EBA/DP/2022/01

17 January 2022

Discussion Paper

on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry

Contents

List of figures

Abbreviations

DP	Discussion Paper
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
EU	European Union
NCA	National Competent Authority
PIS	Payment Initiation Services
PSD2	Second Payment Services Directive
PSP	Payment Service Provider
PSU	Payment Service User
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SCA&CSC	Strong Customer Authentication & Common and Secure Communication

Responding to this discussion paper

The EBA invites comments on all the proposals put forward in this discussion paper (DP) and, in particular, on the specific questions included herein. Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed / rationale proposed.

Submissions of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 19 April 2022. Please note that comments submitted after this deadline or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found in the legal notice section of the EBA website.

Executive Summary

The Revised Payment Services Directive (PSD2) requires all payment service providers in the EU to report payment fraud to national competent authorities (NCAs), and for NCAs then to provide the EBA and the European Central Bank (ECB) with statistical data on fraud relating to different means of payment. In 2017, the EBA issued Guidelines detailing the reporting requirements under PSD2 (EBA/GL/2018/05). The data is provided by the NCAs to the EBA in the form of reports on a biennial basis and includes the aggregate volumes and values of all payment transactions and their subsets of fraudulent transactions. This is done for a wide set of payment instruments and thus goes beyond the card payments fraud collected and reported elsewhere.

Based on the reports thus submitted by NCAs, the EBA has assessed the fraud data related to four reporting periods: H1 2019 (i.e. the first half of 2019), H2 2019, H1 2020 and H2 2020. This DP provides the preliminary observations of the EBA in relation to selected subsets of the data received, with the aim to obtain feedback from external stakeholders on said observations and the emerging patterns. The qualitative inputs collected will support the EBA in deriving meaningful insights from the more comprehensive data that the EBA will receive, and that may be published, from 2022/23.

The first chapter of the DP explains the methodological approach chosen by the EBA, including the EBA's aim to present data that is reliable and consistent, which led to the decision to exclude some data from the scope of this publication due to quality issues, pending resolution of those issues. The preliminary observations provided in this DP are thus based on a sample of countries that does not cover the entire EU payment market.

The DP then continues by presenting some patterns that the EBA observed for said data, for the most part focusing on the most recent reporting period of H2 2020, in other cases spanning all four reporting periods. These offer a general picture of the nature and the occurrence of fraudulent payments depending on where the payments originated, the payment instruments used and the transaction's operational modalities, such as the use of a remote channel or the authentication with SCA.

The DP concludes by also highlighting emerging patterns that the EBA considers not to be immediately intuitive or plausible, or that diverge from the general trends. For these instances, the views from external stakeholders would be particularly beneficial. This feedback will contribute to a sound interpretation by the EBA of future reports it will receive on fraud data.

Next steps

The EBA invites stakeholders to respond to the 9 questions included in this DP by the 19 April 2022.

Background and rationale

Background

1. Article 96(6) of the revised Payment Services Directive (PSD2)[1] requires Member States to "ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities". These NCAs are further required "to provide the EBA and ECB with such data in an aggregated form".

2. Based on these requirements, the EBA, in close collaboration with the ECB, issued Guidelines on fraud reporting under Article 96(6) of the PSD2 (thereafter "the EBA Guidelines"), which set out the semi-annual reporting of payment and fraud data from PSPs to their NCAs, as well as the reporting of aggregated information from the NCAs to the ECB and EBA[2]. The Guidelines were published on 18 July 2018 and apply as of 1 January 2019.

3. The first reporting of data under the Guidelines took place at the end of 2019 for data corresponding to the first six months of 2019 (H1 2019). Finally, the EBA Guidelines were amended on 22 January 2020 (EBA/GL/2020/01) to mainly incorporate minor clarificatory amendments to the reporting tables, with the amended version applying to the reporting of payment transactions initiated and executed from 1 July 2020 onwards.

4. Based on the reports submitted by NCAs under these Guidelines, the EBA has assessed the fraud data related to four reporting periods: H1 2019, H2 2019, H1 2020 and H2 2020. This DP provides the preliminary observations of the EBA in relation to selected subsets of the data received, with the aim to obtain feedback from external stakeholders on said EBA's preliminary observations.

5. The EBA is interested in the views of the PSPs that provided the original data, but also in the views of other interested stakeholders, such as trade associations, consulting firms, academics, and anyone else that deem themselves in a position to offer complementary explanations for, and views on, the patterns identified.

6. The qualitative inputs collected in the context of this DP will support the EBA in deriving meaningful insights from any the comprehensive data that may be published from 2022/23 onwards, and that can potentially be used by the industry, the NCAs, and by the EBA for assessing whether the security and fraud related requirements set out in PSD2, and complemented by EBA legal instruments, have achieved their expected aim of enhancing

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no 1093/2010, and repealing Directive 2007/64/EC.

[2] EBA/GL/2018/05.

security and reducing payment fraud. The collected inputs are also expected to support the ECB and the national central banks in the achievement of their respective tasks.

Rationale

7. The DP presents some preliminary trends identified by the EBA across several different payment instruments, for a large number of EEA Member States, and half-yearly reporting periods that end on 31 December 2020. As such, it supplements other publications on payment fraud, such as the ECB's regular report on card fraud, which focuses on card payment fraud and does therefore not cover other payment instruments, is based on a different sample of countries, and covers reporting periods that go back longer in history but also end on 31 December 2019. As a result, the data presented in the DP cannot be readily compared with the findings presented in said ECB reports[3].

8. In what follows below, the rationale section sets out the methodological approach applied by the EBA and, the data limitations faced; and presents a number of observations, with 9 questions distributed across the document.

[3] See the seventh report on card fraud published in October 2021.

Methodological approach and data limitations

9. The present preliminary observations draw on data reported under the EBA Guidelines for four reference periods: H1 2019, H2 2019, H1 2020 and H2 2020. The quality and completeness of the reported information has continued to improve over the four reporting periods, as a result of increasing familiarity of the reporting PSPs with this data collection, along with data quality management efforts from the ECB, EBA and NCAs. Nevertheless, several data limitations persist, which need to be taken into consideration when aggregating and assessing the data across countries and periods. These are outlined below.

10. First, the geographical scope of the dataset is incomplete and inconsistent across the reporting periods, as several NCAs decided to comply with the EBA Guidelines on fraud reporting with a delay, inter alia to implement them at the same time as the revised ECB Regulation on payment statistics from 2022. The EBA exceptionally accepted this approach in order to benefit from synergies and facilitate relevant compliance with applicable requirements, and as a result, not all NCAs have reported data for all reporting periods in 2019 and 2020. Further, several countries are not EU Member States, which were required to transpose the underlying Directive by January 2018, but are EEA Member States that may have chosen to transpose the Directive at a later stage.

11. Second, the EBA excluded from the scope of this DP the countries for which no data has been received for any of the four reporting periods as well as the reports submitted in a format other than the one specified in the Guidelines. The EBA also excluded from the scope the reports in which substantial sets of data were missing or in which the EBA identified significant outlier figures (presumably due to reporting errors).

12. On this basis, the sample of countries that the EBA included in the DP observations of for the H2 2020 reporting period comprises 18 EEA countries: BE, BG, EE, EL, ES, FI, HR, HU, IE, IT, LV, NO, PL, PT, RO, SE, SI and SK. The EBA considers the figures provided by these countries to be sufficiently consistent.

13. Additionally, some observations across the four reporting periods are reflected in the subsequent chapters, but only for a subset of 14 EEA countries for which the data was reported across those periods in a reliable manner and with sufficient quality. This sample of countries comprises BE, BG, EE, EL, ES, FI, HR, IE, IT, PT, RO, SE, SI and SK.

14. Also, in this first publication of the EBA on payments fraud, the observations focus on the data on credit transfers, card payments (reported by both issuing PSPs and acquiring PSPs) and cash withdrawals, thus making data available for two additional instruments than the card payments that are usually reported on.

15. The fraud data on transactions initiated by PIS providers have been particularly poor and often implausible, suggesting that PIS providers are not compliant with applicable requirements, which the EBA will further investigate.

16. Based on the methodological approach outlined above, this DP is structured as follows: in the first substantive chapter below, some patterns are presented that can be derived from the available dataset. The subsequent chapter then highlights other patterns that appear not to be immediately intuitive and that cannot be plausibly explained by the EBA and the NCAs, and for which the comments from market stakeholders would be particularly beneficial.

Patterns emerging from the selected data

17. This chapter provides an overview of the patterns that can be derived from the selected fraud dataset collected as per the EBA Guidelines.

Fraud rate per payment instrument

18. The fraud rate expressed in terms of total volume and total value of all payments differs significantly between the selected payment instruments as depicted in Figure 1 for the reference H2 2020 period.

Figure 1: Selected fraud figures reported for H2 2020, per payment instrument

Payment instrument	Volume of transactions in millions	Value of transactions in € bn	Fraud rate in % of total volume	Fraud rate in % of total value	Avg. fraud amount per transaction in €
CARDS (ISSUERS)	15,671	744	0.0163	0.0252	73
CARDS (ACQUIRERS)	16,597	564	0.0345	0.0458	45
CREDIT TRANSFERS	6,175	27,199	0.0012	0.0011	4,191
CASH WITHDRAWAL	1,719	320	0.0020	0.0048	459

19. As shown in the figure above, for the most recent reporting period of H2 2020, credit transfers are the payment instrument for which the fraud rate is the lowest, both in terms of volume and value, while card payments reported by acquirers are the payment instrument for which the fraud rate is the highest. More specifically, the fraud rate for H2 2020 reporting period ranges from 0.0012 % of the total volume of credit transfers to 0.0345 % of the total volume of card payments reported by acquirers, i.e. a rate that is 29 times higher than that for credit transfers. Also, the fraud rate in the same period ranges from 0.0011 % of the total value of credit transfers to 0.0458 % of the total value of card payments reported by acquirers, i.e. a rate 42 times higher.

20. While the fraud rate for credit transfers is relatively low, the average value of a fraudulent credit transfer amounts to € 4,191, which is substantially higher than the average amounts per fraudulent transaction observed for the other payment instruments. Nevertheless, the average value of a fraudulent credit transfer is lower than the average value of a credit transfer, which amounts to € 4,404 on the basis of the reports included in the DP observations.

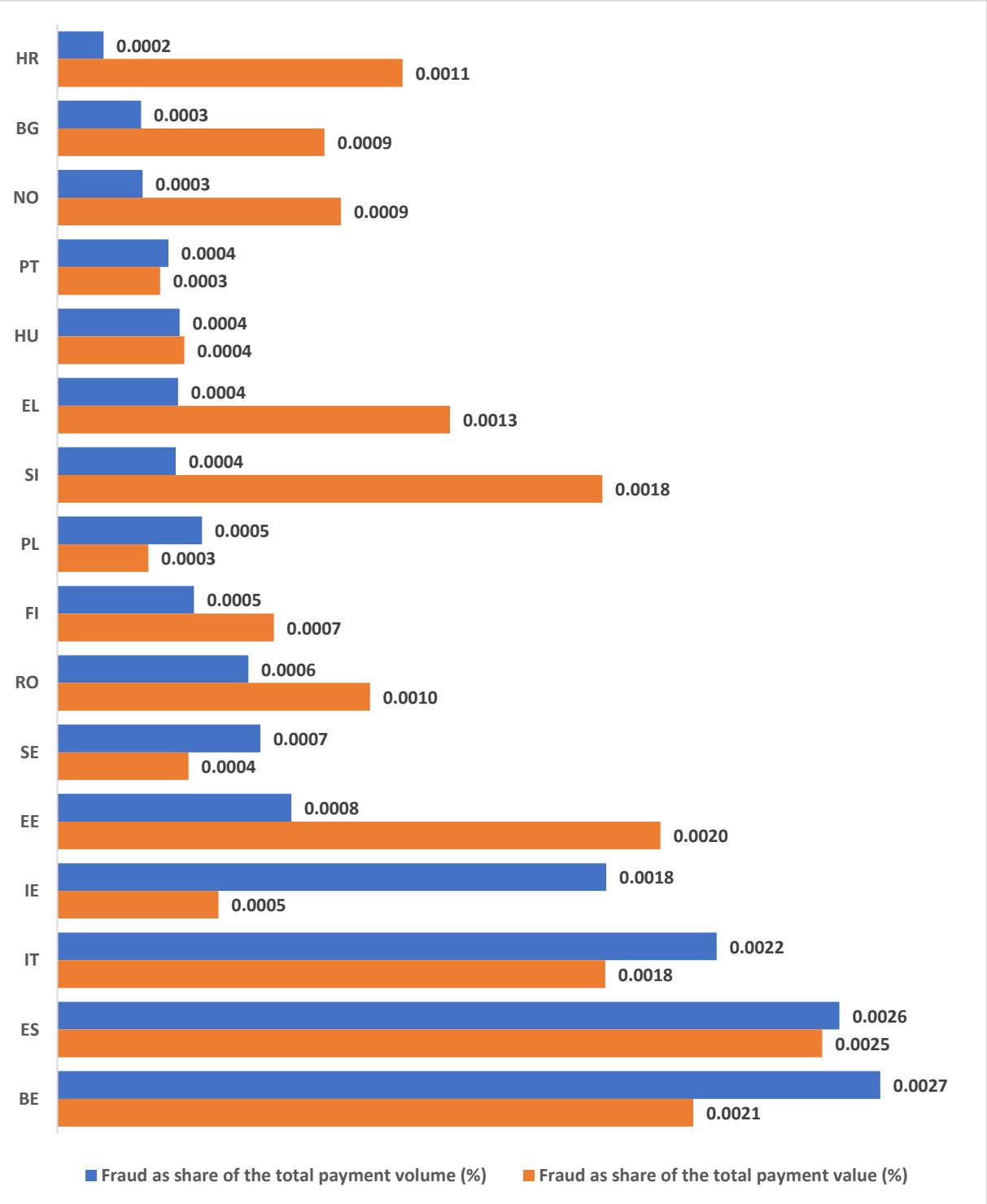
21. Furthermore, the data shows that card payments are by far the most frequently used payment instrument, and that these transactions experience higher fraud rates but lower average fraud amounts compared with other selected payment instruments.

Fraud rate by EEA Member State

22. Fraud as share of the total volume and value of payments differs significantly between the EEA countries in the sample and across the selected payment instruments.

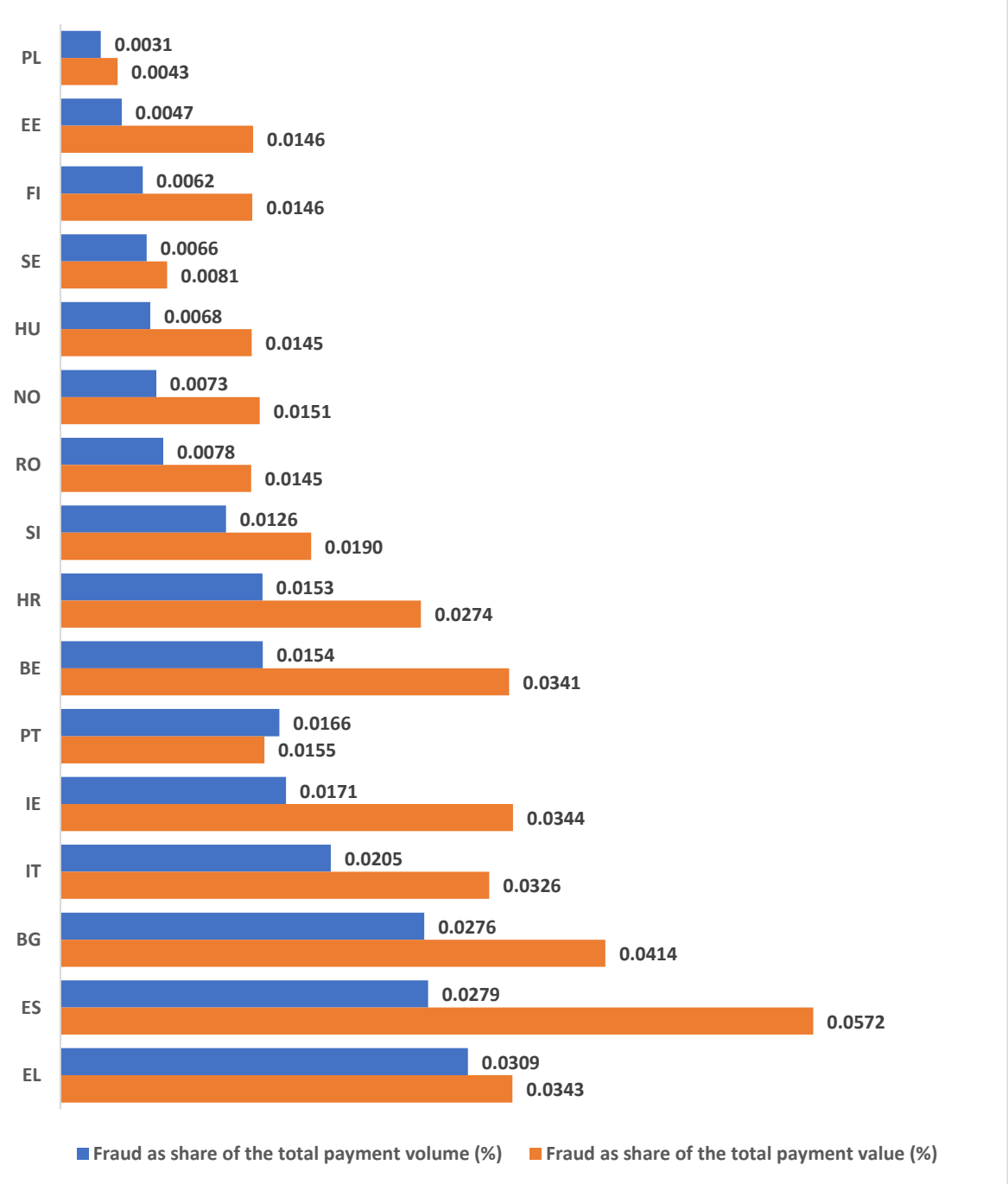
23. First, for credit transfers, the share of fraud in the volume of payments ranges between countries, from a rate of 0.0002 % to 0.0027 %, while the median fraud rate is 0.0005 % across the EEA countries included in the sample. Fraud as share of payment value ranges from 0.0003 % to 0.0025 %, while the median fraud rate is 0.0010 %. By way of illustration, Figure 2 depicts these country-based fraud rates. It is worth noting that Figure 2 (as well as Figures 3, 4 and 5) provides the fraud rates only for the countries from which good quality data has been submitted (and has thus been included in the sample) and for which the received data has not been reported as confidential. Therefore, these figures should not be read as a ranking of the country-based fraud rates, but merely highlight the diversity and the range of the fraud rates computed on the basis of the data provided by the domestic industries.

Figure 2: Fraud rate for credit transfers in H2 2020, per country, in percentage



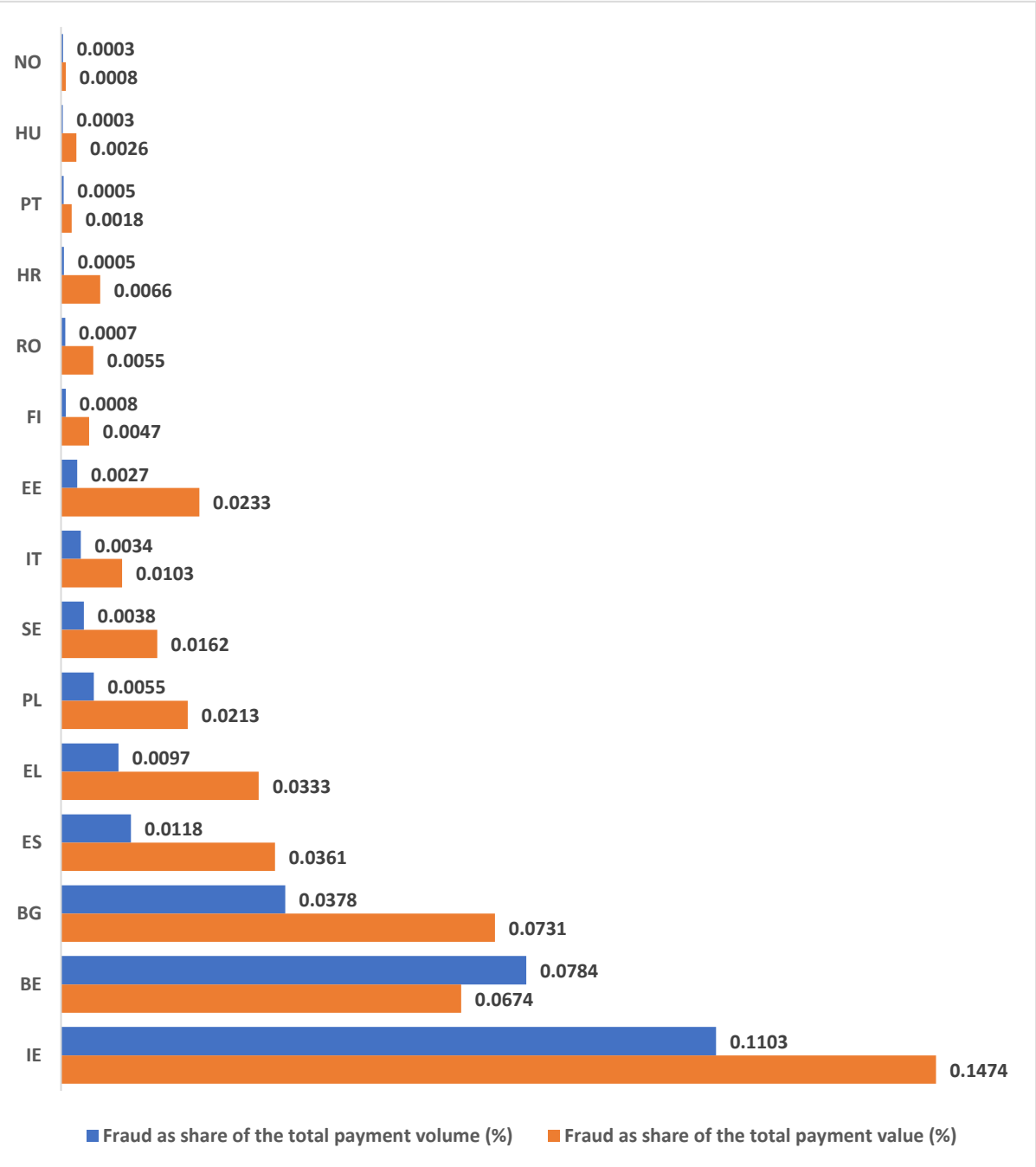
24. Second, for card payments as reported by issuers, the share of fraud in the total volume of payments ranges from 0.0031 % to 0.0309 %, while the median fraud rate is 0.0103%. The share of fraud in the total payment value ranges from 0.0043 % to 0.0572 %, while the median fraud rate is 0.0191 %. By way of illustration, Figure 3 depicts these country-based fraud rates.

Figure 3: Fraud rate for card payments reported by issuers in H2 2020, per country, in percentage



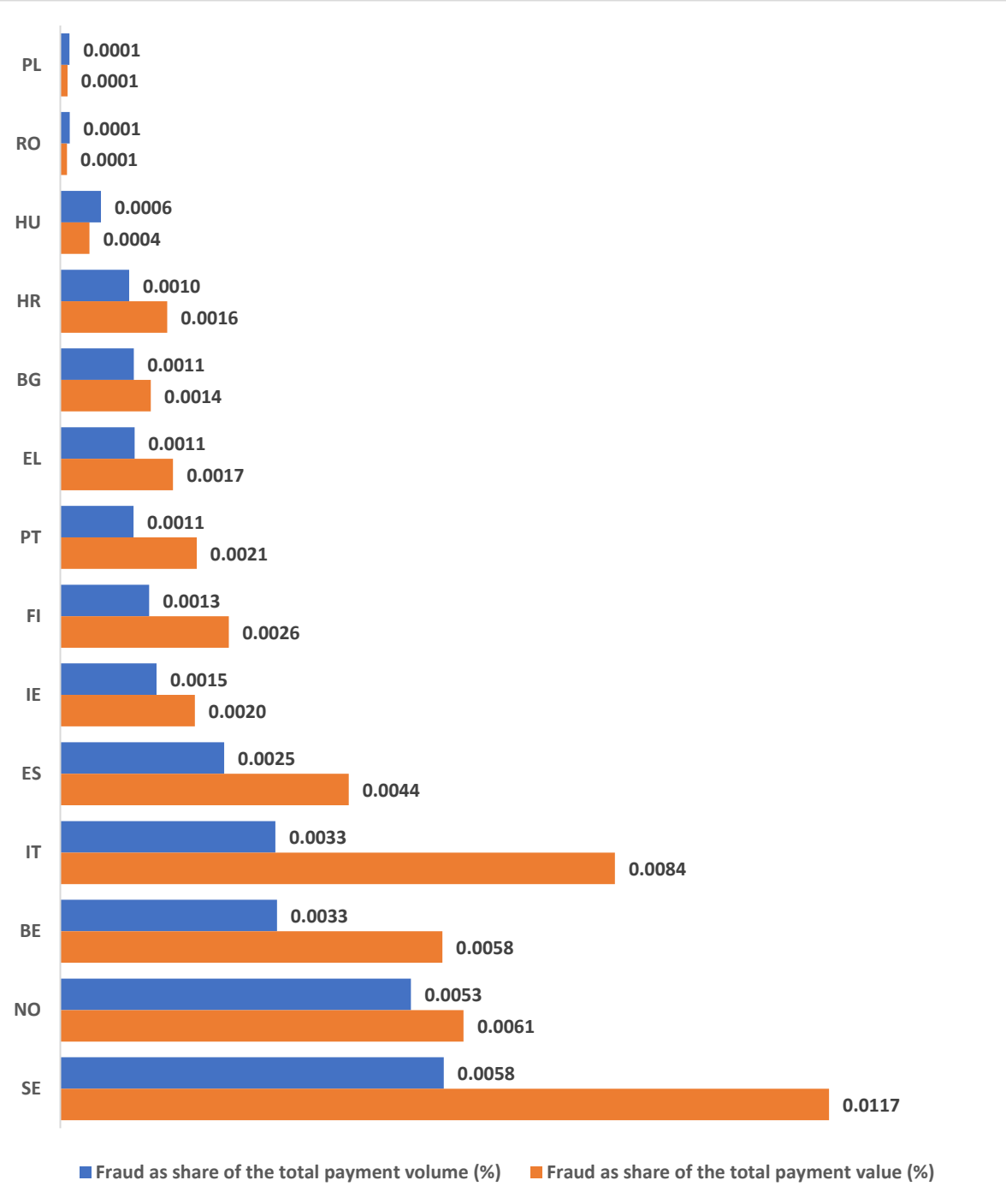
25. Third, for the card payments as reported by acquirers, the share of fraud in the total volume of payments ranges from 0.0001 % to 0.1103 %, while the median fraud rate is 0.0036 %. The share of fraud in the total value of the same transactions ranges from 0.0004 % to 0.1474 %, while the median fraud rate is 0.0188 %. By way of illustration, Figure 4 depicts these country-based fraud rates.

Figure 4: Fraud rate for card payments reported by acquirers in H2 2020, per country, in percentage



26. Fourth, for cash withdrawals, the share of fraud in the total volume of payments ranges from 0.0001 % to 0.0058 %, while the median fraud rate is 0.0011 %. The share of fraud in the total value of the same transactions ranges from 0.0001 % to 0.0117 %, while the median fraud rate is 0.0017 %. By way of illustration, Figure 5 depicts these country-based fraud rates.

Figure 5: Fraud rate for cash withdrawals in H2 2020, per country, percentage



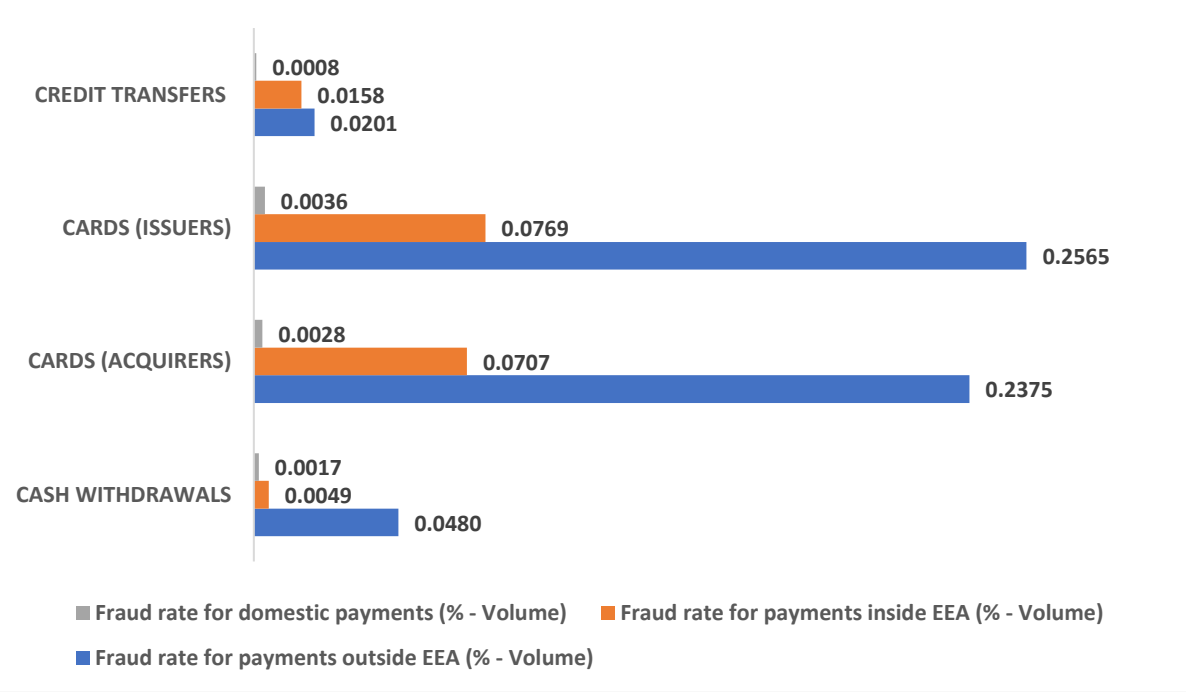
Fraud rate for domestic vs. cross-border transactions

27. In H2 2020, the cross-border transactions represent a low or relatively low share of the total volume of payment, i.e. 2 % of cash withdrawals and credit transfers, 15 % of card payment reported by issuers and 28 % of card payments reported by acquirers. However, the share of the cross-border transactions in the volume of fraudulent transactions is significantly higher. More specifically, fraudulent cross-border transactions represent 17 % of fraudulent cash withdrawals, 31 % of fraudulent credit transfers, 81 % of fraudulent card payments reported by issuers and 94 % of fraudulent card payments reported by acquirers. It is worth noting that the data reported for H2 2020 may have been impacted by the specific circumstances of the COVID-19 pandemic. This context may have reduced the opportunities of frauds for cross-border non remote payments but increased the relevance of targeting remote payments from the fraudsters' perspective.

28. Among the cross-border payments, the payments with counterparts located outside of the EEA are more frequently subject to fraud compared to the payments executed inside the EEA. This is the case for all the selected payment instruments. For instance, the share of fraud in the total volume of card payments outside the EEA reported by issuers is three times higher than the fraud share in the volume of payments inside the EEA and 85 times higher than the fraud share for the domestic transactions. These preliminary observation for 2019/2020 are consistent with statistics published by the ECB for earlier reporting periods.

29. Figure 6 highlights these differences for H2 2020. However, it is worth noting that the payments conducted outside the EEA represent a small subset of the total volume of transactions, i.e. between 0.3 % (for credit transfers) and 7.5 % (for cards reported by acquirers). By comparison, domestic payments, for which the fraud share is substantially lower, represent between 72 % and 98 % of the total transactions depending on the payment instrument.

Figure 6: Fraud rate when payments are executed domestically, inside EEA and outside EEA



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

Electronically initiated and non-electronically initiated transactions compared

30. The fraud rate also diverges across the payment initiation method used:

- Regarding the credit transfers reported for H2 2020, the fraud share in the total volume of payments initiated electronically is two times higher than the fraud share for payments non-electronically initiated. Similarly, the fraud share in the total value of payments initiated electronically is three times higher. The transactions initiated electronically represent 94 % of the credit transfers reported in H2 2020, therefore the fraud rate is higher for the type of payment initiation that is the most used by the PSUs.

- By contrast, regarding card payments reported by issuers for H2 2020, the fraud share in the total volume of payments initiated non-electronically, and therefore outside of the scope of the SCA requirements under PSD2 and the EBA's RTS, is four times higher than the fraud share in the total volume of payments initiated electronically. Similarly, the fraud share in the total value of payments initiated non-electronically is four times higher. However, it is worth-noting that the transactions initiated non-electronically represent only

1 % of the card payments reported by issuers in H2 2020 and 4 % of the fraudulent said card payments.

- In the case of cash withdrawals, the fraud rate is higher regarding the payments initiated via a card with a credit or a delayed debit function compared to the payments initiated via a card with a debit function. In H2 2020, the share of fraud in the total volume of credit-card payments is six times higher than the share of fraud in the total volume of debit-card payments. Similarly, the share of fraud in the total value of credit-card payments is three times higher. However, it is worth-noting that the transactions initiated via a card with a credit or a delayed debit function represent only 5 % of total volume of the cash withdrawals and 24 % of the fraudulent cash withdrawals reported in H2 2020.

31. The patterns identified above are summarised in Figure 7 for each payment instrument. These are consistent over time from H1 2019 to H2 2020.

Figure 7: Payment initiation method with the higher fraud rate, by payment instrument

Payment instrument	CREDIT TRANSFERS	CARDS (ISSUERS)	CARDS (ACQUIRERS)	CASH WITHDRAWALS
Payment method with higher fraud rate	Electronic initiation	Non electronic initiation	Non electronic initiation	Credit / delayed debit card

Fraud rate for card payments with and without SCA

32. For card payments, the figures reported for H2 2020 show that the share of fraud in the total volume and value of payments is higher for payments that are not authenticated with SCA compared to payments authenticated with SCA.

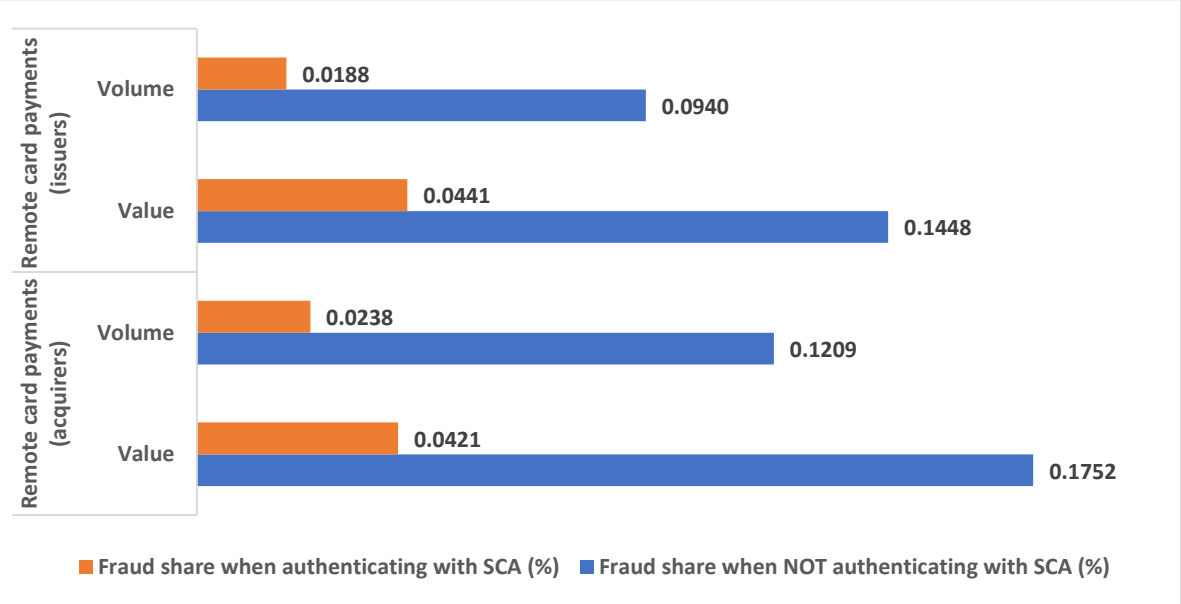
33. More specifically and as depicted in Figure 8, for remote card payments reported by issuers, the share of fraud in total volume is five times higher for payments authenticated without SCA compared to the payments authenticated with SCA. Similarly, the fraud share in total value is three times higher for the payments authenticated without SCA compared with the payments authenticated with SCA. It is worth noting that the payments authenticated without SCA represent 85 % of the volume and 71 % of the value of remote card payments reported by issuers.

34. For remote card payments reported by acquirers, the share of fraud in total volume is five times higher for the payments authenticated without SCA compared with the payments

authenticated with SCA. The share of fraud in total value is four times higher for the payments authenticated without SCA compared with the payments authenticated with SCA. These payments authenticated without SCA represent 83 % of the total volume and 78 % of the total value of remote card payments reported by acquirers. This particular observation is not surprising, as the reporting period in question still benefited from the supervisory flexibility the EBA had granted at the time to respond to the very low level of industry readiness and compliance, by allowing national authorities to not yet enforce the requirement on this subset of transactions.

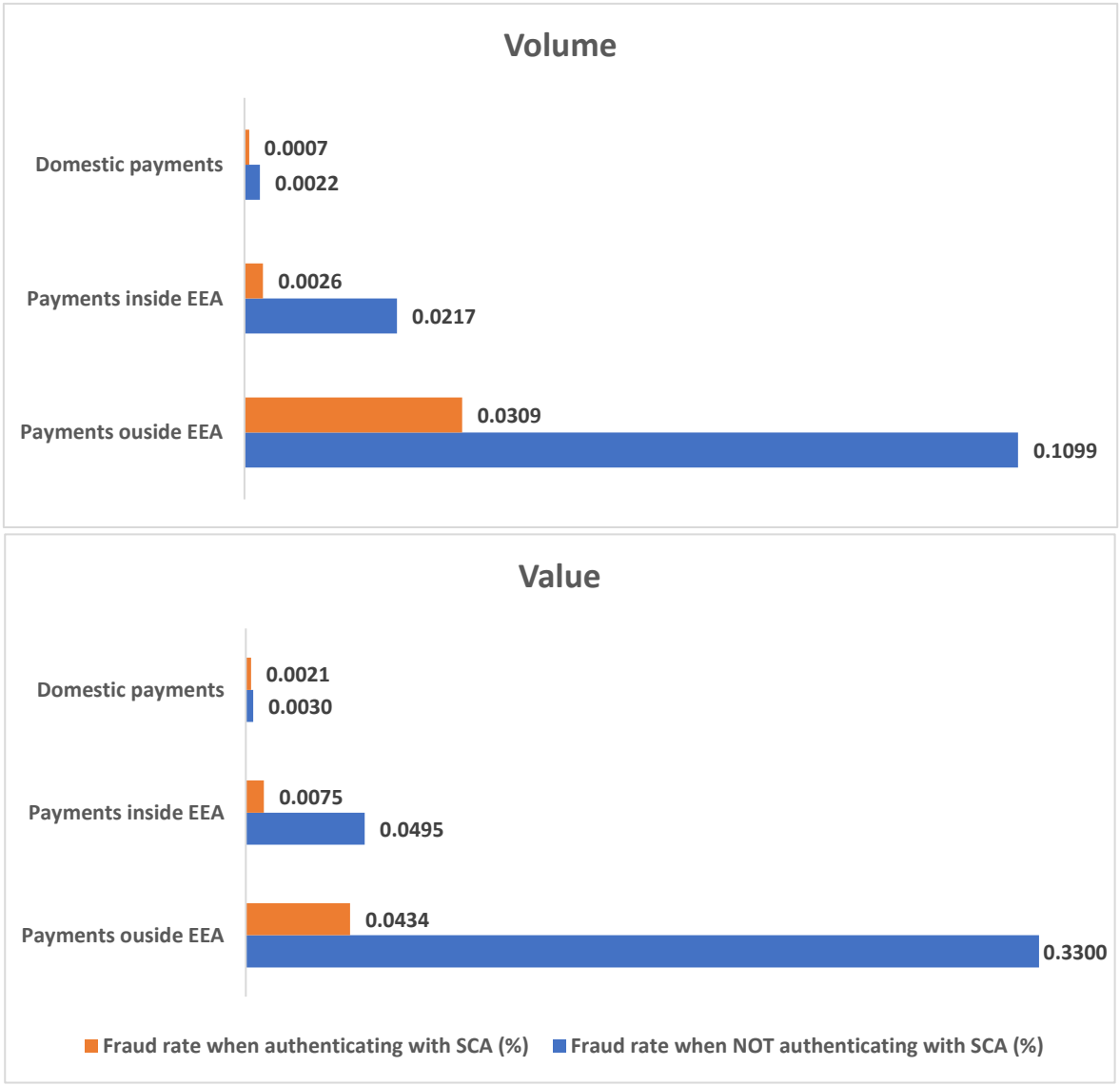
35. Expressed differently, card payments with SCA have share of fraud in the total volume and value of transactions that are 70-80 % lower than those without. And this is so even though in the reporting period of H2 2020, many acquirers, issuers and merchants in the EU were still not compliant with SCA requirements.

Figure 8: Fraud rate for remote card payments reported by issuers and acquirers, with and without SCA



36. This correlation between a lower fraud rate and the authentication with SCA is also observed with regard to non-remote card payments. Such correlation between a lower fraud rate and the authentication with SCA is even stronger when looking into the cross-border card transactions, in particular those cross-border transactions with counterparts located outside the EEA, and therefore outside of the scope of the SCA requirements under PSD2 and the EBA's RTS. This pattern is illustrated in Figure 9.

Figure 9: Fraud rate of non-remote card payments reported by issuers, with and without SCA, by geographical scope



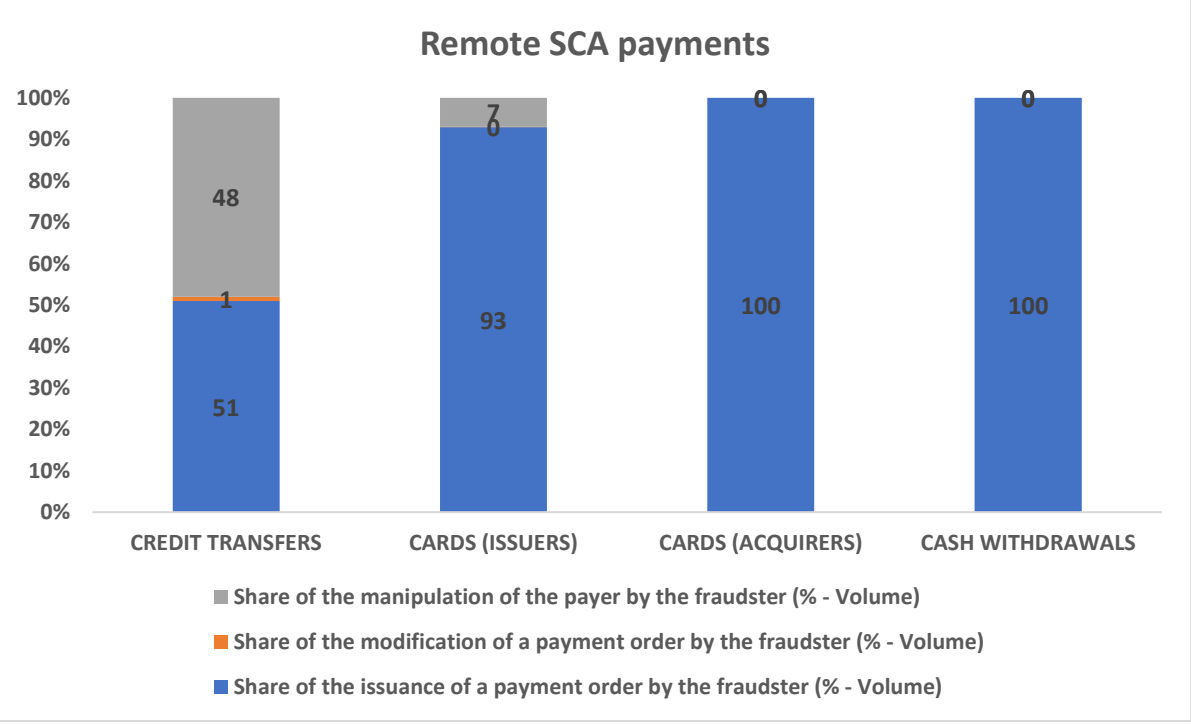
37. The abovementioned patterns related to the authentication with SCA of card payments are consistent over time from H1 2019 to H2 2020 (not shown). The data collected as per the EBA Guidelines does not distinguish the transactions authenticated with SCA and without SCA regarding cash withdrawals. As a result, this paper does not provide assessments on this specific aspect. The observations related to credit transfers will be developed in the subsequent chapter of the DP.

Occurrence of the different types of fraud

38. Among the various types of fraud that have been reported, the issuance of a payment order by the fraudster is the most common fraud type for cards payment and cash withdrawals. This accounts for more than 90 % of the volume and value of the fraudulent card transactions (reported by both issuers and acquirers) and cash withdrawals. This is so for all the types of payment, i.e. transactions authenticated with SCA and those authenticated without SCA as well as remote and non-remote transactions.

39. By contrast, the modification of a payment order by the fraudster is a very infrequent fraud type, irrespective of the payment instrument. These patterns are consistent over time from H1 2019 to H2 2020 (not shown). Figure 10 provides some examples for remote transactions authenticated with SCA for the H2 2020 reference period.

Figure 10: Share of the different types of fraud for the selected payment instruments (remote tansactions authenticated with SCA)



40. Turning into the more detailed breakdowns of fraud types underlying the issuance of a payment order by the fraudster, some notable differences across payment instruments and initiation channels can be observed. Regarding remote card payments reported by issuers, the theft of card details is the most common event and represent 75 % of the value of the fraudulent SCA payments and 60 % of the value of the fraudulent non-SCA payments in H2 2020. 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.

41. For non-remote card payments reported by issuers, the lost or stolen cards are the most common fraudulent event and represent 45 % of the value of the fraudulent payments authenticated with SCA and 46 % of the value of payments that are not authenticated with SCA.

42. The counterfeit cards represent about 20 % of the volume and value of the fraudulent non-remote payments (both authenticated with and without SCA). It is worth noting that the non-remote card payments represent only 13 % of the fraudulent card payments reported by issuers, therefore the share of counterfeit cards in the total volume of these fraudulent payments can be considered as limited. These abovementioned patterns are consistent over time from H1 2019 to H2 2020.

43. Patterns comparable to the ones observed for card payments reported by issuers also are observed in relation to card payments reported by acquirers.

44. Regarding cash withdrawals, the payments done via a lost and stolen cards are the main fraud type and represent 70 % of the total volume of fraudulent cash withdrawals in H2 2020.

45. By contrast, credit transfers authenticated with SCA experience other types of fraud. The share of the manipulation of the payer by the fraudster accounts for 47 % of the volume of the fraudulent remote payments and 53 % of the fraudulent non-remote payments that are authenticated with SCA in H2 2020 (but the issuance of a payment order by the fraudster remains the most prevalent fraud type regarding the credit transfers that are not authenticated with SCA).

46. Over the four reporting periods, credit transfers are the payment instrument for which the manipulation of the payer by the fraudster as a share of the total fraudulent transactions appear most prevalent compared with the other payment instruments. This pattern may be explained by the fact that the issuance of a fraudulent payment order for credit transfers may be more complex from the fraudster's perspective and the manipulation of the payer, for example by means of social engineering, may be the more prevalent practice for credit transfers.

47. The patterns presented in this chapter offer an overview of the preliminary observations that can be conducted on the basis of the selected fraud data reported as per the EBA Guidelines. Additional views and comments would be beneficial in order to improve the understanding.

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

Potentially inconclusive patterns that require additional analyses

48. In contrast with the above, this chapter highlights some further patterns that appear to be not immediately intuitive based on the information at hand.

Higher fraud rate for remote credit transfers authenticated with SCA

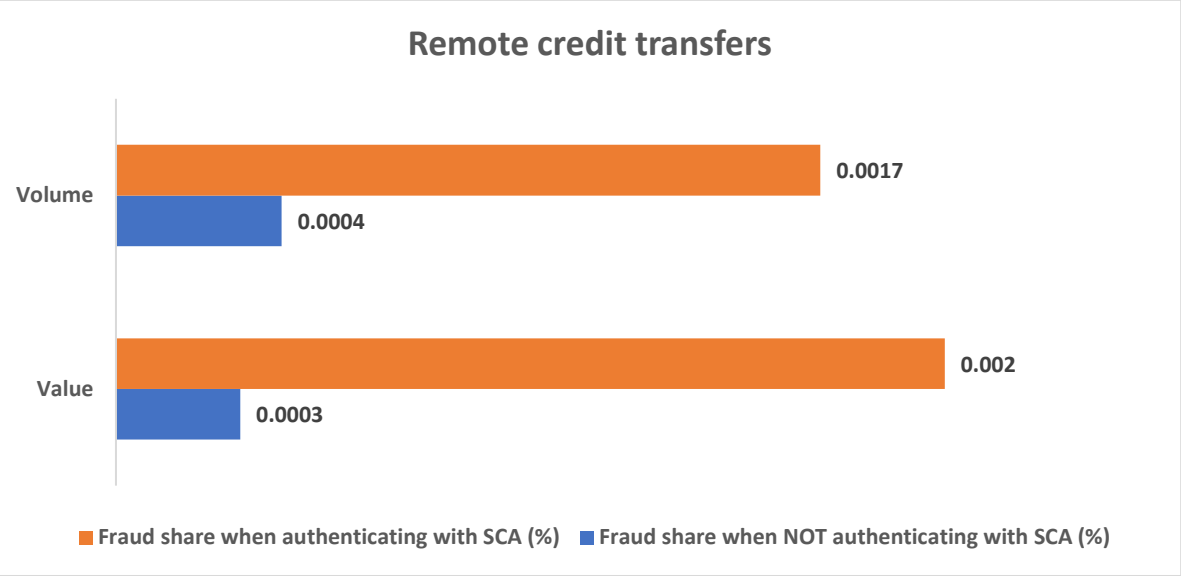
49. As shown in the previous chapter, card payments authenticated with SCA have fraud rates that are lower than the payments authenticated without SCA. This pattern is also observed regarding the non-remote credit transfers. Similarly, for H2 2020, the share of fraud in the total volume of non-remote credit transfers authenticated without SCA is two times higher compared to the share of fraud in the total volume of the same transactions that are authenticated with SCA.

50. However, this general pattern of the reductive impact of SCA on fraud rates does not appear to materialise in the specific case of remote credit transfers. For this category, the fraud rate is higher for payments authenticated with SCA compared to payments that are not authenticated with SCA. Some examples are provided below.

    - In H2 2020, as depicted in Figure 11, the share of fraud in the total volume of remote credit transfers that are authenticated with SCA is four times higher compared to the share of fraud in the total volume of remote credit transfers that are not authenticated with SCA. Similarly, the share of fraud in the total value of the remote credit transfers that are authenticated with SCA is seven times higher. Even though these transactions are a specific segment in the total transactions authenticated with SCA included in the sample, the remote payments authenticated with SCA represent 60 % of the total volume and 49 % of the total value of credit transfers reported for H2 2020. The fraudulent remote credit transfers authenticated with SCA represent 85 % of the total volume and 86 % of the total value of the fraudulent credit transfers.

    - In H1 2020 (based on a smaller sample of 14 countries), the fraud share in the total volume of remote credit transfers authenticated with SCA is two times higher compared to the fraud share in the total volume of remote credit transfers that are not authenticated with SCA. Also, the fraud rate in the total value of remote credit transfers authenticated with SCA is six times higher compared to the fraud rate of remote credit transfers that are not authenticated with SCA.

Figure 11: Fraud rate of remote credit transfers when payments are authenticated with SCA vs. not authenticated with SCA



51. There are several potential explanations for these observations, and the EBA is interested to hear respondents' views, First, the EBA Guidelines on fraud reporting, as amended in January 2020, provide that the transactions authenticated via non-SCA are transactions for which an exemption to SCA under the RTS on SCA&CSC[4] was applied or for which SCA was not applied due to other reasons (e.g. merchant-initiated transactions or one-leg transactions for card-based transactions). Therefore, one potential explanation might be that payments for which an exemption was applied (such as for example the low-value payment exemption in Article 16 of the RTS) are lower-risk transactions. Conversely, SCA payments can also be said to be exposed to a higher risk of fraud, as those payments are inherently of higher risk than the SCA exempted lower-risk transactions.

52. Moreover, the fraudulent credit transfers where SCA was applied might be due to spoofing, authorized push payments and transactions initiated by the account holders after social engineering from the fraudsters, such as phishing. The implementation of SCA is not sufficient to prevent fraud in such instances. Nevertheless, these types of fraud may also be applicable to other selected payment instruments and thus do not fully explain why the identified pattern seems to be specific to credit transfers.

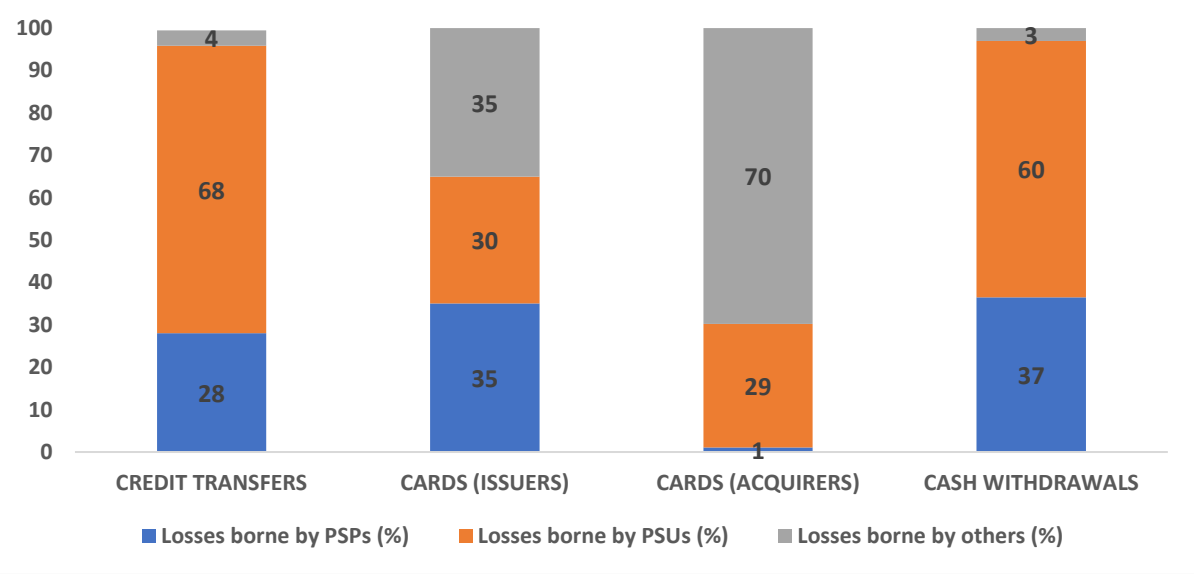
Question 3: Do you have any potential further explanations as to why, in the specific case of the remote credit transfers, the fraud rate reported by the industry is higher for payments authenticated with SCA compared to payments that are not authenticated with SCA?

[4] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Significant losses due to fraud borne by the PSUs[5]

53. As reported for the H2 2020 reference period, the PSUs bear most of the losses due to fraud regarding credit transfers and cash withdrawals. By way of example, PSUs bore 68 % of the losses due to fraudulent credit transfers in H2 2020 as illustrated in Figure 12. This pattern is consistent from H1 2019 to H2 2020 for credit transfers, while for cash withdrawals, the share borne by PSUs significantly increased over time (not shown).

Figure 12: Percentage of the losses due to fraud by liability bearer and payment instrument



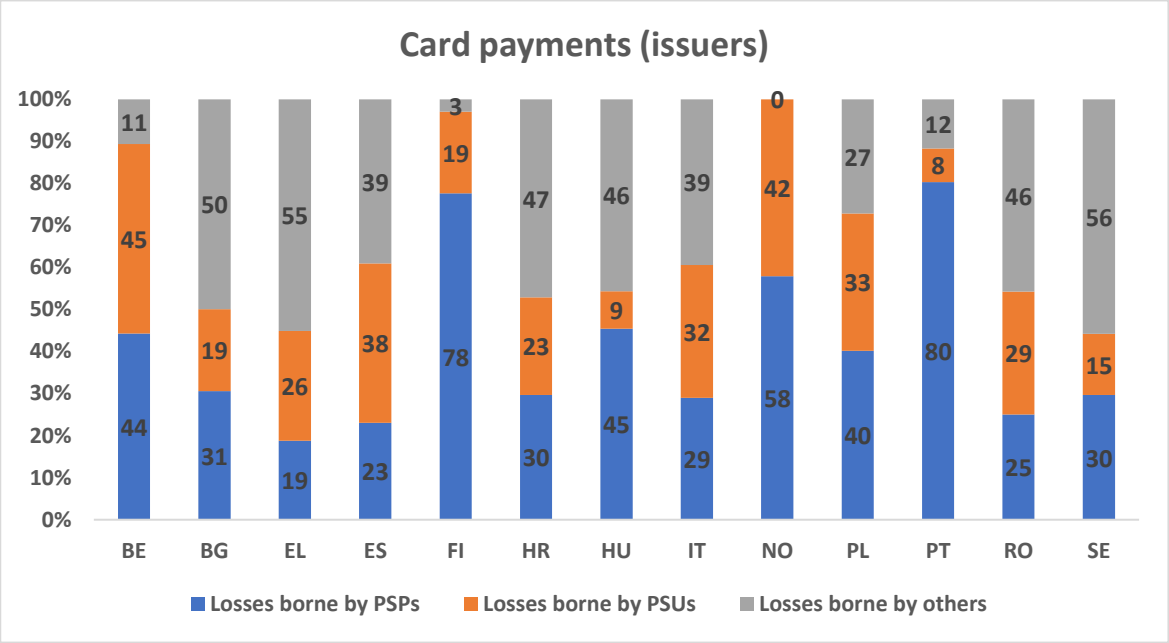
54. This pattern is somewhat at odds with Article 73 of the PSD2, which provides that liability for unauthorised transactions should lie primarily with the PSPs (unless the user has acted fraudulently). The high share of losses due to fraud borne by PSUs may be partially explained by the fact that under Article 74 of the PSD2, the PSU bears the losses relating to any unauthorised payment transactions when due to the PSU acting fraudulently or failing to fulfil its obligations as set out in Article 69 of the PSD2 with intent or gross negligence. In particular, the events covered by the notion of gross negligence might be differently understood and applied by the market stakeholders.

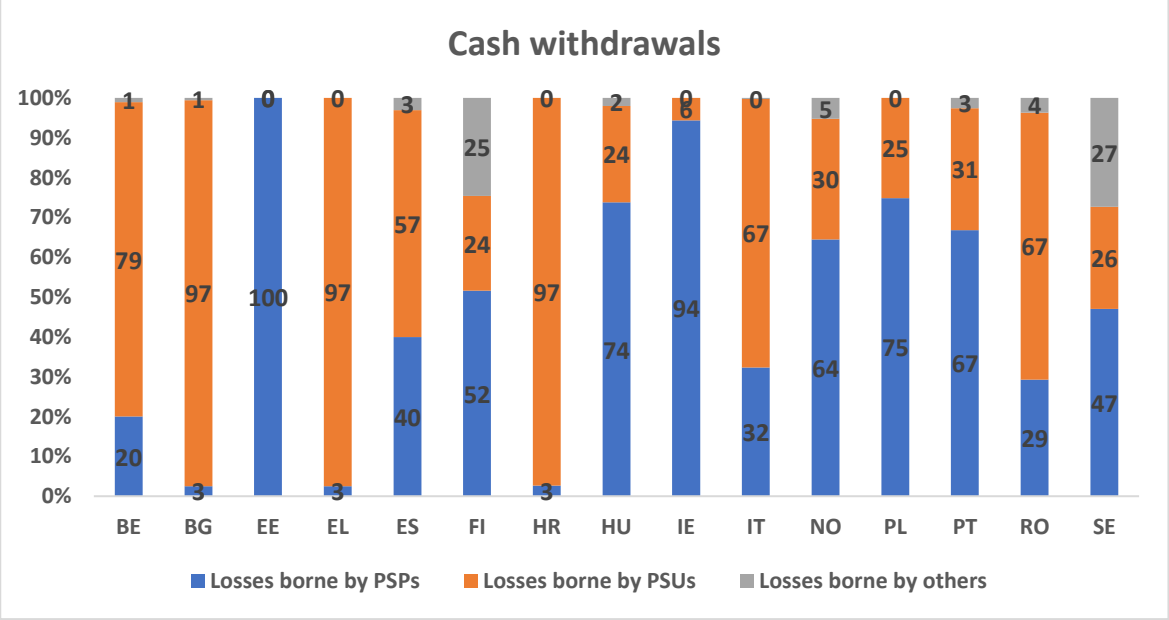
55. Additionally, it appears that the share of the losses borne by the PSUs significantly differs across EEA countries. This pattern is observed for all the selected payment instruments. Figure 13 provides some figures related to card payments reported by issuers and cash withdrawals as examples derived from the H2 2020 data. It is worth noting that Figure 13 provides the fraud

[5] As specified in Annex 2 of the EBA Guidelines, for the purpose of the reporting requirements under the Guidelines, the PSU should be understood as the payer in the context of credit transfers and cards payment reported by issuers, as the payee in the context of card payments reported by acquirers and as an account holder in the context of cash withdrawals.

rates only for the countries from which good quality data has been submitted (and has thus been included in the sample) and for which the received data has not been reported as confidential.

Figure 13: Percentage of losses due to fraud borne by liability bearer and by EEA Member State





56. For card payments reported by issuers, the share of the losses due to fraud borne by PSPs in the total volume of losses due to fraud ranges between countries, from a share of 19 % to 80 %.

The share of the losses due to fraud borne by PSUs ranges from 8 % to 45 %. For cash withdrawals, the share of the losses due to fraud borne by PSPs in the total volume of losses due to fraud also ranges between countries, from a share of 3 % to 100 %. The share of the losses due to fraud borne by PSUs ranges from 24 % to 79 %.

57. These substantial discrepancies may be partially explained by the abovementioned different interpretation of the notion of gross negligence, and / or the different national frameworks established when transposing the PSD2.

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

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

Significant losses due to fraud borne by bearers other than the PSPs and the PSUs

58. Regarding card payments, the reported losses due to fraud are borne to a large extent by bearers other than the PSPs and PSUs, which are reported under the residual category "Others" according to the taxonomy of the EBA Guidelines. As shown in Figure 12, these other stakeholders bear most of the losses from fraudulent card payments reported by acquirers (70 %) but also bear a substantial share of the losses from fraudulent card payment reported by issuers (35 %) in H2 2020. This pattern is consistent over the four reporting periods (not show).

59. The category of other bearers might include for example acquirers (for card-based payments reported by issuers), issuers (for card-based payments reported by acquirers) and possibly any merchants involved in the transactions.

60. Similarly to the percentage of the losses borne by the PSUs, it appears that the percentage of the losses borne by "Others" significantly differs from one EEA country to another. As shown in Figure 13 in relation to card payments reported by issuers, the share of the losses due to fraud borne by "Other" bearers in the total volume of losses due to fraud ranges from 3 % to 56 %.

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

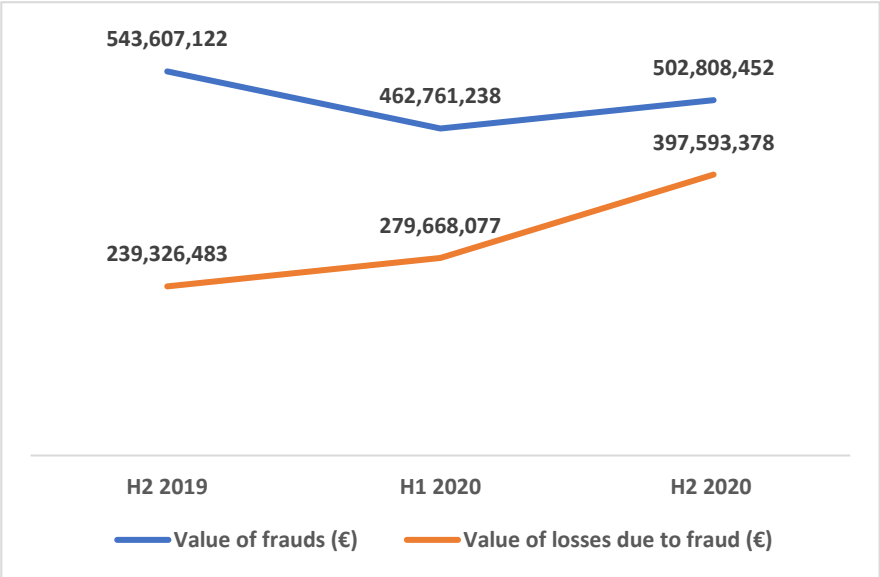
The correlation between the value of fraud and the value of losses due to fraud over time

61. The variations in the total value of fraud and the total value of reported losses due to fraud partially appear not to be in sync over the period from H2 2019 to H2 2020. First, regarding the time period between H2 2019 and H1 2020, the value of reported fraud decreased by 15 % while the value of the reported losses due to fraud increased by 17 %.

62. Furthermore, regarding the period of time between H1 2020 and H2 2020, both variables experienced positive growth at very different growth rates. In detail, the value of the reported fraud slightly increased compared with the previous period (+ 9 %) while the reported losses due to fraud grew significantly (+ 42 %). Figure 14 illustrates said variations observed in a sample of 14 EEA countries. The amounts provided in Figure 14 are aggregations of the fraud values and the losses due to fraud reported for credit transfers, cash withdrawals and card payments from the perspective of issuers. The cards payments reported by acquirers have not been included in these aggregates in order to avoid double counting the fraudulent card payments.

63. The data reported for H1 2019 is not considered here because more substantial data quality issues have been identified for this period. In particular, the value of fraud is significantly lower compared to the other reporting periods, probably due to initial issues encountered for the reporting of fraud information in the context of the first iteration of the data collection exercise.

Figure 14: Comparison between the value of fraud and losses due to fraud from H2 2019 to H2 2020



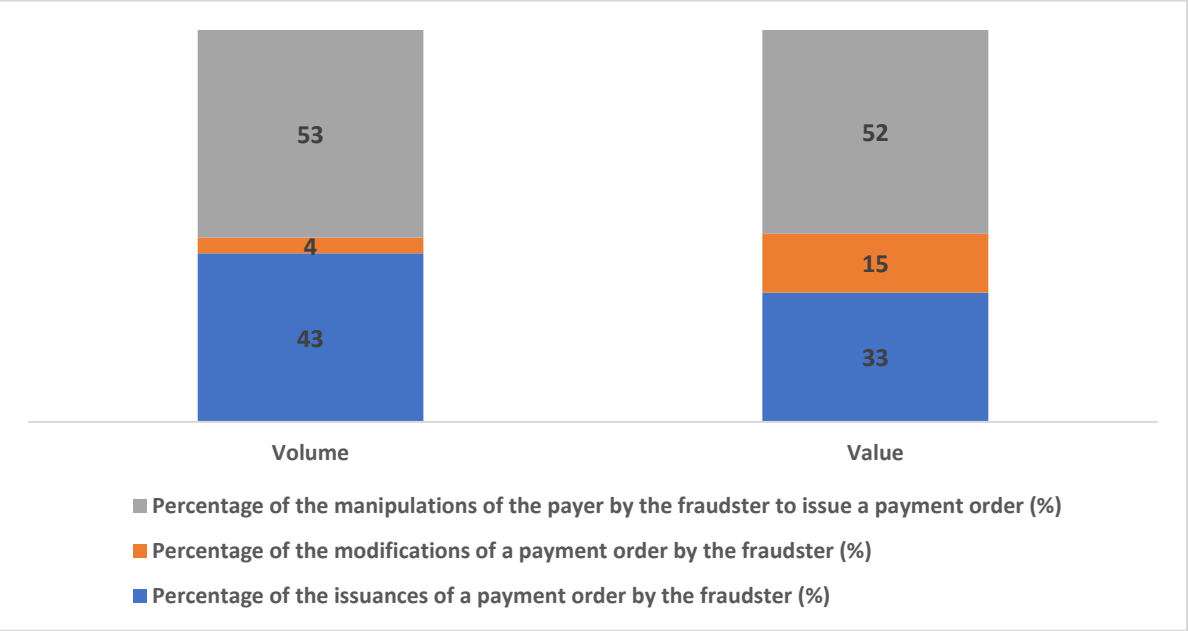
64. Since the value of losses due to fraud is assumed to derive from the value of fraud, a proportional correlation over time between these two variables would have been expected. Such different observed trends might stem from data quality issues but also from different allocation or computation of the losses over time from one individual fraud case to another. For example the losses due to fraud might only be included in the balance sheet of the PSPs with a delay after the fraud occurred, and thus, may be reported only for subsequent reference period. Also, the fraud data collection has been established recently and the number of reporting periods considered may be too low to extract reliable tendencies. There will be merit in reconducting this assessment on the basis of a longer timeframe once available.

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?

Substantial share of the fraudulent non-remote credit transfers reported as manipulations of the payer by the fraudster

65. The manipulation of the payer by the fraudster represents a substantial percentage of the fraudulent non-remote credit transfers in H2 2020. By way of example, the manipulation of the payer by the fraudster represents 53 % of the volume and 52 % of the value of the fraudulent non-remote SCA credit transfers in H2 2020, as outlined below in Figure 15. This pattern is consistent over time from H1 2019 to H2 2020 (not shown). Nevertheless, the manipulation of the payer is assumed as practically easier from the fraudster's perspective as regards remote credit transfers, compared to proximity payments. The practical execution of this type of fraud should be further clarified.

Figure 15: Fraudulent non-remote SCA credit transfers by fraud types

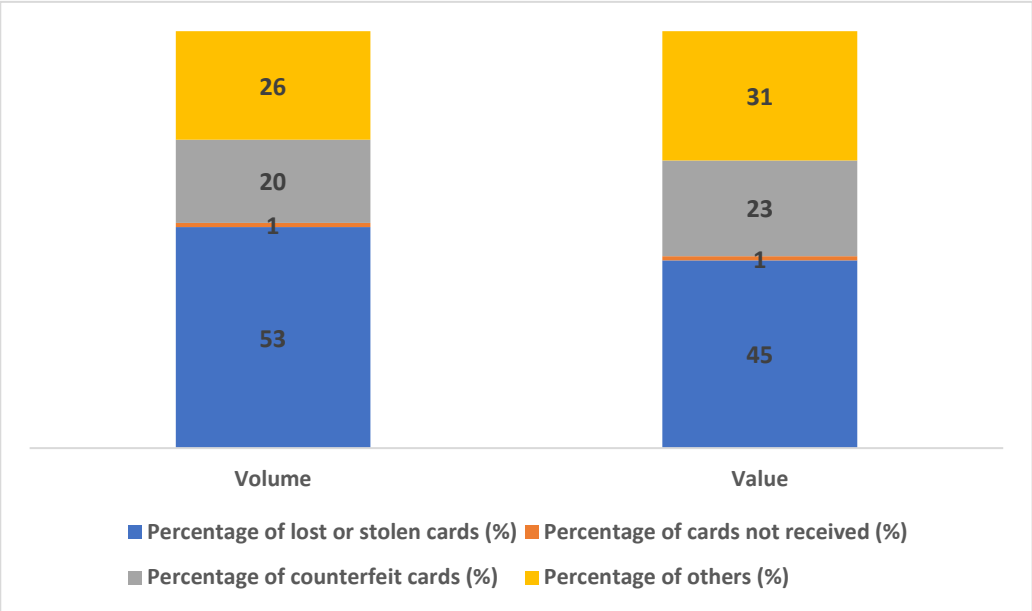


Question 8: How do you explain the fact that the manipulation of the payer by the fraudster represents a substantial share of the fraudulent non-remote credit transfers authenticated with SCA? How is this fraud type concretely executed by the fraudsters?

Substantial share of the fraudulent card payments stemming from fraud events reported under the breakdown "other"

66. Among the various types of fraud under the category "issuance of a payment order by the fraudster" (which includes "lost and stolen card", "card not received", "counterfeit card", and the category "other"), the fraudulent events reported under the category "other" represent a substantial percentage of the issuances of a payment order by the fraudster for card payments. As shown in Figure 16, these other fraudulent events represent 26 % of the volume and 31 % of the value of the fraud reported under the category "issuance of at payment order by a fraudster" for the non-remote SCA card payments from issuers in H2 2020.

Figure 16: Percentage of the different fraud types among the issuances of fraudulent payment orders for non-remote SCA card transactions reported by issuers



67. This pattern is consistent over time from H1 2019 to H2 2020 and also observed for remote card payments from issuers and for card payments from acquirers (irrespective of the payment method used and the implementation of the SCA). It appears important to clarify which types of fraud have been reported in the sub-category "others" under the category "issuance of a payment order by a fraudster".

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"?

Questions for discussion

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

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

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?

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

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

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

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?

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?

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"?