Svenska Bankföreningen
Swedish Bankers' Association

2022-04-19

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

The Swedish Bankers' Association welcomes the opportunity to participate in EBA's consultation and indeed appreciate the initiative to invite the market to a discussion about the outcome of fraud reporting under PSD2.

Question 1: Do you have any views on the high share of cross-border frauds in the total volume of fraud?
Payments outside EEA shows the highest fraud rates, and an obvious reason for that is that SCA is not required and can often not be applied. Cross-border transactions have always shown higher fraud rates than domestic payments for several reasons, and that has not changed by the SCA requirement.

Fraud rates are higher for cross-border transactions in relation to domestic transactions. This is explained by the vast difference in the number of transactions, both fraudulent and legitimate. The majority of actual fraudulent transactions are made domestically, however this also applies for the legitimate transactions. Hence, the large number of fraudulent domestic transactions is not as easily visible in the fraud rate.

The reasons for cross-border payments showing higher fraud rates are:

- E-commerce fraud is cross-border by nature and especially big tech companies are used for fraudulent card transactions. Big tech companies reroute card transactions via multiple EEA and Non-EEA countries and often applies exemptions (MIT, recurring) if in EEA.
- Criminal groups which execute fraud payments are located in non-EEA country and/or using non-EEA payee.
- Some Cross Border-2-leg Merchants allow for card transactions using PSD2 exemptions even though they should not be applied. These decisions drive fraud.
- Fraudsters typically want to avoid surveillance and KYC process which often means that checkout for card transactions in other countries than victims' location is preferable.
- There are also situations in which local criminal groups attempt to make it more difficult to trace the funds by utilizing mule accounts in other countries.
- Social engineering is the most representative fraud type behind cross-border credit transfers. This is likely due to this being the most effective fraud modus

for payment fraudsters to succeed in transferring funds abroad (in contrast to e.g., marketplace fraud, that is more common domestically).

We want to highlight that the fraud rates much depend on how strong presence that international organizations behind the scam have in the country. It also depends on the services provided, i.e., how easy it is to get access to cross-border services.

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

Fraud in payments initiated non-electronically (MOTO and other paper-based): For credit transfers the fraud share in non-electronic payments is lower than for electronic payments. For card payments the fraud share in non-electronic payments is higher than for electronic payments. (Although in both cases non-electronic payments stand for a small share of total payments). Why?

- For non-electronic payments, there is no SCA requirement, therefore it would be logic for fraud rates to be higher for non-electronic payments initiated through the payee, as for card payments. For cards, the MOTO flag is sometimes used by merchants for remote payments in cases where the SCA requirements are avoided, for example in the travel industry**.**
- Non-electronic credit transfers would mainly be payments initiated by the payer inside the bank premises, where the bank customer would need to verify his/her identity e.g. with a passport or id-card. This explains why non-electronic credit transfers show less fraud than electronic credit transfers. Non-electronic credit transfers could also be credit transfers initiated through telephone order or paying bills by post, which is probably not an attractive solution for fraudsters as the modus operandi does not scale.

For cash withdrawals, fraud rates are higher for credit and charge cards than for debit cards, with regards to both volume (transactions) and value. Why?

- Credit and charge cards often have higher spending limits, which makes them more attractive for fraudsters and makes higher withdrawals possible.
- As stated in point 27, fraud is higher for cross-border withdrawals than for domestic withdrawals. In Member States with domestic schemes, these schemes dominate the debit card market in the country and are not possible to use outside the country if not co-badged. Credit cards are typically always internationally branded allowing for cross-border transactions.
- The reason that relative cash withdrawal fraud rates are higher in credit and charge cards is because debit cards are more commonly used in genuine cash withdrawal. Relatively smaller genuine credit card use in cash withdrawal lifts fraud rate.

Fraud rate for card payments with and without SCA:
As expected, fraud rates for card payments are substantially higher without SCA than with SCA. The misuse and bad transaction flagging on possible SCA exceptions is loading the good legal SCA exemption opportunities with undeserved fraud. The better legal usage of exemption will reduce fraud levels as is the aim of having PSD2 exemptions.

Occurrence of the different types of fraud:

A general comment is that there might be different interpretations by different card issuers in which report categories different card fraud types should be reported. This could relate to modus operandi such as e.g. cards account testing and BIN attacks. In these modus operandi fraudsters get access to card data by using software and testing issuers BIN ranges. In account testing they execute a low value payment to validate the card and in case of BIN attacks fraudsters execute fraudulent transactions. Further examples are:

- Non-remote: nightclub cases, holiday destination cases where merchants add zeros to the total value of the bill.
- Remote: subscription scams, investments scams, romance scams**.**

For remote card payments (CNP) the most common fraud type is theft of card details. EBA says "This can be explained by fraud arising from social engineering such as phishing. In these instances, the authentication with SCA may not be effective in preventing such type of fraud."

A general comment is that it is premature to draw such conclusions, since the SCA requirement was not in force in practice for remote (e-commerce) card-based payments before 1 January 2021 and has therefore not affected the reporting periods included in the report.
However, we believe that SCA has a significant impact on reducing e-commerce card payment fraud, including theft of card details. Theft of card details, indicates theft of card data, i.e. PAN + Expiry Date + CVC without actually steeling the physical card (which would be categorised as Lost and Stolen). The theft of data does not necessarily need to include also SCA credentials. Card data breach by hacking merchants or using software for cards account testing is the main reason for the theft of card details. However, in these attacks, fraudsters cannot get access to the cardholders' authentication methods and therefore SCA is effective in preventing fraud.
Solid SCA methods used for remote card payments, such as the Mobile BankID in Sweden, would not be exposed to fraudsters in relation to theft of card details. For such a card, the fraudster would need to get hold not only of the card details, but also the physical possession of the mobile phone of the cardholder, AND both the screen-lock code to the device AND the separate PIN code of at least 6 digits exclusively used in the Mobile BankID.

Having said that, not all fraud will be prevented by SCA. It is common that fraudsters use social engineering, especially phishing to obtain victims payments details which can include authentication methods. Other authentication methods that are not as secure as Mobile BankID could be easier to misuse. This could e.g. be the case for fraudulent enrolment to BigTech apps.

For non-remote card payments (CP): According to the data that our members report, it is surprising that counterfeit stands for 20%. Although EBA states CP is a small share already of the total fraud, and the counterfeit share is therefore a small share of a small share, this percentage is still surprising.

One of the driving factors for manipulation of the payer being more common with credit transfers relative to card payments, is that contact between the fraudster and

victim, when it comes to card fraud, is not necessarily same as for credit transfers. Hence, there is no need to manipulate the payer, leading to a higher percentage of this fraud type for credit transfers. Although the fraud rate for credit transfers is relatively low, the average value of a fraudulent credit transfer is higher than for other payment instruments. This means that credit transfer frauds compared to fraudulent transactions with other payment instruments still have a significant effect on an individual level when they actually occur.

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?

EBA offers two possible explanations:

1) When exemptions are used for CTs, the transactions are already deemed low risk and therefore should also result in lower fraud. There is some merit to this theory and a good illustration to the difference in using exemptions by the payer's PSP for push payments (where the payer's PSP is in full control of both SCA and exemptions, no involvement of the payee and the PSP of the payee) with card payments where both the possibility to use SCA and the circumstances surrounding an exemption is dependent on actions by the payee.

2) That the fraud in CTs "might be due to spoofing, authorized push payments and transactions initiated by the account holders after social engineering from the fraudsters, such as phishing." We believe this is the major explanation. Then EBA states that social engineering might also happen for other payment instruments, and so this cannot be the full explanation. But referring to Figure 10 in the DP, which shows that Manipulation of the payer is almost 50% of fraudulent CTs with SCA, but only 7% for card payments reported by issuers, and 0% for card payments reported by acquirers and for cash withdrawals, it is obvious that this is much more frequent for credit transfers. And for these cases where the payer is manipulated, SCA is not an obstacle for the fraudster as the fraudster manipulates the payer to authorise and authenticate for a payment that the payer does not want to do. It should be noted though that SCA still plays an important role also to limit the extent of the fraud cases where the payer is manipulated by the fraudster: In these cases when SCA is applied, the fraudster needs to do a new manipulation of the payer for each fraudulent transaction. Whereas if exemptions are applied, an initial payment with SCA where the payer has been manipulated by the fraudster, could then easily be followed by subsequent fraudulent transactions that are exempted from SCA and for which the fraudster does not need to initiate further manipulation events with the payer (e.g. Trusted beneficiaries exemption).

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

Compared to card payments, SCA is more commonly used for credit transfers and always for cash withdrawals, whereas exemptions are used more for card payments. When SCA is not applied, the PSU must always be reimbursed, according to PSD2

Article 74. By that logic, it is only when SCA has been used, that the PSU can get to bear the losses. As observed in previous question, for credit transfers fraud rates are higher with SCA than without SCA, whereas the opposite is the case for card payments. As there is a higher degree of fraud payments with SCA for credit transfers, credit transfers have a higher proportion of fraud for which the payer has made an SCA and can be held liable.

As also observed, for credit transfers almost 50% of the fraud is due to manipulation of the payer – i.e. the payer has actually authorised the payment, although manipulated to do so, and this type of fraud is not included in what PSD2 denotes as "non-authorised transactions" and therefore the rules on consumer protection for non-authorised payments in PSD2 does not directly apply to these transactions, and the payers therefore need to take liability v/s the PSP to a higher degree for the transactions that they have in fact authorised.

Question 5: Do you have any potential explanations why the percentage of losses borne by the PSUs substantially differs across the EEA countries?
Consumer protection law has various emphasis and interpretations across the EEA countries. Interpretation of gross negligent behaviour also varies. Consumer protection rights in relation to this should be mainly the same, as that has been the objective with PSD2 to harmonise the rules across Europe, but interpretation in case law of what constitutes "gross negligent" and just "negligent" may differ.

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

All fraud losses are born by the PSPs or the PSUs. In most payments there are two PSPs and two PSUs. In the fraud reporting, the PSP will report losses as born by either themselves or by their own PSU, and the losses born by the other PSP and its PSU will be reported as born by others.

As observed by the EBA, the category of "other" bearers consists of acquirers and merchants for card-based payments reported by card issuers. For acquirers, the category of "others" consists of issuers *and cardholders* (note that in the acquirers' reporting the PSU is the payee, i.e. the merchant). The split of losses as reported by issuers (65% on the payer/payer's PSP, 35% on the payee/payee's PSP) therefore fit rather well with the split of losses as reported by acquirers (70% on the payer/payer's PSP, 30% on the payee/payee's PSP). The observed difference in the split as reported by issuers (65/35) v/s the split as reported by acquirers can probably explained by different shares and sets of one-leg transactions in the data reported by issuers and acquirers, respectively – it should be noted that in this context "one-leg" would include not only payments to/from non-EEA countries but also payments to/from EEA countries not included in the report.

From the report it is evident that for transactions with the liability on the payee side, the PSU (the merchant) and not the PSP (the acquirer) bears the liability in the vast majority of cases. This is due to the liability and risk level being subject to a business

agreement between the acquirer and the merchant. E-commerce merchants are often provided by their acquirer with a choice of accepting card payments with different degrees of support for SCA/3-D Secure, i.e. accepting higher risks of charge-backs in order to achieve a more "frictionless" checkout experience. This would include utilising allowed acquirer exemptions under the RTS, but it should be noted that as the data in the report is reported under the extended "supervisory flexibility" for e-commerce card payments until 31 Dec 2020, the reported data will still include large shares of merchants having chosen not to support 3-D Secure at all and accepting the risks of charge-backs on transactions without SCA, which should not be possible after the supervisory flexibility has extended and the RTS is truly in force.

Differences between countries in the issuer reporting can be explained by differing costs of making chargebacks (e.g. if the facility is in-house or out-sourced). In countries where issuers in general have higher costs of making charge-backs, this will result in a higher degree of fraudulent transactions being written off by issuers without being charge-backed to the acquirer, in cases where the cost of processing the charge-back would supersede the disputed transaction value. In turn, this result in a lower degree of losses being born by others, i.e. acquirers and merchants.

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 EBA states, this can be due to initial reporting issues and losses appearing in another period than the actual fraud, so further monitoring of this when more reporting is done is needed. We also believe it is important to include the acquirer reporting in the further monitoring and analysis.

Also, as EBA explains that H1 2019 has been omitted in this context due to having identified substantial data quality issues for this period, some of these issues might still remain for H2 2019, which could explain the substantially larger gap between fraud and fraud losses in this period than in the other reported periods, in turn resulting in an illogic negative correlation between fraud and losses between H2 2019 and H1 2020.

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?
Non-remote credit transfers SCA is an odd concept in the Nordics, we do not know about any such cases in Sweden. The question is not applicable for Sweden.

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"?
The concept of classifying some fraud cases as either "Modification of a payment order by the fraudster" or "Manipulation of the payer to make a card payment" are new to the card infrastructure and support for such fraud type classification has just

recently been added to the card scheme fraud handling infrastructure. It can therefore be that much fraud cases that should be in either “Manipulation of the payer to make a card payment” (non-remote: nightclub cases, Remote: subscription scams, investments scams, romance scams.) or “Modification of a payment order by the fraudster” (holiday destination cases where merchants add zeros to the total value of the bill.) are still reported as “Other” although they should clearly not go under “Issuance of a payment order by a fraudster”.

Another explanation might be that the fraud types “Modification of a payment order by the fraudster” or “Manipulation of the payer to make a card payment” according to the card schemes only should be used in transactions issued and acquired in the EEA. Therefore, card issuers might use the category "Other" when referring to transactions outside the EEA.