conclusions. We believe that the introduction of the SCA framework has brought many benefits to the security of the sector and of the clients and proved to be an appropriate measure, in particular dynamic linking was very effective. However, frauds in remote payments with counterparts located outside of the EEA confirmed the need to reflect upon the "best-effort" rule for one-leg out transactions in order to reinforce security for providers located inside EEA.
- It might be appropriate to strengthen control mechanisms, e.g. tracking/monitoring of transactions, recovery communication processes with extra-EEA counterparties (especially in the event of a recall), as well as adopt and/or improve best practices (e.g. maintaining internal white/grey/black lists,

analyzing customer behaviour, being transparent in communication to customers, etc.).

- There are new attack patterns used by fraudsters who, in the wider digital ecosystem, are focusing in particular on human vulnerabilities and/or processes involving other actors, including those outside PSPs. Therefore, given that new types of fraud depend on new attack techniques, we suggest that this area be explored in detail and about possible correlation with the regulations in force, e.g. cybersecurity acts, incident/security guidelines, etc.
- A greater harmonisation among countries is also highly desirable to avoid that fraudsters take advantage from regulatory arbitrage.

3 Questions & Answers

Question 1: Do you have any views on the high share of cross-border frauds in the total volume of fraud?

As a general remark, cross border frauds may have a greater chance of success in countries where regulation is less stringent. This is especially true for countries where PSD2 does not apply, i.e. extra-EEA countries, and therefore security measures may be less effective.

As a matter of fact, frauds more often occur also across national borders, i.e. intra-EEA countries, making it easier for fraudsters to circumvent national rules and avoid prosecution. Fraudsters prefer to move money to countries other than their country of origin to make recovery of funds by PSPs and law enforcement by local authorities harder. Therefore, the fact that the share of frauds perpetrated through payments executed inside EEA appears to be much higher when compared to the share for domestic payments could be mainly due to the lack of a common cooperation protocols among Financial Institutions. Such protocols would greatly reduce the effectiveness of the fraudulent attempts and the impact of frauds on EEA payments, thus creating simpler and faster processes for financial institutions could rely on in order to report fraudulent transactions and retrieve the money transferred across countries.

In all these cases, it becomes **more difficult for law enforcement agencies to investigate and trace the fraudsters when the fraud is carried out cross-border, both extra and intra EEA**.

For example, cross-border frauds could involve so-called tax havens countries and countries with few rules on financial transparency. As the regulations are different, it becomes difficult to trace the origin of the funds and whether they were obtained through fraud or illicit actions.

In addition, we think the lower number and volume of cross border payment transactions (especially non-remote / card present) could partially explain the higher fraud rate with regards to those transactions.

As far as **card payments** are concerned, from an issuer point of view, besides the possible exemptions, remote payments are now always authenticated with SCA. With

specific regard to card-present cross-border transactions, some operators reported an important volume contraction due to the pandemic events that reduced a lot travels and especially the use of business cards. On the acquirer side, two reasons can explain the high share of cross-border fraud:
1) Higher number of non-EU merchants compared to European merchants and therefore higher incidence of e-commerce transactions (e.g. USA and China);
2) In case of non-European transactions, the One Leg principle applies, which potentially reduces the security of the transaction.
On the issuer side, we are particularly concerned about cases regarding frauds connected to pre-paid cards with IBAN.

Differently, as far as **credit transfers** are concerned, it was noticed that in the fraudulent attempts, detected before funds are debited, the IBAN and the PSP were typically inside the EEA. In addition, the higher incidence of fraudulent cross-border transfers compared to domestic ones is mainly due to the greater difficulty in the recovery of funds processes and communication with foreign counterparties in the event of a recall, making them more easily exploitable by fraudsters. Indeed, we found that some countries were more affected, perhaps due to the nationality of the fraudsters or the existence of less strict national regulations (e.g. when opening online accounts).

Given the above considerations, on the regulatory side, the "best effort" rule might need reconsideration to limit the impact for EU PSPs and therefore for merchants and users, especially where the payer's bank is located within EEA and the beneficiary's bank is outside the EEA.

Question 2: Do you have any comments on the patterns that are outlined in the chapter "patterns emerging from the selected data"?

As a general remark, the patterns outlined might depend on the lack of homogeneity with regard to anti-fraud tools and processes among countries/operators.

According to some operators, fraud patterns using malware or viruses are limited to "organized" hackers or groups. Following the introduction of PSD2, it became more difficult to perform a fraud due to SCA and dynamic linking required for the authorization of the payment. For example, in the past a simple SIM swap would have been enough to retrieve an OTP and authorize a payment. Therefore, against these developments, fraudsters are now moving to social engineering, phishing and smishing patterns. It is not the fraudster itself to initiate/authorize the payment, but it is the client who is authorizing the transaction being induced by the fraudster, so typically a manipulation of the payer by the fraudster takes place.

Unfortunately, this category is very difficult to be detected and cannot be prevented by the security safeguards of the payment systems.

For major groups and highly skilled hackers, on the other hand, the use of malware is still an option, but they are more concentrated on getting personal data from government and multi-national companies' databases as well as or directly from the PSPs, which creates more alarm and global emphasis, than to steal some money from small clients.

As to payer's manipulation techniques, following the Covid-19 Pandemic and the introduction of new payment instruments (e.g. SCT Inst), it is worth mentioning

telephone spoofing. In such case, the fraudster masks the caller's number by pretending to be the bank and, once he has gained the customer's trust, induces the latter to share personal credentials and authorise payment transactions. In order to prevent these types of fraud, some operators consider appropriate to **promote some form of coordinated action at European level**, aimed at stopping this phenomenon, also **involving directly Telco operators and smartphone operating system manufacturers.**

Specific remarks are also noteworthy with respect to some patterns illustrated in the different figures of the EBA report. For example, observing the pattern illustrated in Figure 1 (where the "Volume of transactions in millions €" could seem inversely proportional to the "Average fraud amount per transaction in €") some operators observed that, rather than suggesting a direct correlation, this might depend on the means of payment used and on the amounts which each means of payment typically involves. As a matter of fact, cards are often used for small value payments, while in the case of larger money transfers a payer can opt for credit transfers. Therefore, it can be noticed an inversely proportional relationship between "Volume of transactions in millions" and "Avg. fraud amount per transaction in €" which is probably correlated to the means of payment and the average amount exchanged per transaction with each payment instrument. When the average amount per transaction by means of payment is greater, the average fraud amount per transaction will also be greater.

As to Figure 7, in order to better understand the phenomenon, it could be useful to clarify whether the cards virtualization in wallets is also included in the non-electronic initiation.

Furthermore, for non-remote / card present transactions, the lost and stolen cards is the pattern we think is most used by the fraudsters, especially because contactless transactions allow the card to be easily used at POS terminal also by non-cardholders. Additionally, at the time the data were reported not all cards had been migrated to a chip and pin solution, (the EBA Q&A 2018_4399 clarified this issue only mid-2020) and some of them might still have been chip and signature only. Cash withdrawals are usually performed with debit cards, which originally are already chip & pin based for all issuers. Therefore, lost and stolen cards are the most common reason of frauds. Unfortunately, it is not unusual that some cardholders use to write their PIN on a paper and keep it together with the card. It is easy for a robber to use the card for withdrawals consequently. This could explain the percentage of issuance of a payment order by the fraudster.

Question 3: Do you have any potential further explanations as to why, in the specific case of the remote credit transfers, the fraud rate reported by the industry is higher for payments authenticated with SCA compared to payments that are not authenticated with SCA?

There is a convergence among operators in agreeing that the focus of fraud attacks on remote credit transfers is **related to the increase in the number of transactions that are now made using SCA combined to the manipulation of the payer**.

In case of remote credit transfers, we think that the reason why the fraud rate reported by the industry is higher for payments authenticated with SCA compared to payments that are not authenticated with SCA is linked to the high number of the transactions that are now made using SCA. Indeed, exactly because SCA has become

the most used method for almost all transactions, criminals have increasingly started looking to the remote credit transfers with SCA to make frauds. As a result, the number of frauds using SCA is higher. Further, fraudsters focus more on SCA credit transfers because they are - on average – more profitable due to the higher amounts involved, as mentioned above.

Additionally, even if SCA is a quite secure authentication/authorization method, it cannot halt the social engineering and phishing and thus the customer manipulation, where the fraudster can get the fraudulent payment authenticated by the client itself. In particular, the use of social engineering (techniques of social deception aimed at exploiting vulnerabilities of people, e.g. uncertainties, fears, distractions) and the falsification of the identity of the sender of a phone call or of an SMS (Spoofing) or the ALIAS of the sender of an email or an SMS (Swap alias), typically pretending to be the payer's PSP, are surely dynamics implemented by fraudsters aimed at stealing customer data. Another typical example is CEO fraud, which occurs rarely but may result in larger individual losses if successful (sometimes several million euros per event). Moreover, it seems to be easier for fraudsters to deceive customers and obtain the complete credentials than to break through the banks' systems.

More in detail, as concerns the manipulation of the payer, the so-called "enrolment process compromise" is worth mentioning. This fraud is usually perpetrated through the following operative stages:

- The victims receive a text message from the fraudster, via SMS spoofing (which means that the text message appears in the same SMS thread as genuine ones, previously sent by the victims' legitimate financial institution), warning them about a suspicious access to their account, urging them to click onto the link attached.
- The victims click on the link, which redirects them to a bank clone page, and fills in a form with their access credentials, as well as sensitive information (e.g. the phone number). Once the victims have entered all the requested information, the web page shows an error message, informing that they will soon be contacted by one of the bank's anti-fraud operators.
- At this point, the fraudster (who in the meantime has already installed the mobile banking app on his/her own mobile device, which requires the victims' credentials in order to be activated (e.g. user code, PIN, etc.), calls the victims via phone, persuading them to hand over their OTP codes, which are required to finalise the activation of the fraudster's mobile banking app, certifying his/her device as belonging to the victim.
- Finally, once the mobile app has been successfully activated, the fraudster will convince the victims (through social engineering) to supply any other OTP code necessary, in order to carry out additional operations in their place (eg. launching unauthorized transactions or overwriting another phone number on the victims' number linked to the targeted bank account, etc.).

In addition, another reason explaining the observed trend is that non-SCA remote credit transfers are possible only for the exemption cases allowed by the RTS, and therefore most of these exemptions are applied to the most secure payments, those whose risk of a fraud is lower (i.e.: trusted beneficiary, low value payments, Transaction Risk Analysis, etc. …) and this was the case already before PSD2 introduction. For example, recurring transfers (exemption under Art. 14 of the RTS "Recurring Transactions") or giro transfers (exemption under. Art. 15 of the RTS "Transfers between accounts held by the same natural or legal person") are

intrinsically types of credit transfers characterized by a low degree of risk and unlikely to be subjected to fraudulent attacks, both before and after PSD2 introduction.

Moreover, also corporate payments, which can benefit from SCA exemption under Art. 17 of the RTS ("Secure corporate payment processes and protocols") are secured by other protocols that prevent fraudulent attacks and this may result in a higher number and especially value of non-SCA payments being in any case protected from fraud (typically corporate payments have higher values than retail customer payments).

As a consequence, overall, higher fraud rates are reported for SCA payments.

Question 4: Do you have any potential explanations why PSUs bear most of the losses due to fraud for credit transfers and cash withdrawals?

Payment service users (PSUs) bear most of the losses due to fraud for **credit transfers and cash withdrawals** because probably the actions that led to these losses are to be attributed directly to the PSU and not to the PSP. For example, even if the PSP has introduced all possible security prevention/detection measures, the **fraud could be connected to incorrect PSU behavior**, e.g. negligence of the customer.

In addition, as mentioned before, **a payment authenticated with SCA by the payer, who is manipulated** and thus victim of phishing, **cannot be considered and is not reported as a "non-authorized"** payment by the PSU. Social engineering frauds are considered as authorized by the payer, unless the pattern used by the fraudster is so complicated that could be difficult to be detected before the authorization took place. Generally, phishing and smishing are events everyone is supposed to be aware of and thus should be able to avoid with a normal degree of care, in line with the obligations set out by Art. 69 PSD2.

The same applies for cash withdrawals, which are possible only with a card and the related PIN, therefore if a cash withdrawal is performed only a few minutes after a card is reported as lost or stolen, this evidences that the PIN was very likely written on the card or next to the card (e.g. in the same stolen bag). In these cases, PSUs bear the loss as their behaviour is considered not in line with Art. 69 PSD2.

Other specific explanations could be related to the **operational limits** for credit transfers and cash withdrawals which are higher than the ones on card payments and therefore losses are more significant; while for **SCT Instant**, given the immediate nature of the payment, it is much more difficult to block the fraudulent transactions in advance or to subsequently recall the transactions when the fraudster has already taken possession of the amount.

Cases in which it is the **ATM** itself which has been **compromised** (i.e.: cameras reading the PIN entry and fork to steal the plastic into the ATM itself), are very rare and some operators adopted the practice of refunding the PSU and bearing the cost of the fraud.

As to **card payments**, the majority of losses are borne by "others", due to chargebacks, or by the PSP. These could also be transactions in which an exception under the RTS was used and/or which are impossible to be recovered through the schemes.

Question 5: Do you have any potential explanations why the percentage of losses borne by the PSUs substantially differs across the EEA countries?

In general, operators agreed with what is stated in EBA DP Para. 57. Indeed, the difference with regards to the notion of "gross negligence" across Member States may have caused differences in their respective national regulatory frameworks. Some operators suggest to define with a higher level of detail, at a European level, **what is intended as gross negligence** and when the PSP has reasonable grounds for suspicion of a negligence by the customer.

In addition, some operators as regards the considerable difference, noticed in the DP, across the EEA countries, give several explanations. Firstly, this fact might be linked to the number of people that use digital and remote channels that is, in turn, correlated to the **different people's culture, awareness, and habits**. Secondly, it might be linked to the **different PSD2 application** (e.g. solutions and preventive/detecting measures implemented) in each country in order to combat fraud.

As to the latter point, some PSPs wondered whether this might depend on the **lack of convergence** on the meaning of the pattern "manipulation of the payer by the fraudster" by the various NCAs and/or national markets, prompting some misalignment from country to country. This might be linked, furthermore, to the possible difference that results from the different application of the opt-outs and funds recovery procedures across countries.

A further explanation for the reason why the percentage of losses borne by the PSUs differs substantially among EEA countries could be found in the different levels of maturity and sensitivity of anti-fraud systems, which also depend on the different amount of investment in solutions and countermeasures to combat fraud and on the varying degrees of awareness (among organization's employees) regarding the issues and challenges raised by frauds.

Question 6: Do you have any potential explanations why the industry has reported fraud losses as having been borne mostly or significantly by "others"?

In general terms, the higher number of actors involved in the payment chain, especially in card payments, leads to greater complexity as each actor has its own policies and contracts, mainly stipulated bilaterally, there is a fragmentation of the payment chain and payment services, so that the exact **distribution of liabilities among parties is more complex**.
As reported by several operators with respect to card payments, a large part of the fraud can be **charged back to the** acquirers, especially because fraud transactions mainly took place in e-commerce without the use of 3D Secure in the reporting periods observed in the EBA DP, or is borne by the card scheme. Therefore, when the liability carrier is the acquirer or the scheme, the relevant data are thus entered under "Other".

Question 7: Do you have any views regarding the observed correlation between the value of fraud and the value of losses due to fraud between H2 2019 and H2 2020?

As regards the correlation observed, the effects of Covid-19 pandemic can be identified in a reduction in the value of individual transactions and therefore in the average value of frauds, but at the same time an increase in fraud losses as **non-digitally native people** with little experience with online transactions have used digital tools as well as carried out purchases on **marketplaces that are not necessarily reliable** (e.g. buy-and-share scams are currently particularly frequent).

In addition, the introduction of new fraudulent scenarios might have had a substantial impact, e.g. scams attacking instruments like, for example, the **Instant Credit Transfer**, which was gradually introduced in the business, allowing fraudsters to quickly monetize the fraudulent transactions. In this scenario, customers usually notice and report fraud late when funds are no longer available. Indeed, due to its instantaneous nature, and to the fact that it is **more difficult to block in advance**, this has led to a higher number of losses.

Further, taking the perspective of an issuer, the fact the two values are not directly proportionate and in sync might depend on the possibility by the Issuer to effectively activate a chargeback (e.g. due to the increasing use of 3DS that does not allow the issuer to recover amounts via chargeback), thus while reporting a gross fraud, the net loss is zero. Typically, there is a **time gap between the fraudulent events, the day the payer realizes it and the refund as a chargeback to the issuer**. This is reflected in reporting and might be a possible explanation of the identified gap.

We would add that the probability for financial institutions to retrieve stolen funds increases in those countries in which there is an active cooperation among organizations. Indeed, according to an analysis carried out on a country-level by the Italian CERTFin co-chaired by Banca d'Italia and ABI, even if focused only on remote credit transfers, it was noticed how the establishment of a strong cooperation protocol recently formalized among financial institutions could facilitate the returning of money stolen by fraudsters.

In fact, CERTFin data show that during 2020 in Italy, despite a great increase in the value of frauds compared to 2019, the value of losses (although it has raised as well, compared to the previous year) did not get anywhere near the same level. Moreover, when comparing the value of frauds that led to the actual losses, the Italian banking sector has shown a great ability to contain the negative effects of frauds thanks both to prevention and detection measures. Data reported to CERTFin by the members of its Constituency corroborates this: with regards to digital banking, the Italian financial sector has proven to be capable of blocking and retrieving the majority of funds stolen by fraudsters (82% in 2020, 47% of which have been returned, thanks to collaboration among financial entities).

Question 8: How do you explain the fact that the manipulation of the payer by the fraudster represents a substantial share of the fraudulent non-remote credit transfers authenticated with SCA? How is this fraud type concretely executed by the fraudsters?

In general, it is worth noting that some customers, **typically of older age**, tend to be **more vulnerable** to manipulation/social engineering and, as mentioned above, those clients were forced in the pandemic to use their online banking instead of using self-service banking directly at the branch. Therefore, in most cases they were the target of the fraudster and as explained above the payers themselves carried out transactions in fraudster's favor.

Non-remote credit transfers authenticated with SCA have high security standards, and often it becomes difficult for a fraudster to circumvent such security systems, including the theft of credentials to be used to carry out payments. The only alternative, or rather, the easier alternative to perform frauds, is that the fraudster deceives the PSU with social engineering techniques and leads the PSU to carry out an operation in his favor. In this case, it is therefore the payer himself who "carries out" the scam and the fraudster acts by convincing and manipulating the payer on a psychological level, but materially the operation is carried out by the payer.

So, a substantial share of the fraudulent non-remote credit transfers authenticated with SCA made with manipulation of the payer is therefore to be attributed to the fact that it is easier to psychologically circumvent PSUs by inducing them to execute a transaction, rather than circumventing technical security systems which would require greater effort and great competence from a technical and IT point of view.

Finally, we would add that for high value fraud a SCT/SCTInst is more suitable to be attacked than a card as it would be more profitable for fraudsters.

Question 9: Do you have any views regarding the types of card payment fraud that have been reported by the industry under the category "issuance of a payment order by the fraudster", sub-category "others"?

It may be possible that this category includes payments performed with a **tokenized card** (e.g. Google-pay, Apple-pay or Samsung/Garmin-pay) or a **family fraud** (flatmates using the card) or **friendly fraud** (unjustified complaints by the cardholder).Moreover, even in cases where the card is associated with a digital wallet, it is possible to perpetrate fraud without taking possession of the card.

Overall, we might suggest that an **enrichment of the codification** could be useful. The current taxonomy seems to assume only physical possession of the card, while fraud can also be carried out by obtaining card data to make non-remote payments instead of the physical card. For example, among the frauds under the label *'issuance of ...*', skimming could be detected (a technique that consists in using card readers that have been suitably tampered with to register and store card data, so that any future charges can be made). Also, "card data theft' could also be present under the category 'non-remote'.