19 April 2022

EBF response to European Banking Authority's Discussion Paper on its preliminary observations on selected payment fraud data under the Payment Services Directive

General remarks

- Overall, the data collected reflects a very low level of incidence of frauds and shows that the safety 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 did not report the corresponding data in the periods under consideration. Therefore, we assume that it would still be too early to draw definite conclusions.
- As a matter of fact, we suggest utmost caution in interpreting the data: the considerations in the Discussion Paper are based on partial information as not all countries have responded, and amongst those providing data, a number of inconsistencies have been identified, therefore any conclusion extracted from the data might not be fully representative. Moreover, the variety of payment services provided to the customers in the different countries and, in particular, those provided in the digital environment, together with the diverse digital adoption are another reason for additional caution in designing any possible change in the current legal and/or reporting frameworks.
- One thing that might not be shown by the fraud data reported is that the huge efforts to fight fraud is bearing fruits, a lot is being done to manage the fraud despite the constant growth of the attacks.
- 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 shows 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 to adopt and/or improve best practices (e.g., maintaining internal white/grey/blacklists, analysing 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 the PSPs. Therefore, given that new types of fraud depend on new attack techniques, we suggest that this area be explored in detail and a regulatory link be made with cybersecurity acts, incident/security guidelines, etc.
- A greater harmonisation among countries is also highly desirable to avoid that fraudsters take advantage from regulatory arbitrage.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

- The EBA GL 2020/01 Guidelines on fraud reporting under PSD2 apply to the reporting of payment transactions initiated and executed from 1st July 2020. These amending Guidelines have been drafted according to Article 16 of the EBA Regulation and in fulfilment of the EBA mandate under Article 96(6) of PSD2. In addition, since January 1, 2022, Regulation (EU) No 1409/2013 on payment statistics ECB/2020/59 has been in force, replacing ECB/2013/43. Therefore, even if we realize that the EBA has its own responsibility as one of the European Supervisory Authorities and the desire to continue to closely monitor developments in the fraud domain, this approach is not in line with the objective of creating a single flow for industry and achieve efficient use of industry resources.
- Indeed, although the fraud statistics based on ECB/2020/59 cannot be compared on a one-to-one basis with the current EBA fraud reporting, in our view ECB reporting does provide sufficient insight into fraud developments and trends. We believe that comments from this EBA consultation could also be useful to understand better fraud trends and could be taken into account along with those of the ECB.

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

It is known that crime is an international activity, handled by international networks that know about the difficulties of tracking money across countries. Therefore, it is not surprising that frauds are more frequent in cross-border transactions compared to the total share of licit cross-border transactions. Physical borders do not exist for fraudsters as they exist for administrative purposes, including crime fighting while payments are benefiting from the integrated market for electronic payments [in euro], with no distinction between national and cross-border payments as key element for the proper functioning of the internal market. At the same time, fraudsters take advantage of national differences to circumvent controls as discussed below.

Clear regulation is needed to help to protect the system against fraud, not only with the security measures as already established in PSD2, but also with prevention/detection measures and recovery of funds dispositions once a fraud is identified, regardless the country of origin and destination of the involved funds. The security measures are mainly consumer protection measures, which are welcomed, but anti-fraud measures should be envisaged to prevent/detect the usage of the payment services for unlawful purposes based on those consumer protection measures.

Cross-border card payments have historically had higher fraud rates or shares than domestic transactions. The Discussion Paper notes that the share of fraud in card issuer volumes outside the EEA is three times higher than the share inside the EEA and 85 times higher than in domestic transactions.

These findings are consistent with previous analysis such as the European Central Bank's Seventh report on card fraud[1], UK Finance's Fraud - The Facts 2021[2] and the 2020 annual report of Banque de France's Observatory for the Security of Payment Means[3].

In our view the data collected reflect a very low level of prevalence and show that the safety measures taken by European PSPs are sufficient. We would like to note that the PSD2 SCA regulations have only been in force for a short time (especially for card payments), and reporting was not possible for the periods under consideration. Therefore, we assume that it would still be too early to draw definite conclusions.

Generally, many losses may result from cross-border e-commerce: remote fraudulent card transactions predominantly occur on a larger scale, with fraud attacks, phishing, smishing, targeting larger customer/card groups and therefore significantly increasing the numbers.

[1] Source: Seventh report on card fraud, European Central Bank, 2021. https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html#toc9

[2] Source: Fraud – The Facts 2021, UK Finance, 2021. https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021.

[3] Annual Report of the Observatory for the Security of Payment Means 2020, Banque de France, 2021. https://www.banque-france.fr/en/liste-chronologique/annual-activity-report

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

Cross-border frauds may have a greater chance of success in countries where PSD2 does not apply, i.e., extra-EEA countries, and therefore security measures may be less effective.

Indeed, 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.

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. 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. Fraudsters wish to reduce traceability and recovery possibilities which is easier with cross-border transactions.
A good example of the above is fraud committed against PSUs, deceived with the possibility of investment into cryptocurrencies. The operation of "fraud factories," committing fraud to the detriment of the PSUs by means of telephone fraud (spoofing), in large volume, is more advanced, in which case the beneficiary accounts are almost always outside the country of the origin of funds, which the perpetrators withdraw in cash.

The perpetrators of the crime believe that the crime will go unpunished because:

- there is a great distance between their place of residence and the place of the crime.
- they will be unidentifiable behind IT tools.
- investigative authorities are powerless against perpetrators abroad due to long distance, lack of co-operation and inadequate co-operation.

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. SCA exemptions may have an impact on the fraud rates. On the acquirer side, two reasons can explain the high share of cross-border fraud:

- Higher number of non-EU merchants compared to European merchants and therefore higher incidence of e-commerce transactions (e.g., USA and China).
- In case of non-European transactions, the one-leg principle applies, which potentially reduces the security of the transaction.

In addition, we believe that the following aspects may contribute to higher levels for fraud on cross-border payments:

- For online card transactions, the merchant's country is not always clear for issuers, certainly if the logging of fraudulent transactions happens manually (e.g., merchant PayPal Singapore is in fact not located in Singapore, but in EEA). Therefore, data limitations can also impact this report.
- Skimming usually happens outside EEA, in countries where the chip is not yet used.

With specific regard to **card-present cross-border transactions**, the Covid-19 pandemic considerably reduced travel and especially the use of business cards. Non-remote fraudulent card transactions usually occur on an individual customer basis, e.g., card and PIN are stolen and fraudulently used, but not on a larger scale. Mostly these cards then are used for fraudulent cash withdrawals. It sounds plausible that the fraudulent cash withdrawal amount for cross border is higher because card theft happens more often while customers are travelling. Furthermore, outside of EEA ATMs can be less secure: they can accept cards by reading the magnetic stripe only, which can result in increased fraud.

Regarding **credit transfers**, 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"?

The paper already points to the fact that the reporting period still benefited from the supervisory flexibility the EBA had granted and during which there was a low level of industry readiness in the card-based e-commerce environment.

A clear sign of the criminals' behaviour is the shift from security breach methods to social engineering techniques, as they now target customers instead of remote systems' transactions. More flexibility should be granted to PSPs concerning the methods to apply strong customer authentication and to grant security to their customers' transactions, and support in order to implement more preventive [collective] measures.

Generally, fraud patterns using malware or viruses are limited to "organized" hackers or groups. Following the introduction of PSD2, it became more difficult to perform fraud due to SCA and dynamic linking required for authorisation. 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. In these cases, it is the client who is authorising 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 and/ 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 cases, the fraudster masks the caller's number by pretending to be the PSP and once 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, also directly involving 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 the "volume of transactions in millions" and "Average 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.

As to **cards payments**, for non-remote card fraud, it is mostly individual cases, theft of card and PIN and cash withdrawal with high amounts, whereas for remote card fraud it is mostly bulk cases/fraud attacks with card data obtained from hacking and phishing for high velocity/low value amounts which are hard to distinguish from high velocity genuine transactions. However, an evaluation of the card losses for the year 2020 and thus before the obligation to perform SCA makes little sense. Evaluations from the second half of 2021 onwards would be more appropriate. Furthermore, for non-remote / card present transactions, contactless transactions allow the card to be easily used at POS terminal also by non-cardholders (within the limits of contactless payment thresholds of course).

For cash withdrawals, we have seen a decline in skimming attacks for some time, cases occur particularly outside the EEA. Average loss amounts are typically higher than for card payments. 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. Also, customer negligence of exposing the PIN is an issue. It is worth noting however that the share in volume of cash withdrawals reported

fraudulent are very low compared to the volume of remote/non-remote purchases transactions reported fraudulent.

For **credit transfers**, we see that cases are less frequent but with higher fraud amounts, as the payer is often manipulated by social engineering attacks. Typically, this includes CEO fraud, business email compromise or phishing. Higher spending limits apply to credit transfers (compared to card payments) and therefore the fraud 'revenue' is also higher. For example, the limit for a debit card at an ATM may be € 1,000, while for a credit transfer it may be € 10,000. A difference in limits between a retail customer and a business customer should also be taken into account. For businesses, the limit is usually higher due to operational considerations. Here we would like to highlight that the category "manipulation of the payer" mainly covers cases of social engineering and therefore is not indicative of the security of the underlying payment systems and processes.

For credit transfers, customer education and ways to prevent social engineering could be further explored. It can be assumed that Covid 19 outbreak's negative effects have impacted the fact that an increased volume of PSUs is chasing or easily believing promises for "good bargains" and "quick investment profits", despite the security & fraud awareness tips offered, both nationally and by PSPs. Investment (especially cryptocurrency) and impersonation scam activity has increased significantly in recent years both in terms of attempts made by fraudsters to contact potential victims (online or by phone) and in volume and value of fraud committed.

Furthermore, the data on initiation channel breakdown for credit transfers may be distorted by the fact that there is no data from France or Germany in the analysis. These countries accounted for 37% of electronic credit transfers and 24% of paper-based credit transfers in 2020, according to ECB data. For France, the Observatory for the Security of Payment Means found that credit transfers involving paper-based transfer initiation had a higher fraud rate or share (0.0018%) in 2020 than credit transfers initiated via the Internet or mobile banking (0.0012%). However, the fraud share will fluctuate over time and vary across countries.

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?

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. Fraudsters focus more on SCA credit transfers because they are – on average – more profitable due to the higher amounts involved. Moreover, it seems to be easier for fraudsters to deceive customers and obtain the complete credentials than to break through the banks' systems.

Additionally, even if SCA is a quite secure authentication/authorisation 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 him/herself. 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 (spoofing) or the alias of the sender of an email or an SMS (Swap alias), typically pretending to be the payer's PSP, are all techniques implemented by fraudsters aimed at the theft of 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).

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.) 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. Payments that do not benefit from exemptions from SCA are more likely to be higher value, one-off transactions. 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 behaviour, e.g. gross negligence of the customer referring to art 74.1 PSD2:

"The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence".

According to art. 73 in case of an unauthorised payment transaction, the payer's payment service provider refunds the payer the amount of the unauthorised payment transaction immediately, after noting or being notified of the transaction.

Concerning credit transfers, as shown in figure 10, about half of the fraudulent credit transfers are authenticated with SCA. The figure 11 shows % of the values of fraudulent remote credit transfers authenticated with SCA. The two figures together suggest that most of the transactions has been authenticated by the users and correctly executed. For authorised transactions, PSD2 allocates liability of the PSP to the correct execution of the

payment transaction in accordance with the payment order of the payment service user. In such cases, if the funds involved in a payment transaction reach the wrong recipient due to an incorrect unique identifier provided by the payer, the payment service providers of the payer and the payee are not obliged to cooperate in making reasonable efforts to recover the funds including by communicating relevant information. Unfortunately, the rule imposing that it is not possible to debit the amount incorrectly received without explicit consent of the account holder does not always facilitate the task and despite the cooperation and efforts deployed by the payer's PSP and the payee's PSP funds cannot be recovered. Clear dispositions are required to facilitate the recovering of those funds when a fraudulent transaction is involved.

In addition, as mentioned before, a payment authenticated with SCA by the payer, who is manipulated, 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 who 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. There is a shift and escalation from non-authorised payment fraud to authorised payment fraud (the so-called Authorised Push Payment Fraud)"

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, we agree with what is stated in the Discussion Paper paragraph 57. Furthermore, we suggest defining 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.

As regards to the differences across EEA countries, there can be several explanations. The first explanation for any difference can be the different habits and behaviours by users across countries and different payment services provided according to different market demands or expectations. Maturity of the electronic payment services market, digital adoption, and the way each of payment services is offered to users can also explain those differences. More information is needed to reach any conclusion, such as average amount for the relevant payment instrument per country, and average losses per instrument and per country would allow to better analyse the differences. Secondly, it might be linked to the different PSD2 implementations (e.g., solutions and preventive/detecting measures implemented) in each country in order to combat fraud. We also wonder 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. Also, different reimbursement policies may explain these differences as those are different among banks, probably also among countries.

There could be also the case that technical controls may differ across countries (multilayer cybersecurity and anti-fraud controls).

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, indeed, a fragmentation of the payment chain and payment services, so that the exact distribution of liabilities among parties is more complex.

For card payments a large part of the fraud can be charged back to the acquirers, especially because fraud transactions mainly take place in e-commerce without the use of 3D Secure in the reporting periods observed in the Discussion Paper 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?

The timeframe for analysis is short and it would be prudent to review the data over a longer time series and across more countries. As the EBA notes, the loss liability may only be accounted for with a delay after the fraud occurred. Also, the speed and the extent to which funds are recovered or the final liability is established may vary.

As regards the correlation observed, the effects of Covid-19 pandemic can be detected in a decrease in the value of 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). As security measures also develop and have an impact on the different types of fraud, fraudsters are shifting to more high value types of fraud. If these fraud attempts are executed successfully more money is obtained.

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, 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.

Finally, 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.

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 favour.

The manipulation of the payer by the fraudster are social-engineering frauds (e.g., investment fraud, bank help desk fraud, invoice fraud, WhatsApp fraud, bitcoin fraud, etc.)that are harder for the PSPPSPs to detect & stop. Hence, the higher rate of frauds. Considering the most frequent scams, once the social engineering for the scam has yielded

fruit, it is not surprising that the user makes the transaction even if it requires a non-remote ordering.

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/her favour.

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.

While manipulation of the payer is mainly associated with remote communication (phone, SME messaging, social media, or email) and remote payments (such as online or mobile banking or card not present payments), the victim may also make a payment via a bank branch. Figures from UK Finance indicate that 9.4% of the value of authorised push payment fraud in the UK in 2020 was initiated in branches, down from 10.8% in 2019.

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"?

We see the following possible explanations:

- 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.
- Other fraud types such as identity theft (third-party application fraud or account takeover).
- Unauthorized Card Not Present fraud for remote transactions, where the fraudsters gains card/customer data through data breaches, hacking of data, bought in the dark web, skimming, etc being reported in this category.
- Phishing in 'issuance of a payment order by the fraudster' is not "lost or stolen cards, counterfeit cards, of cards not received" and by consequence reported as others.
- Subcategory "others" is reported whenever facts are unclear (e.g., the customer cannot explain the loss of his/her authentication instruments)
- It is sometimes difficult to exactly determine what occurred during a fraud case. Issuance, modification, and manipulation can usually only be determined based on the story told by the PSU. If this is not clear it is determined that a fraud did occur. However, if no clear fraud type can be established, it is classified as 'others.'

About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure, and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses, and innovators everywhere.

www.ebf.eu @EBFeu

For more information contact:

Anni Mykkänen
Senior Policy Adviser - Payments and Innovation
a.mykkanen@ebf.eu

+32 2 508 37 32