European Banking Authority

EUROPEAN CENTRAL BANK
EUROSYSTEM

2024 REPORT ON PAYMENT FRAUD

Contents

List of charts and tables

Abbreviations

ATM	Automated teller machine
CA	Competent authority
CSC	Common and secure open standards of communication
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
EU	European Union
NCA	National competent authority
NCB	National central bank
PSD	Payment Services Directive
PSP	Payment service provider
PSU	Payment service user
RTS	Regulatory Technical Standards
SCA	Strong customer authentication

Executive Summary

This report, jointly prepared by the EBA and the ECB, assesses the latest payment data reported to the EBA and the ECB under Article 96(6) of Directive EU 2015/2366 (the revised Payment Services Directive, PSD2). It covers semi-annual data reported for the three reference periods H1 2022, H2 2022 and H1 2023, and focuses on the payment instruments of credit transfers, direct debits, card payments (from an EU/EEA issuing perspective), cash withdrawals and e-money transactions. The data covers all EU/EEA countries that reported the full time series and the report analyses total payment transactions and the subset of fraudulent transactions, both in value and volume terms. It further provides more detailed analyses on specific topics such as the main fraud types and the application of strong customer authentication (SCA), as well as some geographical and country-level analyses.

The report assesses the payment fraud reported by the industry across the European Economic Area (EEA), which amounted to EUR 4.3 billion in the year 2022 and EUR 2.0 billion in the first half of 2023. Most payment fraud in value terms was related to credit transfers and card payments, across all three reference periods analysed. More specifically, in the period H1 2023 the total value of fraudulent credit transfers sent by PSPs in the EU/EEA amounted to EUR 1.131 billion, and the value of card fraud using cards issued in the EU/EEA amounted to EUR 633 million. In volume terms, 7.31 million card transactions using cards issued in the EU/EEA in H1 2023 were fraudulent, while the number of fraudulent credit transfers, direct debits, cash withdrawals and e-money transactions was significantly lower.

In relative terms, the highest fraud rates were observed for card payments, where fraud accounted for 0.031% of total card payments in value and 0.015% of total card payments in volume terms in H1 2023, as well as for e-money transactions (0.022% of the total value and 0.012% of the total number of e-money payments). Fraud rates were substantially lower for all other instruments, with the exception of direct debit fraud in volume terms (accounting for 0.014% of the number of direct debit transactions in H1 2023).

Card fraud predominantly occurred for remote transactions, while the majority of overall card payments were conducted non-remotely. By contrast, credit transfers and e-money transactions were mostly initiated remotely, both with regard to overall transactions and fraudulent ones.

Card payment fraud seemed to predominantly occur with fraudulent payment orders issued by the fraudster, with the specific reasons mostly being the use of lost or stolen cards in the case of non-remote card fraud (more than 50% in terms of volumes in H1 2023) and card details theft in the case of remotely conducted card fraud (64% in volumes in H1 2023). By contrast, counterfeit card fraud and manipulations of the payer to initiate a payment order played only a minor role across the three reporting periods. Manipulations of the payer accounted for more than half of the total value of fraudulent credit transfers during this time.

SCA was applied for the majority of electronic payments in value terms, especially for credit transfers (around 77%). In general, SCA-authenticated transactions showed lower fraud rates than non-SCA

transactions, especially for card payments. Furthermore, fraud rates for card payments turned out to be significantly (about ten times) higher when the counterpart is located outside the EEA, where the application of SCA may not be requested.

The use of the exemptions to SCA that are offered in the technical standards developed by the EBA and the ECB varied by payment instrument and initiation channel. Some exemptions, such as the low value exemption, trusted beneficiaries, recurring transactions or transaction types that are outside the scope of SCA requirements under PSD2 showed higher fraud rates than others, such as transactions involving secure corporate processes and protocols. The findings support a beneficial impact of SCA requirements introduced under PSD2 on the security of electronic payments, but also highlight the need for further investigations regarding the correct application of these requirements by the market.

Losses due to frauds were distributed differently among liability bearers depending on the payment instrument. In H1 2023, payment service users (PSUs) bore 45% and 51% of the losses that arose from card payments and cash withdrawals, respectively; this share was below 25% for e-money transactions. In contrast, PSUs endured more than 80% of total fraud losses for credit transfers. However, the distribution of the liability for fraud losses between PSUs and PSPs diverged significantly across countries: in the specific case of card payments, in a significant number of countries PSUs bore more than half of the fraud losses, at times as much as 80% of all losses or more, while in some other countries the share was as low as 30% or less.

Regarding the geographical dimension of fraud, the presented results show that, while most payment transactions were domestic, most card payment fraud (71% in value terms in H1 2023) and a large share of credit transfer and direct debit fraud (43% and 47%, respectively, in H1 2023) were cross-border. A notable share of fraudulent card payments (28% in H1 2023) was thereby related to cross-border transactions outside the EEA.

Looking ahead, the general outlook with respect to overall payment fraud based on the presented analysis appears stable. The widespread adoption of the RTS for SCA and CSC has had a positive effect on reducing fraudulent payments, especially for transactions conducted within the EEA. Additionally, industry measures such as the global implementation of the EMV standard also continued to limit the opportunities to conduct fraud, e.g. with regard to the use of counterfeit cards. Nevertheless, it is important for the industry, regulators and consumers to remain alert. Both the EBA and the ECB will continue to closely monitor developments in payment fraud, using the valuable data collected under PSD2 and the ECB Regulation on payments statistics.

1. Introduction

The EBA and the ECB, in their respective roles as supervisory authority of payment service providers and overseer of payment systems, instruments, schemes and arrangements, closely monitor developments in payment fraud. Both the EBA and the ECB thereby rely on statistical information on the volumes and values of payment transactions and corresponding fraud reported by payment service providers (PSPs) located in the EU/EEA.

In accordance with Article 96(6) of PSD2, PSPs are required to report statistical data on fraud relating to different means of payment to their competent authorities (NCAs). NCAs, in turn, are required to provide both the EBA and the ECB with this data in aggregated form. In support of these provisions, the EBA Guidelines on fraud reporting under PSD2 (EBA/GL/2018/05, hereafter 'EBA Guidelines'), which have applied since 1 January 2019, specify the data that should be reported under PSD2. In addition, Regulation (EU) No 1409/2013 of the European Central Bank on payments statistics (ECB/2013/43), as amended (hereafter 'ECB Regulation on payments statistics'), requires PSPs located in the euro area to report inter alia detailed information on payment fraud to their national central banks, which in turn are obliged to share the data in aggregated form with the ECB.[1] Data under both the EBA Guidelines and the ECB Regulation on payments statistics is reported on a semi-annual basis.

This report, jointly prepared by the EBA and the ECB, presents a comprehensive overview of the latest data collected under the above-mentioned frameworks. As such, it complements and extends previous publications on fraud such as the regular Eurosystem reports on card fraud[2], providing both a more encompassing and a more detailed perspective on fraud across various payment instruments. While observed trends and findings presented in this report appear aligned with the findings included in past Eurosystem reports on card fraud, caution is warranted when comparing these findings, given the substantial differences in terms of data source, reporting methodology, the scope and content of the collected information, and the geographical coverage.

The analysis is based on semi-annual data for three reference periods – i.e. H1 2022, H2 2022 and H1 2023. While data under the EBA Guidelines has been reported for 2019 onwards, full coverage of EU/EEA countries only applies for reference period H1 2022 onwards. H1 2022 is therefore the first period on which this report is based. The results are presented separately for the main payment instruments, i.e. credit transfers, direct debits, card payments, cash withdrawals and e-money transactions.

[1] Non-euro-area EU Member States can comply with the reporting under the ECB Regulation on payments statistics on a voluntary basis. To streamline the reporting process and reduce the reporting burden for PSPs and national authorities, data reported in accordance with the ECB Regulation on payments statistics to the ECB may be considered to fulfil the reporting requirements to both the EBA and ECB under the EBA Guidelines, provided the respective NCAs and, where necessary, cooperating non-euro-area NCBs along with the EBA and ECB have signed a dedicated Memorandum of Understanding and comply with the terms set therein. This is currently the case for all countries that report data in accordance with the ECB Regulation on payments statistics to the ECB (including all euro area countries along with Bulgaria, the Czech Republic, Hungary and Romania).

[2] See for example the Eurosystem Report on card fraud in 2020 and 2021.

Presented figures for card payments are generally derived from an issuing, rather than acquiring, perspective.[3] Only in some cases have results been added from an acquiring point of view, for the purpose of facilitating specific comparisons. Where this occurs, the change of perspective is explicitly stated.

Unless stated otherwise, all aggregate figures refer to the whole EU/EEA, excluding Liechtenstein.[4] Data aggregates analysed for this report are those defined under the EBA Guidelines irrespective of whether the original reporting by PSPs was in accordance with the EBA Guidelines or the ECB Regulation on payments statistics.

Although this report is the most comprehensive publication so far on payment fraud in the EU, several data limitations remain, such as some incomplete data submissions or methodological misclassifications by reporting PSPs, as well as other potential data quality issues that continue to be investigated by the respective national competent authorities and/or national central banks and that may lead to retrospective data corrections when data is reported for forthcoming reporting periods. Where identified and considered relevant, quality disclaimers have therefore been added throughout the report. Also, given that this report only covers three reporting periods, caution should be exercised when attempting to interpret trends over time.

The report is organised as follows: Chapter 2 presents the main findings on the total level of fraud per payment instrument. Chapter 3 focuses on the types of payment fraud observed by the EBA and the ECB. Chapter 4 looks at the application of strong customer authentication (SCA) under PSD2, corresponding fraud rates and the use of exemptions by PSPs. Chapter 5 provides an overview of reported losses due to fraud and to what extent PSPs and payment service users (PSUs) bore the respective costs. Chapter 6 compares fraud figures between domestic transactions and cross-border payments, both within and outside the EEA. Chapter 7 takes a more detailed look at country-specific findings for EU Member States, focusing on both absolute and relative levels of fraud. The annex explains the methodology of the data collection and analysis, and further outlines some potential quality issues persisting in the data.

Looking ahead, the general outlook with respect to overall payment fraud based on the presented analysis appears stable. The widespread adoption of the RTS for SCA and CSC has had a positive effect on reducing fraudulent payments, especially for transactions conducted within the EEA. Additionally, industry measures such as the global implementation of the EMV standard also continued to limit the opportunities to conduct fraud, e.g. with regard to the use of counterfeit cards. Nevertheless, it is important for the industry, regulators and consumers to remain alert.

The EBA and the ECB will continue to monitor fraud data and publish the aggregate data on a yearly basis. While this initial report is focused on a factual presentation of the data, future editions may

[3] Results presented 'from an issuing perspective' refer to payments made with cards issued within the EU/EEA and acquired worldwide. Results 'from an acquiring perspective' refer to transactions conducted using cards issued worldwide and acquired within the EU/EEA. The focus on the issuing perspective was chosen for simplicity as well as data quality considerations as regards data reported from the acquiring perspective.

[4] Data for Liechtenstein started to be reported for reference period H2 2022 onwards and hence does not cover the whole time series between H1 2022 and H1 2023 analysed in this report. In consequence, it was removed from the analysis included in this report.

include more detailed explanations underlying the data and observed trends. In the process, as new data becomes available and reporting quality further improves, the EBA and the ECB will also incorporate further data and analysis, with a view to enhancing transparency for all stakeholders and to informing security requirements that the EBA and the ECB will develop going forward.

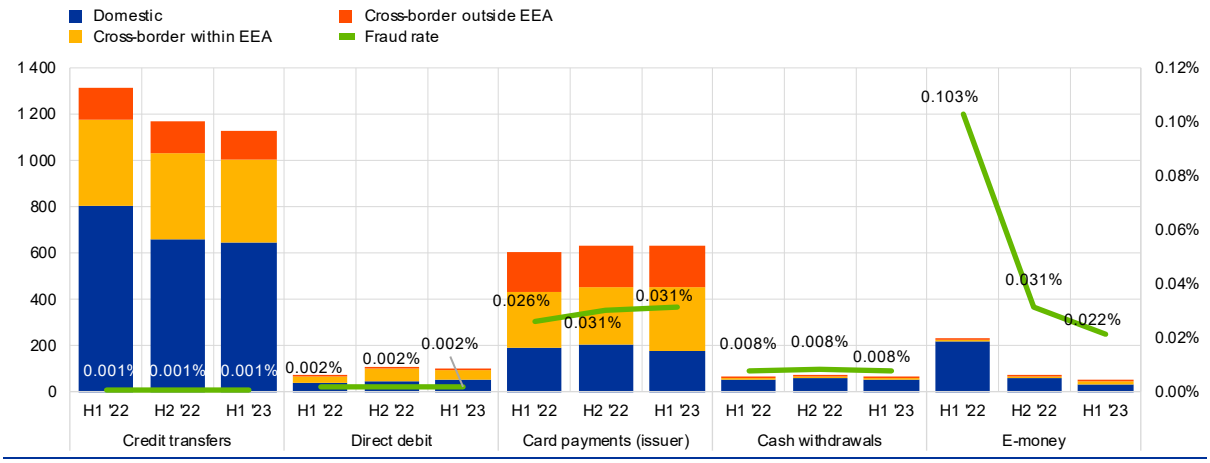
2. Levels of payment fraud

The total value of fraudulent transactions reported by the industry across the European Economic Area (EEA) amounted to EUR 4.3 billion in 2022 and EUR 2.0 billion in the first half of 2023. This considers the sum of all fraudulent transactions reported for credit transfers, direct debits, card payments, cash withdrawals and e-money transactions[5] (as per Chart 1a).

The highest fraud values between H1 2022 and H1 2023 were reported in credit transfers and card payments. In the first half of 2023, the total value of fraudulent credit transfers sent from PSPs in the EU/EEA and received worldwide amounted to EUR 1.131 billion (see Chart 1a), which was 14% lower compared with the first half of 2022. Card fraud using cards issued in the EU/EEA amounted to EUR 633 million in the first half of 2023, with fraud values remaining fairly stable over the three reporting periods. In comparison, the value of total fraudulent card payments acquired by EU/EEA PSPs (not shown) was higher, amounting to EUR 826 million in the first half of 2023. In contrast, the value of fraudulent direct debits, cash withdrawals and e-money transactions in absolute terms remained at more moderate levels (i.e. below EUR 100 million in the first half of 2023 in each case).

In relative terms, fraud rates (i.e. fraud as a share of the total value of transactions) remained at low and stable levels for credit transfers, direct debits and cash withdrawals. The vast majority of the value of overall electronic payment transactions was related to credit transfers (amounting to more than EUR 141 trillion in the first half of 2023). As a result, the fraud rate for this in value terms remained relatively low in comparison, i.e. at 0.001%[6] for the three reference periods between H1 2022 and H1 2023. Fraud rates for direct debits and cash withdrawals were on similar levels albeit slightly higher, at 0.002% and 0.008%, respectively.

Chart 1a: Absolute and relative levels of fraud by type of payment instrument (in values)
(left axis: total value of fraud (million EUR); right axis: fraud as a share of the total value of transactions of that type)

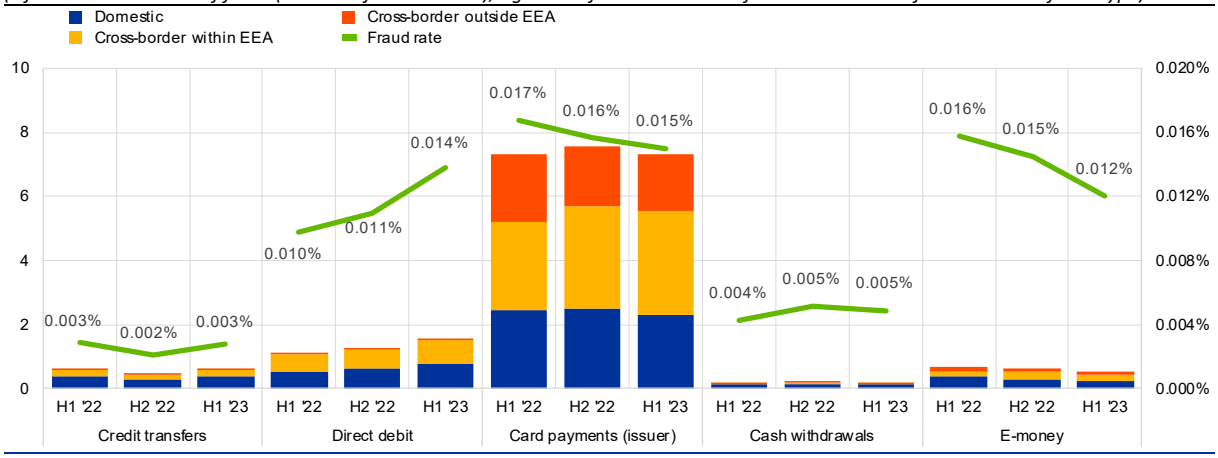


5 This refers to data as reported by the payer's PSP for all payment instruments with the exception of direct debits, for which data on fraud is reported by the payee's PSP given that these transactions are initiated by the payee.

6 A fraud rate of 0.001% implies that 1 cent per EUR 1 000 worth of transactions is subject to fraud.

In contrast, fraud rates appear noticeably higher for card payments and e-money transactions. For the former, the value of fraud as a share of the total value of card payments using cards issued in the EU/EEA slightly increased over the three reporting periods, from 0.026% in H1 2022 to 0.031% in H1 2023. The increased fraud rate for card payments in the last two reference periods compared with the first half of 2022 is the result of a decline in overall card payments of -12% year on year in H1 2023 that coincided with an increase in the value of card fraud per se of +4% year on year in the same period. For e-money transactions, the corresponding fraud rate in the first half of 2023 was at 0.022%, which is significantly lower than in the previous two reference periods.

Chart 1b: Absolute and relative levels of fraud by type of payment instrument (in volumes)
(left axis: total volume of fraud (millions of transactions); right axis: fraud as a share of the total volume of transactions of that type)



Turning to volumes, card payment fraud accounted for by far the largest number of fraudulent transactions between H1 2022 and H1 2023. The high number of fraudulent transactions in comparison to other instruments mirrors the fact that card payments account for the majority of electronic payments in volume terms. In H1 2023, the number of total card payments with cards issued in the EU/EEA amounted to around 48.77 billion transactions, out of which around 7.31 million transactions were fraudulent (see Chart 1b). In relative terms, card fraud volumes accounted for 0.015% of the total number of card payments in H1 2023, which marked a slight year on year decline from 0.017% in H1 2022. Overall, fraud rates for card payments in terms of volumes remained considerably below the corresponding figures for values in all three reporting periods that were analysed.

The fraud rate for direct debits in volume terms was noticeably higher than the corresponding fraud rate in value terms across all reference periods. Overall, around 1.50 million direct debit transactions were reported as fraudulent for the EU/EEA in H1 2023, which accounted for around 0.014% of the total number of direct debits during this period. The fraud rate of direct debit payments thereby increased over the three reference periods, from 0.010% in H1 2022 to 0.011% in H2 2022 and 0.014% in H1 2023.

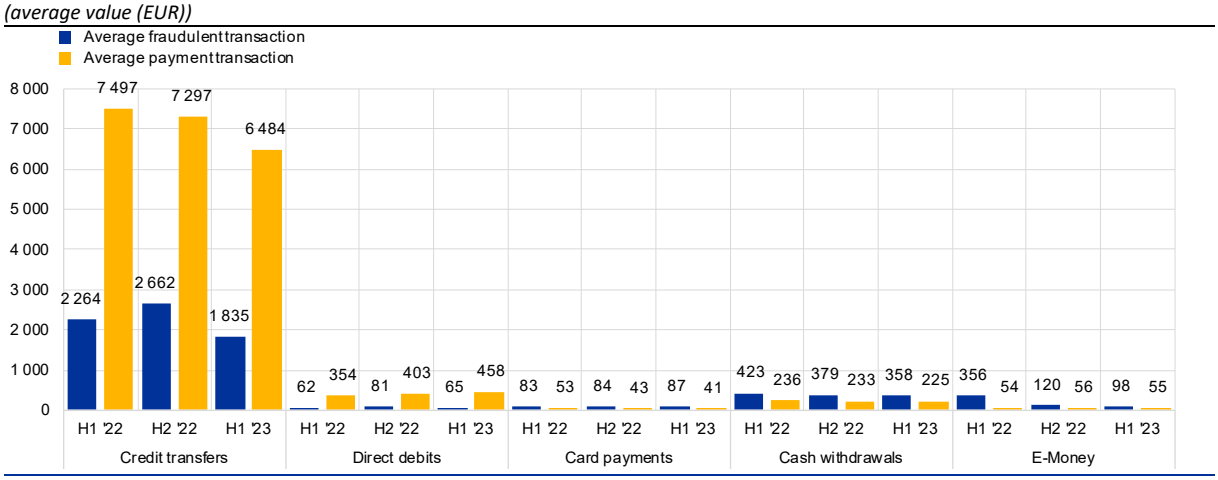
Fraud rates for e-money transactions in volume terms were on similar levels to those for card payments and direct debits. The volume of fraudulent e-money transactions amounted to around 540 000 transactions in H1 2023. In a similar way to card payments, the fraud rate for e-money

transactions in volume terms declined over the three reporting periods (from 0.016% in H1 2022 to 0.012% in H1 2023).

The reported volumes of fraudulent credit transfers and cash withdrawals were low both in absolute and relative terms. Whereas credit transfers accounted for a large share of total electronic transactions and fraud in value terms, they played a less significant role in terms of volumes. The total number of credit transfers sent from PSPs in the EU/EEA in H1 2023 amounted to 21.81 billion transactions, of which around 616 000 transactions were fraudulent. Consequently, the corresponding fraud rate for credit transfers in H1 2023 was at 0.003% (i.e. unchanged compared with H1 2022). The number of fraudulent cash withdrawals in H1 2023 amounted to around 174 000 transactions. Compared with a total number of 3.57 billion cash withdrawals during the same period, the corresponding fraud rate was at 0.005% (remaining fairly stable from previous reference periods).

The average value of a fraudulent transaction appeared highest for credit transfers compared with other payment instruments. In H1 2023, the average fraudulent credit transfer amounted to EUR 1 835, which however was substantially lower than the average value of a credit transfer in general (at EUR 6 485 in H1 2023; see Chart 2). In comparison, the average fraudulent cash withdrawal and e-money payment amounted to EUR 358 and EUR 98 in H1 2023, respectively. The average fraudulent card payment and direct debit transaction was even lower, at EUR 87 and EUR 65, respectively. This is not surprising, because credit transfers are the preferred instrument for high-value transactions, while direct debits and card payments are often used for lower-value retail payments in shops or for e-commerce. The observed average values related to fraudulent card payments, cash withdrawals and e-money transactions were higher than the average overall transaction value for these instruments. In contrast, the average fraudulent credit transfer or direct debit transaction was lower than the corresponding average transaction value for these instruments in general.

Chart 2: Average value of a transaction and a fraudulent transaction by payment instrument
(average value (EUR))



3. Main fraud types

The data collected allows for a more differentiated perspective on the type of fraud and the initiation channel used. Section 3.1 will look at electronically initiated credit transfers, card payments and e-money transactions and corresponding fraud, distinguishing between non-remotely initiated transactions (at the point of sale or terminal) and remote transactions (via the internet or electronic devices used for distance communication). Section 3.2 will provide an analysis of the main fraud types under PSD2 observed for each payment instrument.[7] The latter will further include a more detailed look at card fraud, which allows for a more granular breakdown of specific fraud types.

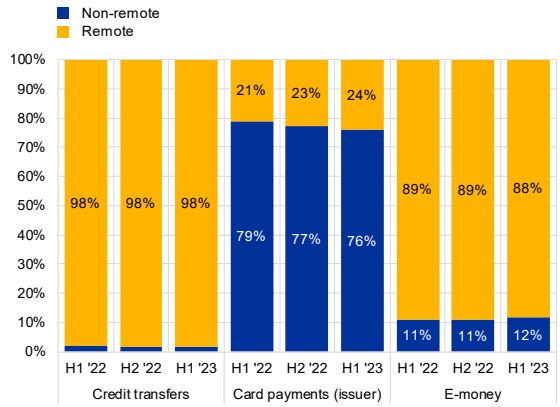
3.1 Remote versus non-remote transactions and fraud

Electronically initiated credit transfers are almost exclusively initiated remotely, both with regard to overall transactions and fraud. Around 98% of the total value of electronically initiated credit transfers and 99% of the value of corresponding credit transfer fraud, in each of the three reference periods analysed, related to payment transactions that were initiated remotely, i.e. via the internet or through a device that can be used for distance communication (see Charts 3a and 3b). The same overall trends are observed for volumes (see Charts 4a and 4b).

Chart 3: Value shares of non-remotely versus remotely initiated payment transactions and fraud

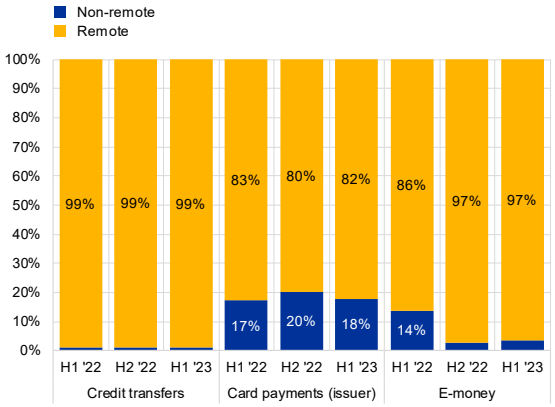
a) Value of payment transactions by instrument

(value of remotely and non-remotely initiated payments in % of the total value of payments per instrument)



b) Value of fraud by instrument

(value of remotely and non-remotely initiated fraudulent payments in % of the total value of fraud per instrument)



While the majority of card payment transactions were initiated non-remotely, card fraud was predominantly related to remotely initiated payments. Remote card payment fraud accounted for 82% of the value of card fraud in H1 2023 (80% in volume terms). In contrast, remotely initiated payments accounted for only around 24% of the total value of overall card transactions in H1 2023;

[7] According to the categorisation used, 'manipulation of the payer' only refers to the initiation of a fraudulent transaction by the payer. The manipulation of a payer to perform an action against their own interests, often used as one step in the process of fraud, usually leads to the initiation of a payment by the fraudster at a later point in time.

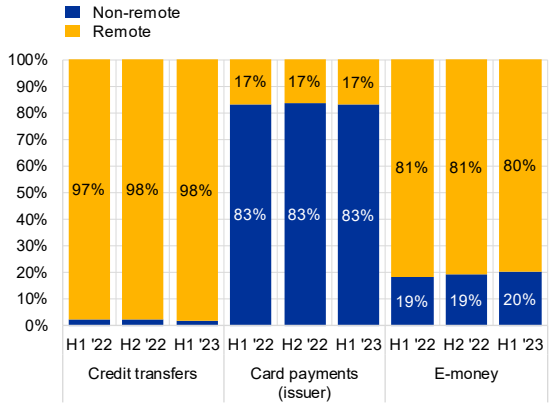
the corresponding share in volume terms was even lower (17%). In consequence, the relative fraud rate in H1 2023 was substantially higher for remote (0.101% in values; 0.068% in volumes) compared with non-remote payments (0.007% in values; 0.004% in volumes). This trend was observed across all three reference periods analysed.

In a similar way to credit transfers, e-money transactions were mostly initiated remotely. Close to 90% of the total value of e-money transactions related to remotely initiated transactions (i.e. payment transactions initiated via the internet or through a device that can be used for distance communication) in each of the three periods analysed (around 80% in volume terms). In terms of fraud, 97% of all e-money fraud in H1 2023 in terms of value was initiated remotely (95% in volume terms).

Chart 4: Volume shares of non-remotely versus remotely initiated payment transactions and fraud

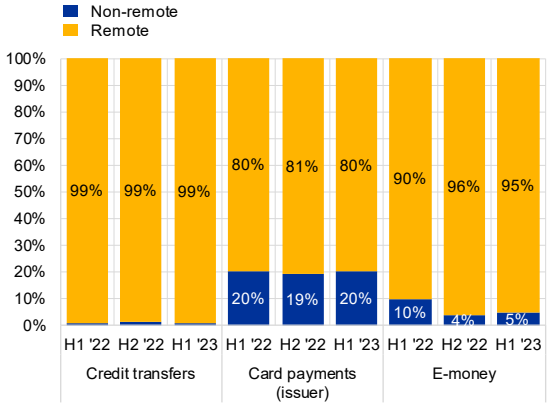
a) Volume of payment transactions by instrument

(number of remotely and non-remotely initiated payments in % of the total number of payments per instrument)



b) Volume of fraud by instrument

(number of remotely and non-remotely initiated fraudulent payments in % of the total volume of fraud per instrument)

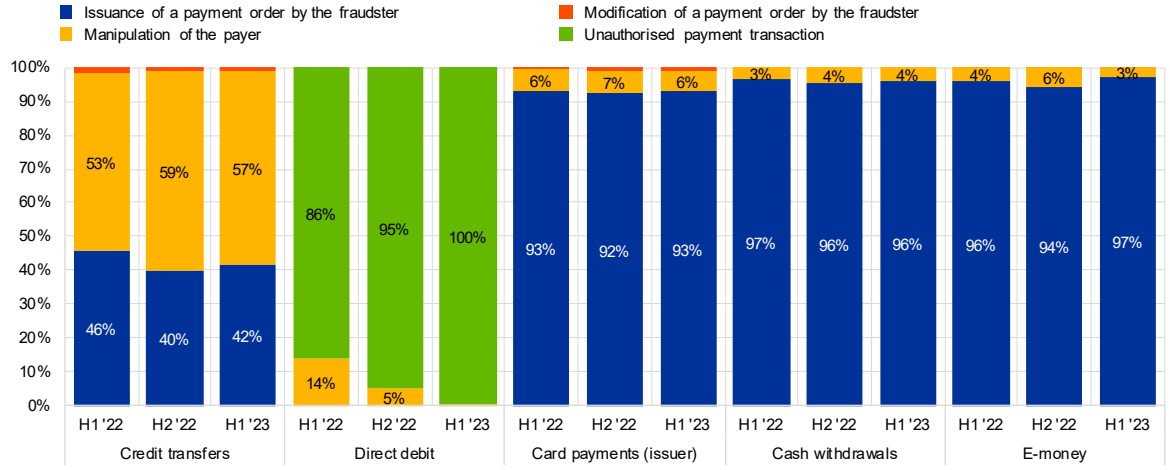


3.2 Fraud types by payment instrument

Fraud in card payments, cash withdrawals and e-money transactions was almost exclusively due to the issuance of payment orders by the fraudster. In each of the three reference periods analysed, more than 92% of the total value and around 98% of the total volume of card fraud was related to this type (see Charts 5 and 6). A more detailed analysis of underlying fraud types for this category of card payment fraud is provided below. In a similar way to card fraud, more than 95% of fraudulent cash withdrawals and e-money transactions in both value and volume terms were initiated by the fraudster. Manipulation of the payer to initiate a fraudulent transaction and modification of a payment order by the fraudster appeared to only play a very limited role with respect to card payments, cash withdrawals and e-money fraud.

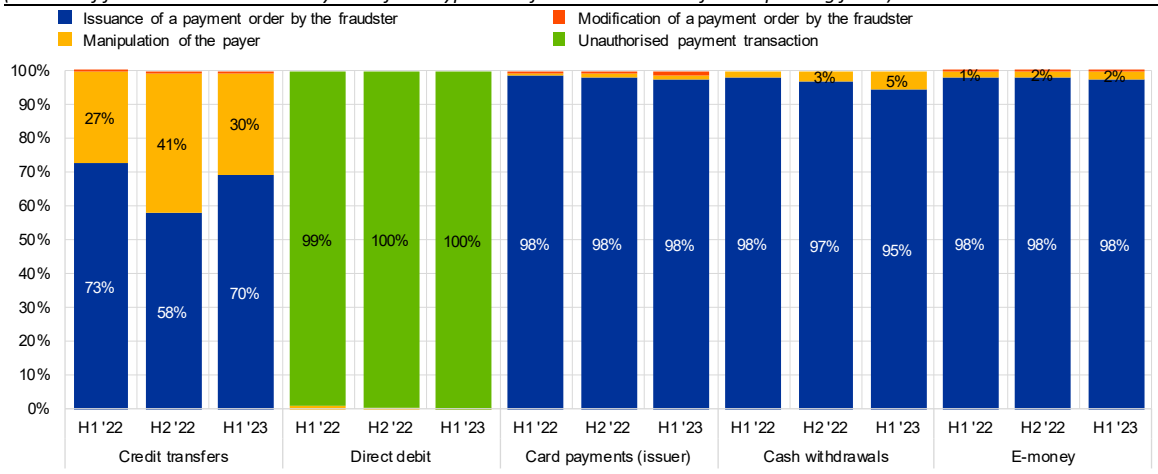
By contrast, for credit transfers a large share of fraudulent transactions was due to the manipulation of the payer to initiate a transaction. This type of fraud accounted for 57% of the total value of credit transfer fraud in H1 2023 (see Chart 5). In terms of volumes, the issuance of a payment order by the fraudster still appeared to be the more frequent type, accounting for close to 70% of fraudulent credit transfers in H1 2023 (see Chart 6).

Chart 5: Composition of the value of fraud by main types of fraud
(value of fraudulent transactions by main fraud type in % of the total value of corresponding fraud)



Finally, most cases of direct debit fraud were accounted for by unauthorised[8] payment transactions. More than 99% of all fraudulent direct debits in both volume and value terms were related to this type of fraud in H1 2023. While this percentage was also observed for both H1 and H2 2022 for the number of fraudulent direct debits, some more notable shares were observed with regard to the manipulation of the payer in value terms (i.e. 14% and 5% of the total value of direct debit fraud in H1 and H2 2022, respectively).

Chart 6: Composition of the volume of fraud by main fraud types
(number of fraudulent transactions by main fraud type in % of the total volume of corresponding fraud)



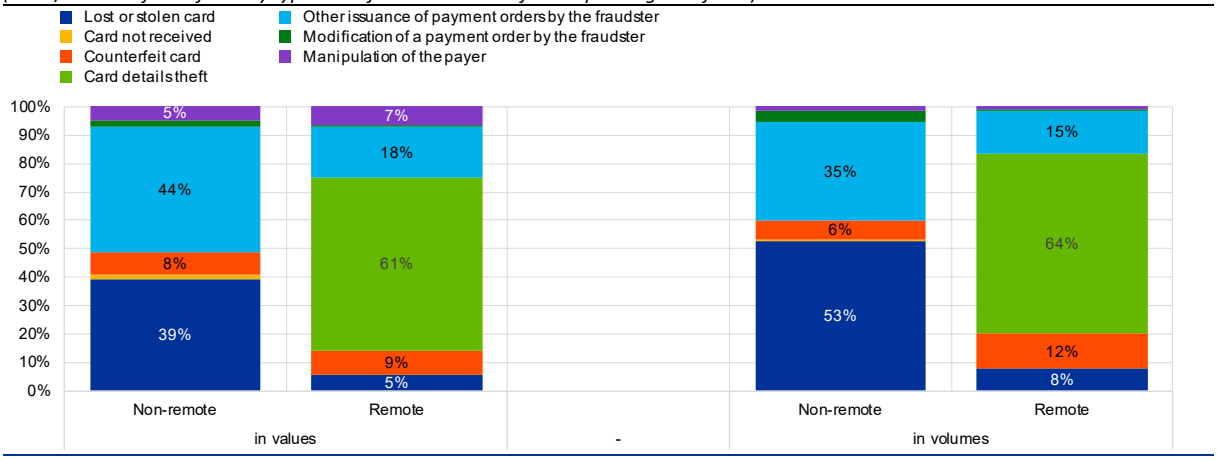
Around two-thirds of remote card fraud is due to card details theft. The collected data on card payment fraud contains additional breakdowns in terms of the fraud types underlying the broader category of issuance of a payment order by the fraudster. Chart 7 shows a more detailed composition

8 This report uses the term 'authorised transaction', which is consistent with the wording in the reporting requirements set out in the EBA Guidelines. However, the EBA and the ECB acknowledge that, since the development of the EBA Guidelines in 2018, legal discussions have evolved such that a transaction that is authenticated cannot automatically be assumed to also have been authorised. While in hindsight it would have been preferable for the EBA Guidelines to use the term 'authenticated', for the purpose of these Guidelines the term 'authorised' and its meaning will be retained and remain unchanged.

of card payment fraud in both value and volume terms for reference period H1 2023 only, which further distinguishes between non-remotely and remotely initiated fraudulent transactions. The theft of card details (e.g. via data breaches, phishing or other social engineering techniques) in H1 2023 accounted for 61% and 64% of remotely initiated card fraud in terms of value and volumes, respectively.[9] Counterfeit card fraud accounted for 9% of remote card fraud in value and for 12% in volume terms. Other types of remote issuance of a payment order by the fraudster accounted for 18% of remote card fraud in value and for 15% in volume terms. As mentioned above, only a low share of card fraud was due to the manipulation of the payer to initiate a payment, accounting for 7% in value and 1% in volume terms.

A large share of non-remote card payment fraud is conducted using lost or stolen cards. Lost or stolen cards accounted for 39% of the value of non-remote card fraud in H1 2023 and for 53% of the volume of fraudulent, non-remote card payments. In addition, 44% of card fraud in value terms (35% in terms of volumes) in H1 2023 was reported under the category of other types of fraud related to the issuance of a payment order by the fraudster. This includes, for instance, account takeovers and compromised application fraud, where fraudsters apply for a card in someone else's name or request a replacement card by falsely reporting theft or loss. In the wake of the global rollout and maturity of EMV terminals, non-remote card fraud using counterfeit cards played only a minor role in H1 2023, accounting for 8% of the value of non-remote card fraud (6% in volume terms).

Chart 7: Composition of the value and volume of card fraud by initiation channel and fraud type (H1 2023)
(value/volume of card fraud by type in % of the total value of corresponding card fraud)



[9] If fraudulent transactions include social engineering techniques, such as phishing, smishing, vishing or impersonation, the manipulation of the payer (to perform an action against their own interests) becomes part of the process.

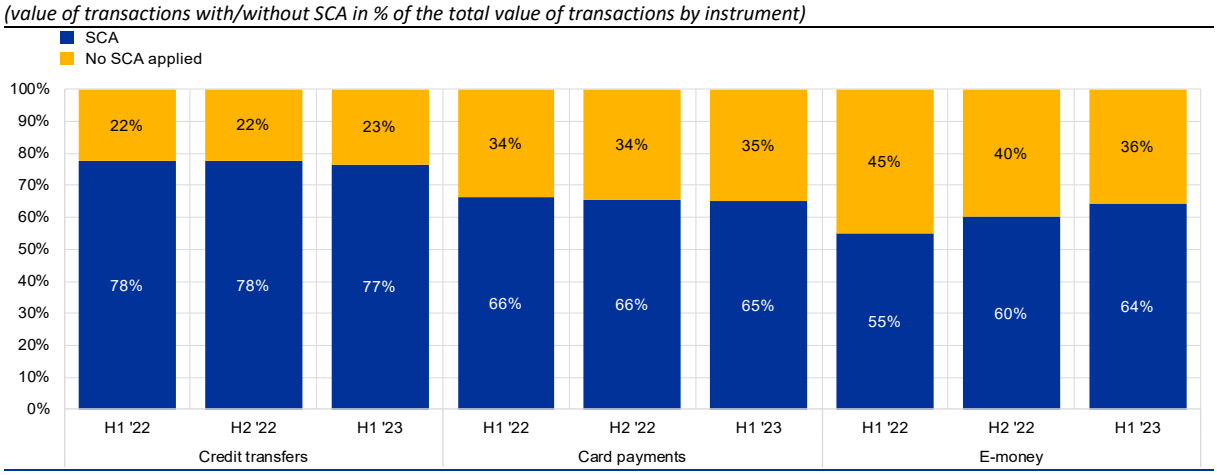
4. The role of strong customer authentication (SCA)

The present chapter focuses on the application of SCA in line with the requirements defined in Delegated Regulation 2018/389 with regard to Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (hereafter 'RTS on SCA and CSC') under the revised EU Payment Services Directive (PSD2). These enhanced security standards for payment service providers, drafted by the EBA in collaboration with the ECB, were published by the Commission in November 2017 and entered into force in September 2019, with a subsequent EBA opinion granting flexibility regarding the implementation for the subset of transactions that are e-commerce, card-based payment transactions until 31 December 2020. The chapter entails a more detailed analysis of the use of SCA with regard to electronically initiated credit transfers, card payments and e-money transactions (section 4.1), an overview of corresponding fraud rates observed for both transactions with and without SCA (section 4.2) as well as a further look into the use of exemptions to SCA as defined under the RTS on SCA and CSC (section 4.3).

4.1 Use of SCA for electronically initiated payments

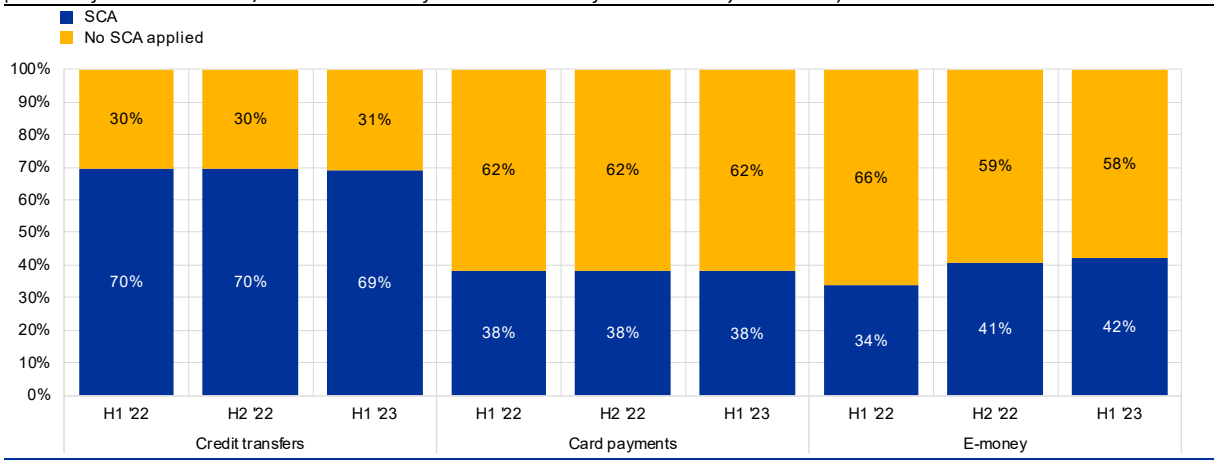
The majority of electronic payments in value terms in 2022 and H1 2023 were authenticated using SCA. Transactions authenticated using SCA accounted for 77% of all electronically initiated credit transfers in H1 2023 (see Chart 8). A similar share (78%) was observed for both semi-annual reference periods in 2022. Around two-thirds of the total value of electronically initiated card payments using cards issued in the EU/EEA was authenticated via SCA in each of the three reference periods analysed. The share of transactions authenticated via SCA was slightly lower for e-money transactions in comparison to credit transfers and card payments, accounting for 64% of the total value of e-money transactions in H1 2023.

Chart 8: Share of SCA v non-SCA transactions for credit transfers, card payments and e-money payments (in value)
(value of transactions with/without SCA in % of the total value of transactions by instrument)



The share of transactions without SCA was significantly larger in volume than in value terms, in particular for card payments and e-money transactions. While 69% of the total volume of electronically initiated credit transfers in H1 2023 was authenticated using SCA, SCA was applied only in 38% and 42% of the total number of electronically initiated card payments and e-money transactions, respectively (see Chart 9). The main reason for the observed difference between values and volumes lies in the fact that for a notable share of transactions, in particular with respect to non-remotely initiated card payments, PSPs applied the contactless payments at point of sale exemption granted under Art. 11 of the RTS on SCA and CSC.

Chart 9: Share of SCA v non-SCA transactions for credit transfers, card payments and e-money payments (in volumes)
(number of transactions with/without SCA in % of the total volume of transactions by instrument)



4.2 Relative fraud levels for transactions with and without SCA

Fraud rates for SCA-authenticated card payment transactions were consistently below fraud rates for card transactions without SCA. This pattern was observed both with respect to transactions conducted within the EEA and with respect to card payments acquired outside the EEA (see Charts 10 and 11). Fraud rates for transactions with SCA using cards issued in the EU/EEA and acquired by PSPs located in the EEA are substantially lower than corresponding fraud rates for overall card payments in both value (ranging between 0.013% in H1 2022 and 0.017% in H1 2023) and volume terms (0.006% in each reporting period).

Fraud rates for credit transfers were generally low, irrespective of the application of SCA or the geographical location of the receiving PSP, while the picture is more mixed for e-money transactions. As also depicted in Chart 10, observed fraud rates for credit transfers remained consistently at 0.002% or below across all categories analysed. Fraud rates for e-money payments within the EEA that were authenticated via SCA were lower than for transactions without SCA in terms of transaction volumes while, interestingly, the opposite was observed in value terms and for transactions received outside the EEA.

Chart 10: Fraud rates for SCA v non-SCA-authenticated transactions by payment instrument and geography (in value)
(value of fraud in % of the respective value of transactions)

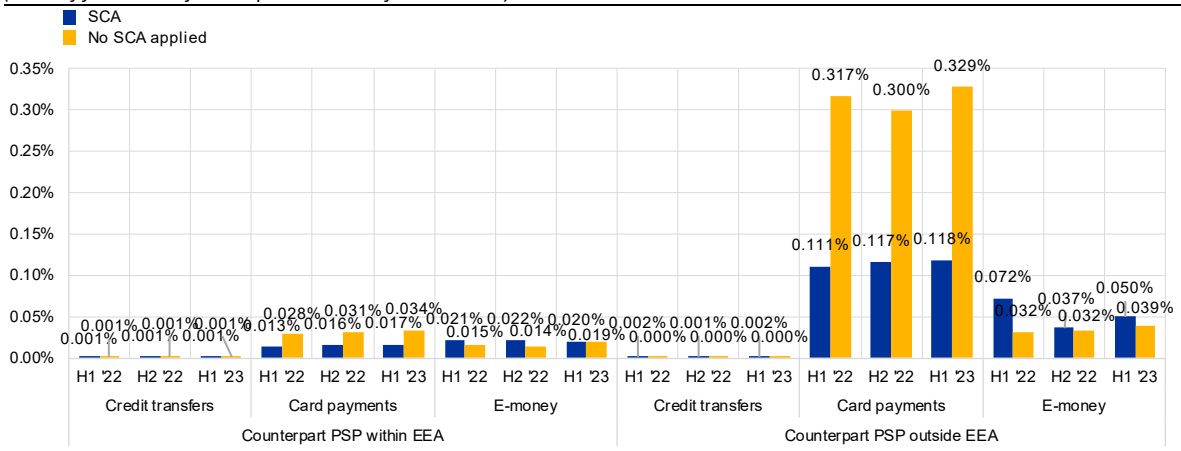
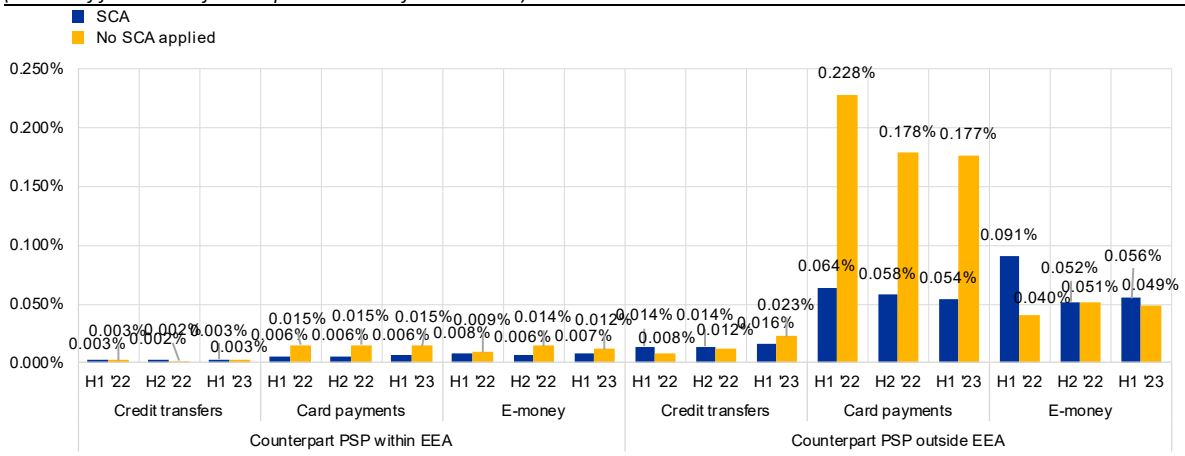


Chart 11: Fraud rates for SCA v non-SCA-authenticated transactions by payment instrument and geography (in volumes)
(volume of fraud in % of the respective value of transactions)



Fraud rates for transactions within the EEA were consistently lower compared with transactions where the counterpart PSP was outside the EEA. This is observed for both card payments and e-money transactions as well as in both value and volume terms. In particular fraud rates for card transactions acquired by PSPs outside the EEA for both SCA and non-SCA transactions were substantially higher than for other transactions. This confirms that SCA requirements imposed in the EU/EEA, through PSD2 and the technical standards developed by the EBA in close cooperation with the ECB, have the desired beneficial impact on fraud levels. As mentioned above, these trends were not observed for fraud rates related to credit transfers, where individual fraud rates were generally low for all categories.

4.3 Focus on transactions not authenticated via SCA

As non-SCA transactions showed higher fraud rates compared to SCA transactions, it is worthwhile to take a deeper look at these transactions. Charts 12, 14 and 15 show the composition of the number of non-SCA transactions by type of exemption or reason for not applying SCA separately for credit transfers, card payments and e-money transactions, also considering that exemptions may differ depending on the channel (remote or non-remote). Charts 13, 16 and 17 show corresponding fraud rates per exemption or reason for not applying SCA used for the three above-mentioned payment instruments.

Fulfilling a mandate under PSD2 and with the aim of finding a proper balance between the interest in enhanced security in payments and the needs of user-friendliness and accessibility of payments, the RTS on SCA and CSC has defined different exemptions to the principle of SCA based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

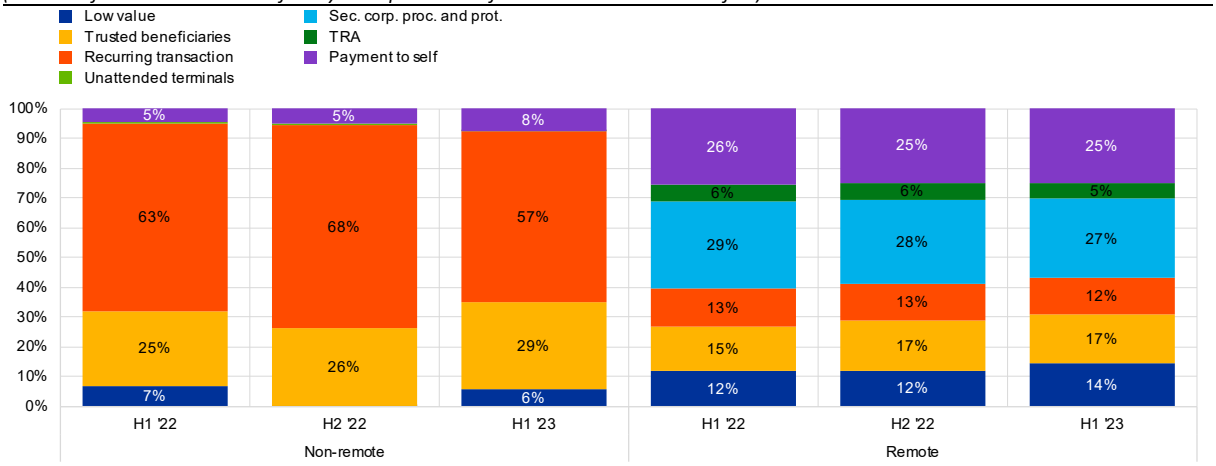
The exemptions under Art. 11 ('Contactless payments at point of sale') and Art. 16 ('Low-value transaction') of the RTS on SCA and CSC are linked to the same rationale, which considers both a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions. An exemption for 'unattended terminals' (Art. 12) is meanwhile meant for cases where the use of SCA may not always be easy to apply due to operational reasons (i.e. to avoid queues and potential accidents at toll gates or for other safety or security risks). Other exemptions, like 'trusted beneficiary' (Art. 13) and 'recurring transactions' (Art. 14), have instead in common the fact that the SCA-exempted payments are a repetition of a transaction once authorised with SCA. For the former, the payee is recalled from a list of trusted beneficiaries previously created by the payer; for the latter, the payment is subsequent to a previous transaction created, amended or initiated via SCA and is automatically initiated using the same parameters as said previous transaction.

Art. 15 of the RTS on SCA and CSC refer to credit transfers between accounts held by the same natural or legal person, providing a specific SCA exemption if the payer and the payee are the same natural or legal person and both payment accounts are held by the same account servicing PSP. Yet another exemption to SCA can be applied to transactions where payers are not consumers, provided that 'secure corporate payment processes and protocols' that guarantee at least equivalent levels of security to those provided by PSD2 have been implemented (Art. 17). Furthermore, the RTS on SCA and CSC allows for an additional exemption for remote payments that, based on the result of a 'transaction risk analysis' (TRA), pose a low level of risk (Art. 18).

For credit transfers, the type of exemption to SCA that PSPs most frequently applied was for recurring transactions under Art. 14 of the RTS on SCA and CSC in the case of non-remote transactions and for secure corporate processes and protocols under Art. 17 in the case of remote transactions. In H1 2023, close to 60% of all non-remotely initiated credit transfers exempted from SCA were recurring transactions. Corresponding shares for H1 and H2 2022 were even higher, at 63% and 68% respectively (see Chart 12). Payments to trusted beneficiaries were the second most frequently used exemption for these types of transactions, accounting for 29% of non-remote credit

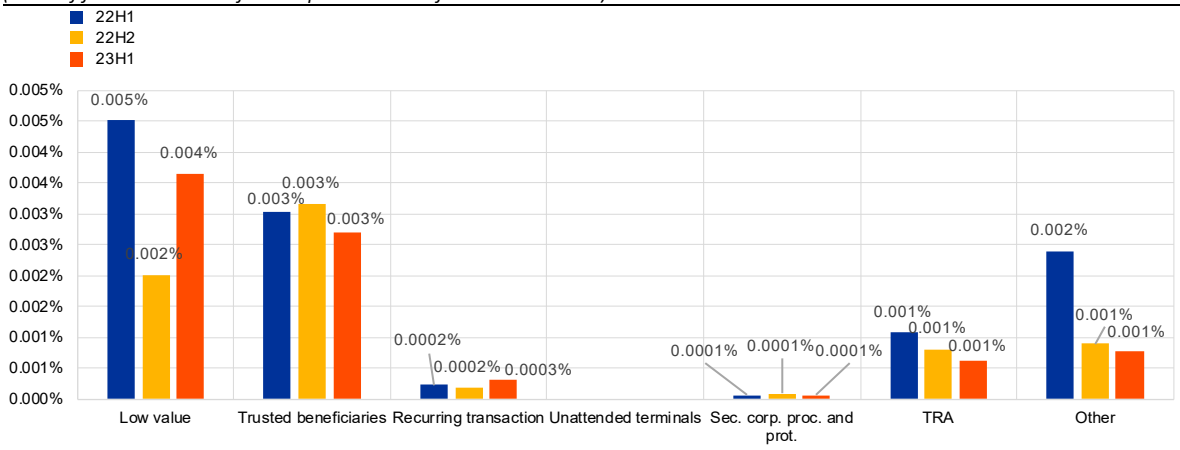
transfers for which no SCA was applied.[10] As regards remotely initiated credit transfers, 'secure corporate payment processes and protocols' under Art. 17 of the RTS on SCA and CSC appeared to be the most used exemption from SCA, accounting for close to 30% of remote credit transfers without SCA. In addition, around one-quarter of the number of remote credit transfers without SCA seem to have been exempted under Art. 15 of the RTS on SCA and CSC due to the payer and the payee being the same natural or legal person. Low value, trusted beneficiary and recurring transaction exemptions also accounted for between 12% and 17% of exempted remote transactions. In contrast, the use of the TRA exemption appeared rather limited with respect to credit transfers.

Chart 12: Composition of the volume of electronic credit transfers without SCA by exemption type
(number of non-SCA credit transfers by exemption in % of total non-SCA credit transfers)



Note: the category of 'low value' exemption shown in this graph refers to exemptions under Art. 11 of the RTS on SCA and CSC on contactless low-value payments for non-remote transactions and to exemptions under Art. 16 for remote transactions.

Chart 13: Fraud rates of credit transfers without SCA by exemption type (in value)
(value of fraud as a share of the respective value of total transactions)

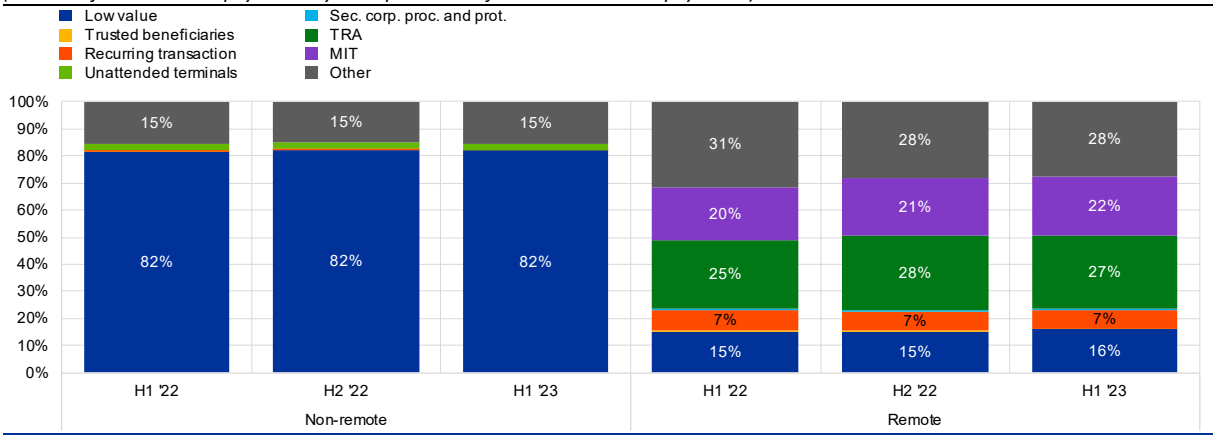


Fraud rates for SCA-exempted credit transfers in value terms were highest for the low value and trusted beneficiary exemptions (Art. 16 and 13), while recurring transactions (Art. 14) and secure corporate processes and protocols (Art. 17) appeared to carry lower fraud risk. The latter two exemptions, while accounting for a noticeable number of SCA-exempted transactions, showed very

[10] The finding that no low value exemptions appear to have been applied for non-remote credit transfers in H2 2022 is currently under investigation and may be revised in future data submissions.

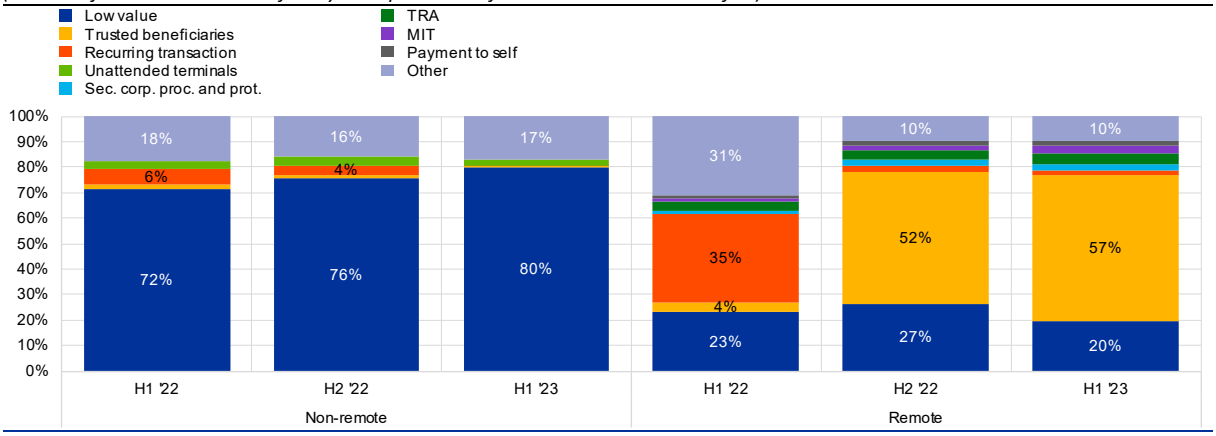
low fraud rates across all reference periods (see Chart 13). Fraud rates for TRA-based exemptions appeared moderate, i.e. at similar levels to corresponding fraud rates for credit transfers overall. In comparison, fraud rates for transactions exempted from SCA based on the low value or trusted beneficiary exemptions appeared three to five times higher compared to the observed fraud rates for overall credit transfers (0.001%).

Chart 14: Composition of the volume of electronic card payments without SCA by reason for not applying SCA
(number of non-SCA card payments by exemption in % of total non-SCA card payments)



Note: the category of 'low value' exemption shown in this graph refers to exemptions under Art. 11 of the RTS on SCA and CSC on contactless payments for non-remote transactions and to exemptions under Art. 16 for remote transactions.

Chart 15: Composition of the volume of e-money transactions without SCA by reason for not applying SCA
(number of non-SCA credit transfers by exemption in % of total non-SCA credit transfers)



Note: the category of 'low value' exemption shown in this graph refers to exemptions under Art. 11 of the RTS on SCA and CSC on contactless payments for non-remote transactions and to exemptions under Art. 16 for remote transactions.

The majority of non-remote card payments and e-money transactions where SCA was not applied were due to the contactless low value exemption. This exemption under Art. 11 of the RTS on SCA and CSC accounted for around 82% of the total volume of non-SCA card payments and for between 72% and 80% of non-SCA e-money transactions that were initiated non-remotely (see Charts 14 and 15). Among the remainder, no dedicated exemption specified under the RTS on SCA and CSC showed strong relevance for non-remote payments. In this regard it should be recalled that while non-remotely initiated payments accounted for the majority of card payments (83% in H1 2023; see Chart 4a), they only related to a rather minor share of e-money transactions (20% in H1 2023).

TRA was the most used exemption to SCA for remote card payments, while a significant number of non-SCA payments was classified as outside the scope of SCA requirements under PSD2. In H1 2023, 27% of remote card payments without SCA were exempted due to TRA; similar shares were observed in 2022 (see Chart 14). At the same time, however, 22% of non-SCA remote card payments were classified as merchant-initiated transactions (MIT)[11] in H1 2023 and 28% were exempted due to other reasons (even higher shares in H1 and H2 2022). These relatively high shares of transactions that were considered by PSPs to be outside the scope of SCA requirements warrant further investigations to ensure SCA requirements under PSD2 are applied correctly. [12]

For remote e-money transactions, for more than half of all non-SCA transactions in H2 2022 and H1 2023 the trusted beneficiary exemption was used. This is different compared with H1 2022, where 35% of non-SCA transactions were recurring transactions and only 4% related to a trusted beneficiary[13]. In addition, the low value exemption under Art. 16 of the RTS on SCA and CSC was applied for 20% or more of non-SCA e-money transactions that were initiated remotely in all three reference periods. In a similar way to card payments, a significant share of remote e-money transactions was exempted due to other reasons, equally requiring further follow-up investigations.

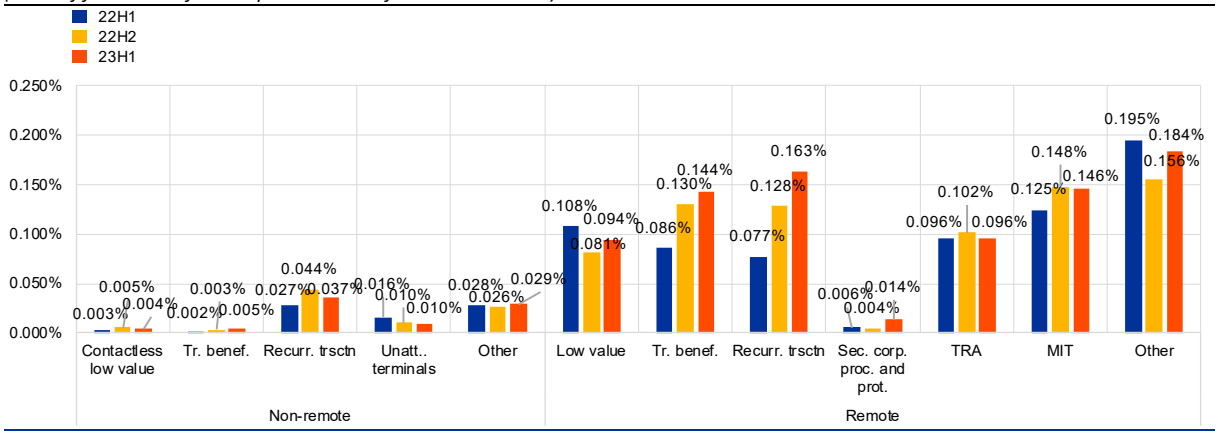
Fraud rates for SCA-exempted remote card payments were relatively high across most exemption types with the exception of secure corporate processes and protocols. Individual fraud rates for remote card payments without SCA were mostly between 0.1% and 0.2% of the corresponding total value of respective card payments, with regard both to exemptions defined under PSD2 and to transaction types outside the scope of the PSD2 SCA requirements (see Chart 16). The only exception were transactions exempted from SCA due to secure corporate processes and protocols being used, where corresponding fraud rates were below the overall fraud rates for card payments in general. Fraud rates related to non-remote card payments exempted from SCA were overall much lower in comparison to corresponding fraud rates for remote payments, in most cases in line with or below the overall fraud rates for card payments in general.

11 MIT refers to card-based payment and e-money transactions that meet the conditions specified by the Commission in Q&A 2018_4131 and Q&A 2018_4031 and which are, as a result, considered as payee-initiated and not subject to the requirement in Article 97 of PSD2 to apply SCA.

12 For example, as per relevant EBA Single Rulebook Q&As, mail order and telephone order (MO-TO) transactions should not be exempted from SCA and thus should not be reported under the category of other reasons for not applying SCA (see EBA Q&As 2019_4788 and 2019_4790).

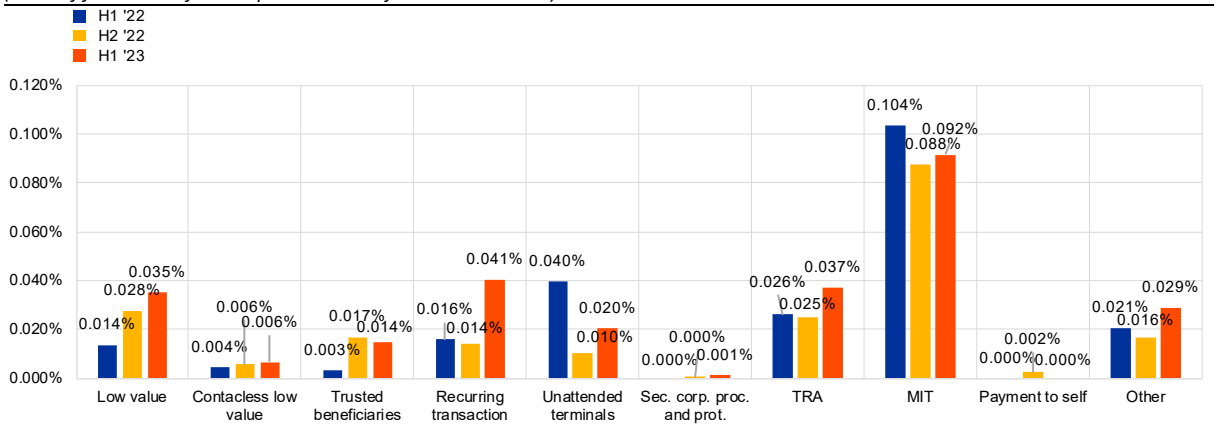
13 Please note that these divergences across reference periods may indicate improved reporting among PSPs in later reference periods instead of changes in payment trends. The corresponding figures are currently still under investigation and may be subject to further revisions in the future.

Chart 16: Fraud rates for card payments without SCA by initiation channel and reason for not applying SCA (in value)
(value of fraud in % of the respective value of total transactions)



Fraud rates for e-money transactions without SCA varied noticeably by exemption type or reason for not applying SCA. In a similar way to credit transfers and card payments, transactions exempted based on secure corporate processes and protocols showed very low to no fraud (see Chart 17). In contrast, transactions classified as MIT experienced fraud rates of 0.088% of the total value of transactions or above, bearing in mind that these transactions only accounted for a relatively small fraction of non-SCA e-money payments (see Chart 15). Fraud rates for the more often used contactless low value (non-remote), low value (remote) and trusted beneficiary exemptions appeared smaller compared to fraud rates for overall e-money transactions, while transactions exempted due to other reasons showed higher fraud rates.

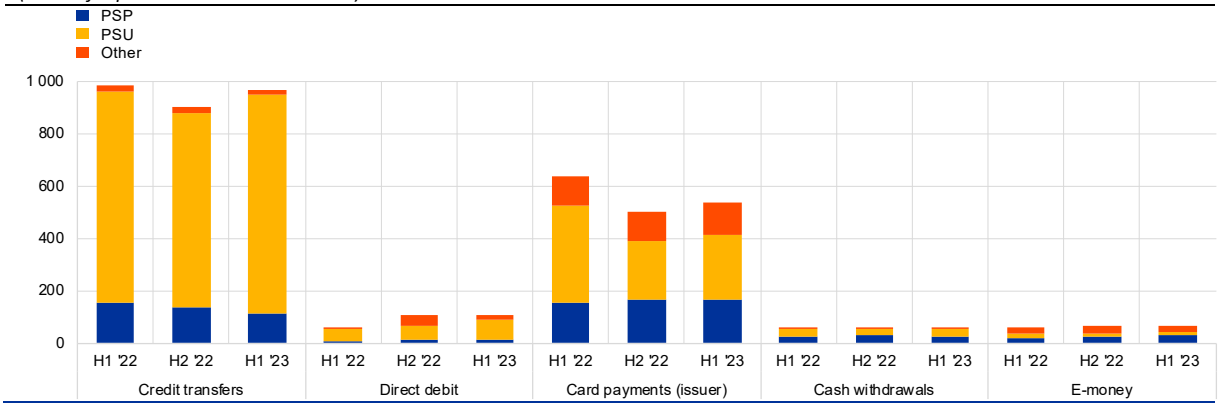
Chart 17: Fraud rates for e-money transactions without SCA by reason for not applying SCA (in value)
(value of fraud in % of the respective value of total transactions)



5. Losses due to fraud

Besides information on the level of fraudulent transactions in both volume and value terms, further information is collected on reported losses due to fraud. These refer to the losses borne by the reporting PSP, its payment service user (PSU) or others (e.g. the PSP counterpart to the respective transaction), reflecting the actual impact of fraud on a cash flow basis. Final fraud losses are reported by PSPs for the period in which they were recorded in the PSP's books, which may be disassociated timewise from the period in which the actual fraudulent transactions took place.[14] Unless stated otherwise, presented figures in this chapter refer to reference period H1 2023.

Chart 18: Total value of reported losses due to fraud by liability bearer
(value of reported losses in million EUR)



The highest overall losses due to fraud across liability bearers were reported for credit transfers and card payments. PSPs reported losses of EUR 967 million for credit transfers and EUR 537 million for card payments with cards issued in the EU/EEA (see Chart 18). Reported total losses for direct debits, cash withdrawals and e-money transactions were much lower, being slightly above EUR 100 million for direct debits in both H2 2022 and H1 2023 while remaining significantly below EUR 100 million for cash withdrawals and e-money transactions across all three reporting periods analysed. In comparison, reported losses for card payments acquired in the EU/EEA using cards issued worldwide (EUR 940 million; not shown in the chart) were higher than losses for transactions with cards issued in the EU/EEA.[15] Findings for reported losses due to fraud appear in line with the trends observed for overall fraud levels (see chapter 2).

Substantial shares of reported losses due to fraud seem to be borne by PSUs. Liabilities with regard to reported losses for card payments and cash withdrawals were approximately equally split between PSUs on one side, who bore 45% of reported losses for card payments and 51% of the losses for cash withdrawals, and PSPs along with other entities on the other side (see Chart 19). Meanwhile, the vast

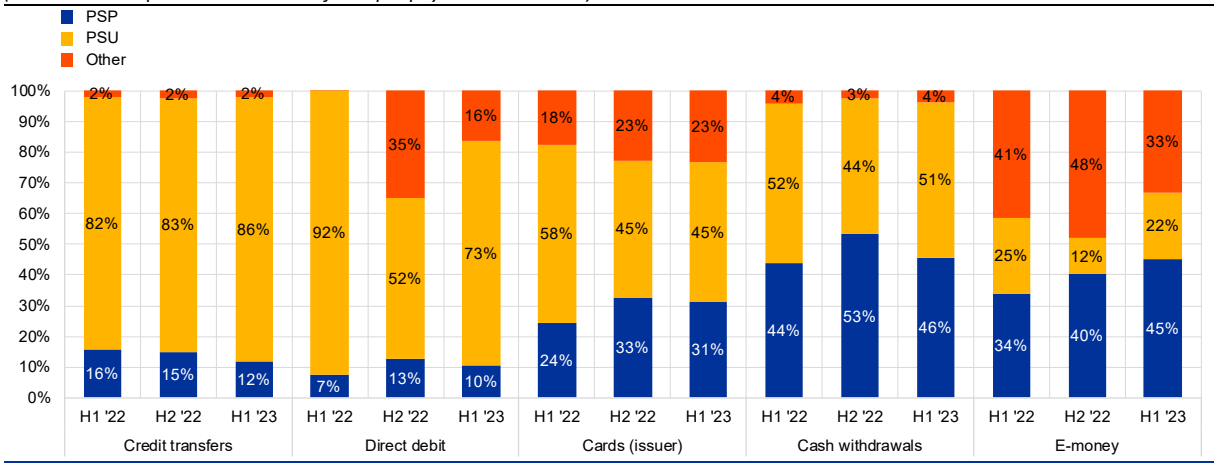
[14] Reported loss figures do not take into account refunds by insurance agencies because they are not related to fraud prevention for the purposes of PSD2.

[15] In H2 2022, reported losses for card payments acquired in the EU/EEA using cards issued worldwide accounted for the largest losses reported across all instruments (amounting to EUR 1 068 million).

majority of losses relating to fraudulent credit transfers were borne by the PSU (86% in H1 2023). In a similar way to credit transfers, a large share of losses for direct debits were borne by the PSU (73% of losses for direct debits in H1 2023). The picture appeared slightly different for e-money fraud, where less than 25% of fraud losses were borne by PSUs.

The distribution of the liability for fraud losses between PSUs and PSPs diverges significantly across the EEA. In a significant number of countries, PSUs bore more than half of the reported losses due to card payment fraud, at times as much as 80% of all losses or more (not shown). In some other countries, by contrast, the share borne by PSUs remained below 30% or even less, with the bulk of the remainder borne by PSPs and/or by other means, such as insurance contracts. Similar though less extreme divergences were observed for credit transfers (not shown), where in the vast majority of countries the PSU had to bear most or all of the losses, while in four countries PSPs bore between 35% and 71% of the losses. Due to persisting issues in the quality of the data reported for some countries, it remains difficult at this stage to make fully accurate comparisons across countries. In consequence, the present report refrains from providing a full depiction of the respective distributions of liabilities at country level.

Chart 19: Composition of losses by liability bearer and payment instrument
(share in total reported losses due to fraud per payment instrument)



6. The geographical dimension of fraud

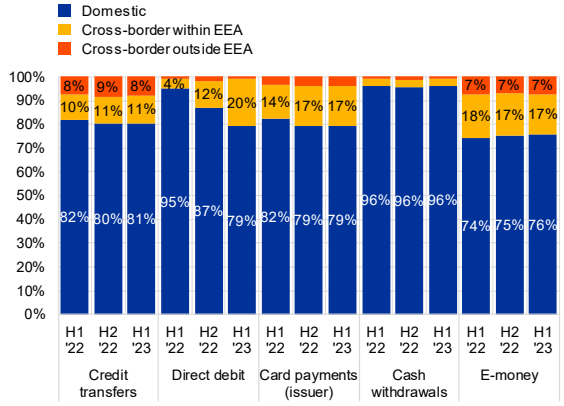
Whereas most payment transactions were domestic[16], most card payment fraud was related to cross-border transactions. The value of domestic credit transfers and card payments accounted for between 79% and 82% of the total value of credit transfers and card payments, respectively, in each of the three reference periods analysed (see Chart 20a); in volume terms, the shares of domestic in total transactions ranged between 95% and 96% for credit transfers and between 82% and 83% for card payments (see Chart 21a). In contrast, more than two-thirds of card fraud was related to cross-border transactions in both value and volume terms (see Charts 20b and 21b). Cross-border card fraud in H1 2023 accounted for 71% of the total value of card fraud and 68% of the total volume of fraudulent transactions using cards issued in the EU/EEA.

In addition, a large share of fraudulent credit transfers and direct debits took place across borders. As regards credit transfers, 43% of the total value of credit transfer fraud and 36% of the volume of fraudulent credit transfers were related to cross-border payments in the first half of 2023. For direct debits, cross-border fraud accounted for around half of total fraud in both value and volume terms. In contrast, the majority of fraudulent cash withdrawals was domestic (87% in value and 74% in volume terms in H1 2023). For e-money transactions domestic transactions accounted for more than two-thirds of the total value of fraud, while the share of cross-border fraud appeared higher in volume terms (55% for H1 2023).

Chart 20: Composition of payment transactions and fraud by instrument and geographical dimension I

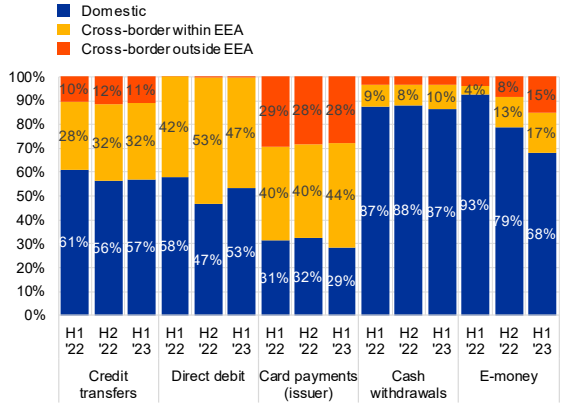
a) Value of payment transactions

(value of payments by geographical dimension in % of the total value of transactions for each instrument)



b) Value of fraudulent payment transactions

(value of fraud by geographical dimension in % of the total value of fraud for each instrument)

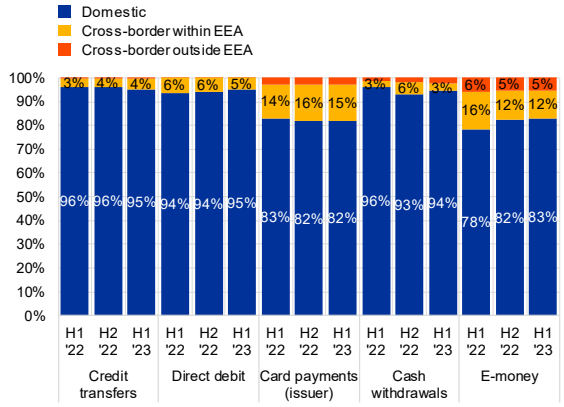


16 Domestic payments comprise those transactions where the sending and receiving PSP (and for non-remote card payments additionally the location of the point-of-sale terminal or ATM) are located in the same country.

Chart 21: Composition of payment transactions and fraud by instrument and geographical dimension II

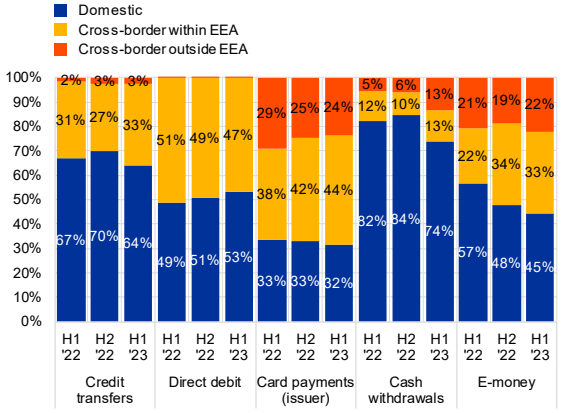
a) Volume of payment transactions

(volume of payments by geographical dimension in % of the total number of transactions for each instrument)



b) Volume of fraudulent payment transactions

(volume of fraudulent transactions by geographical dimension in % of total fraud for each instrument)



Significant shares of card payment and e-money fraud were related to cross-border transactions with PSPs located outside the EEA. Cross-border transactions outside the EEA accounted for almost 30% of the value of card fraud using cards issued in the EU/EEA in H1 2023, compared with only 4% of the total value of card payments. Similarly, such transactions accounted for more than 20% of e-money fraud in H1 2023 in terms of volumes, in comparison with only 5% of total e-money payments.

7. A country-by-country and regional perspective on fraud

For this inaugural report, the quality of the data reported to the EBA and the ECB is not sufficient to allow for robust country-by-country comparisons of payment fraud levels. The EBA and ECB continue to work hard with national authorities to enhance the data quality for future editions of the report, including, where possible, retrospective corrections of data that the EBA and ECB have already received. However, in order to accommodate the interests of stakeholders to some extent, this chapter offers some country-specific insights into fraud, in aggregate and for each of the five payment instruments separately.

Absolute fraud levels by country appear connected to the overall value and volumes of respective payment transactions, while relative fraud rates vary noticeably across countries. Tables 1 and 2 provide an overview of the total value and volume of fraud in both absolute and relative terms by individual reporting country and payment instrument for reference period H1 2023. The majority of fraudulent payments took place in those countries that accounted for larger numbers of overall payment transactions.

As regards **credit transfers**, relative fraud rates in terms of both value and volumes remained in general rather low across all countries, i.e. significantly below 0.01% of total credit transfers for all countries with one exception. The lowest absolute levels of fraud were observed for Iceland (amounting to 125 fraudulent transactions with a value of EUR 398 000). In relative terms, the highest fraud rate in value terms was observed for Malta at 0.006%, while the Netherlands accounted for the highest fraud rate in terms of volumes (0.014%[17]).

Direct debits show extremely low fraud rates across all countries except for the Netherlands. The lowest fraud levels among countries reporting non-zero fraud were reported by Lithuania (two fraudulent transactions with a value EUR 145). The highest fraud levels were reported for the Netherlands, at 1.2 million fraudulent transactions with a total value of EUR 61 million. The latter also experienced the largest fraud rates both in terms of volume (0.109%) and value (0.031%).

In a similar way to credit transfers, **fraudulent card payments** were concentrated in those countries where more transactions occurred. Fraudulent card payments reported by issuing PSPs located in the respective countries for H1 2023 show the lowest fraud volume in Cyprus (7 800 transactions) and the highest in France (around 3 million transactions). The latter also reported the highest card fraud value (at EUR 211 million). Card fraud as a share of the total value of card payments ranged from 0.009% in Finland to 0.087% in Iceland. The highest fraud rate in terms of volume was observed for France (0.032%).

[17] Please note that the data reported for the Netherlands at the cut-off date for this analysis still contained several reporting errors, which will be resolved with subsequent data submissions and reflected in future editions of the present report.

Cash withdrawals showed generally low fraud rates across countries in H1 2023 with some exceptions. The highest fraud rates in value terms were observed for Denmark (0.053%), the Netherlands (0.047%) and France (0.029%). In contrast, very low levels of fraud and corresponding fraud rates were observed for Latvia and Romania. In volume terms, the highest fraud rates were observed for Bulgaria [18] (0.076%), the Netherlands (0.029%) and Denmark (0.021%), while particularly low relative fraud levels were observed for Estonia, Latvia and Slovenia. No fraudulent cash withdrawals were reported for Iceland in H1 2023.

Fraudulent e-money transactions in H1 2023 appeared to be highly concentrated in two countries, which also accounted for the majority of overall e-money payments. Relative fraud rates exceeded a rate of 0.020% in four countries in terms of volumes and in five countries in terms of value. The highest fraud share in volume terms was observed for Italy and Spain at 0.024%. The highest fraud share in value terms was observed for Slovakia, at 0.12%.

[18] This fraud rate currently appears strongly overestimated due to an incorrect data submission, which will be corrected when data is reported for forthcoming reporting periods.

Table 1: Absolute and relative levels of payment fraud in value terms (H1 2023, value in EUR)

Country	Credit transfers		Direct debits		Cards (issuer)		Cash withdrawals		E-money	
	Value of fraudulent transactions	Fraud in % of total payments	Value of fraudulent transactions	Fraud in % of total payments	Value of fraudulent transactions	Fraud in % of total payments	Value of fraudulent transactions	Fraud in % of total payments	Value of fraudulent transactions	Fraud in % of total payments
AT	28 300 241	0.001%	16 921	0.000%	7 313 044	0.021%	287 204	0.001%	4 957	0.003%
BE	72 403 381	0.002%	4 347 782	0.005%	30 275 027	0.041%	1 254 574	0.010%	0	0.000%
BG	7 975 287	0.003%	0	0.000%	2 579 493	0.035%	182 646	0.002%	680 441	0.016%
CY	1 344 917	0.001%	159 506	0.008%	1 099 218	0.021%	19 324	0.001%	226 042	0.011%
CZ	20 295 420	0.001%	0	0.000%	10 717 851	0.034%	707 313	0.004%	0	0.000%
DE	146 516 621	0.000%	3 029 141	0.000%	64 755 673	0.025%	13 743 048	0.008%	32 323	0.015%
DK	18 756 456	0.001%	0	0.000%	10 658 067	0.027%	1 207 558	0.053%	2 950	0.001%
EE	3 460 872	0.002%	0	0.000%	1 014 230	0.021%	53 763	0.002%	0	0.000%
ES	52 994 617	0.001%	1 549 870	0.000%	60 191 062	0.037%	2 336 667	0.004%	1 025 153	0.025%
FI	20 537 896	0.001%	0	0.000%	2 999 247	0.009%	119 574	0.003%	700	0.001%
FR	155 903 705	0.001%	26 230 967[19]	0.002%	211 361 921	0.054%	19 747 278	0.029%	104 844	0.016%
GR	19 868 324	0.004%	0	0.000%	10 006 456	0.030%	1 911 448	0.013%	178 344	0.035%
HR	5 404 435	0.001%	0	0.000%	2 393 388	0.027%	89 741	0.002%	22 909	0.004%
HU	20 132 574	0.001%	0	0.000%	8 944 988	0.041%	431 363	0.004%	0	0.000%
IE	32 441 554	0.001%	28 708	0.000%	21 031 364	0.035%	411 054	0.006%	986 516	0.003%
IS	398 273	0.000%	0	0.000%	4 828 174	0.087%	0	0.000%	1 035	0.000%
IT	26 686 866	0.001%	667 943	0.000%	32 724 076	0.019%	7 840 645	0.008%	14 089 309	0.040%
LT	10 496 228	0.004%	145	0.000%	15 609 500	0.052%	429 395	0.006%	401 579	0.004%
LU	4 849 779	0.000%	0	0.000%	4 942 624	0.053%	157 978	0.008%	34 885 130	0.025%
LV	3 375 418	0.002%	0	0.000%	869 403	0.019%	4 664	0.000%	0	0.000%
MT	2 276 131	0.006%	0	0.000%	1 335 034	0.041%	14 335	0.002%	131 185	0.001%
NL	162 487 711	0.001%	60 504 837	0.031%	32 029 596	0.036%	7 790 217	0.047%	7 228	0.001%
NO	25 387 079	0.001%	0	0.000%	9 347 274	0.019%	134 850	0.009%	32 999	0.010%
PL[20]	211 352 265	0.001%	515	0.000%	52 644 713	0.016%	1 869 925	0.001%	0	0.000%
PT	3 557 632	0.000%	138 083	0.001%	9 862 807	0.015%	311 001	0.002%	13 950	0.001%
RO	13 716 082	0.001%	0	0.000%	6 271 106	0.024%	97 404	0.000%	8 045	0.023%
SE	51 200 058	0.001%	354	0.000%	9 912 696	0.019%	831 306	0.009%	94 231	0.008%
SI	3 084 887	0.002%	0	0.000%	2 233 289	0.039%	22 890	0.001%	3 993	0.005%
SK	6 046 077	0.001%	13 138	0.001%	4 747 771	0.039%	215 040	0.002%	118 939	0.120%
EU/EEA	**1 131 250 786**	**0.001%**	**96 687 909**	**0.002%**	**632 699 092**	**0.031%**	**62 222 205**	**0.008%**	**53 052 802**	**0.022%**

19 This figure currently appears strongly inflated due to an incorrect data submission by one reporting PSP, which will be corrected when data is reported for forthcoming reporting periods.

20 Please note that reported absolute values for Poland are currently strongly inflated (by a factor of around 4) due to an incorrect data submission, for which corrected data have been submitted after the cut-off date of the present analysis and will be considered for future editions of the report.

Table 2: Absolute and relative levels of payment fraud in volume terms (H1 2023)

Country	Credit transfers		Direct debits		Cards (issuer)		Cash withdrawals		E-money	
	Volume of fraudulent transactions	Fraud in % of total payments	Volume of fraudulent transactions	Fraud in % of total payments	Volume of fraudulent transactions	Fraud in % of total payments	Volume of fraudulent transactions	Fraud in % of total payments	Volume of fraudulent transactions	Fraud in % of total payments
AT	12 620	0.003%	55	0.000%	63 620	0.008%	567	0.001%	82	0.003%
BE	23 949	0.002%	15 360	0.006%	188 498	0.011%	2 515	0.004%	0	0.000%
BG	755	0.001%	0	0.000%	24 755	0.011%	960	0.076%[21]	4 259	0.006%
CY	141	0.001%	269	0.004%	7 822	0.009%	59	0.001%	873	0.021%
CZ	15 143	0.002%	0	0.000%	79 277	0.006%	635	0.001%	0	0.000%
DE	75 163	0.002%	11 824	0.000%	638 036	0.011%	32 151	0.004%	268	0.003%
DK	5 014	0.001%	0	0.000%	78 200	0.008%	2 207	0.021%	28	0.000%
EE	2 640	0.002%	0	0.000%	8 354	0.004%	62	0.000%	0	0.000%
ES	27 400	0.002%	5 726	0.001%	1 146 976	0.023%	7 340	0.002%	23 007	0.024%
FI	7 190	0.001%	0	0.000%	32 302	0.003%	379	0.001%	3	0.000%
FR	44 577	0.002%	224 424[22]	0.010%	3 047 131	0.032%	53 641	0.010%	1 263	0.003%
GR	9 231	0.003%	0	0.000%	150 606	0.016%	2 875	0.004%	4 801	0.020%
HR	2 241	0.001%	0	0.000%	26 051	0.008%	399	0.001%	682	0.004%
HU	8 563	0.004%	0	0.000%	93 262	0.011%	1 801	0.004%	0	0.000%
IE	13 265	0.003%	62	0.000%	174 228	0.014%	1 556	0.003%	11 118	0.005%
IS	125	0.001%	0	0.000%	9 444	0.008%	0	0.000%	19	0.000%
IT	9 242	0.001%	142	0.000%	339 031	0.010%	16 006	0.004%	252 236	0.024%
LT	10 137	0.004%	2	0.000%	133 399	0.011%	2 295	0.005%	3 795	0.005%
LU	1 229	0.002%	0	0.000%	48 914	0.027%	478	0.006%	236 291	0.009%
LV	2 522	0.002%	0	0.000%	9 652	0.004%	14	0.000%	0	0.000%
MT	587	0.007%	0	0.000%	8 247	0.017%	46	0.001%	1 144	0.005%
NL	275 786	0.014%	1 238 110	0.109%	377 663	0.012%	25 439	0.029%	112	0.001%
NO	4 846	0.001%	0	0.000%	66 074	0.005%	460	0.001%	135	0.002%
PL	36 822	0.001%	4	0.000%	130 271	0.003%	1 901	0.001%	0	0.000%
PT	1 153	0.001%	213	0.000%	211 648	0.017%	1 982	0.001%	1 007	0.002%
RO	4 116	0.001%	0	0.000%	64 055	0.007%	315	0.000%	46	0.003%
SE	18 093	0.001%	17	0.000%	97 521	0.005%	17 053	0.014%	63	0.006%
SI	355	0.000%	0	0.000%	23 370	0.014%	71	0.000%	92	0.004%
SK	3 574	0.001%	391	0.002%	28 360	0.006%	432	0.001%	108	0.017%
EU/EEA	**616 479**	**0.003%**	**1 496 599**	**0.014%**	**7 306 767**	**0.015%**	**173 639**	**0.005%**	**541 432**	**0.012%**

21 This fraud rate currently appears strongly overestimated due to an incorrect data submission, which will be corrected when data is reported for forthcoming reporting periods.

22 This figure currently appears strongly inflated due to an incorrect data submission by one reporting PSP, which will be corrected when data is reported for forthcoming reporting periods.

Annex: reporting methodology

Process for payment fraud data collection

The data collection process for payment fraud reporting to the EBA and the ECB follows a systematic approach that ensures consistency and comprehensiveness across all reporting entities. PSPs, as defined by PSD2, are required to submit statistical data on fraud related to various payment instruments to the CA of the home MS (EBA Guidelines point 5.1). This data is collected on a semi-annual basis except for PSPs that benefit from an exemption under Article 32 of PSD2, and e-money institutions that benefit from the exemption under Article 9 of the E-Money Institutions Directive (Directive 2009/110/EC) on the taking up, pursuit and prudential supervision of the business of electronic money institutions, which need only report the set of data requested on an annual basis with data broken down into two periods of six months (EBA Guidelines points 3.1 and 3.2). PSPs should submit their data within the timelines set by the respective competent authorities (EBA Guidelines point 3.3). Competent authorities subsequently share the data in aggregated form with both the EBA and the ECB.

Since 2022, detailed semi-annual data on payment fraud has also been collected from PSPs under the ECB Regulation on payments statistics. The regulation applies to the euro area, while non-euro-area EU Member States can comply with the reporting under the ECB Regulation on payments statistics on a voluntary basis. The data requirements on fraud include inter alia those defined under the EBA Guidelines. To streamline the reporting process and reduce the reporting burden for PSPs and national authorities, data reported in accordance with the ECB Regulation on payments statistics to the ECB is currently used to fulfil the reporting requirements to both EBA and ECB under the EBA Guidelines. In this case data reported to the ECB in accordance with the ECB Regulation on payments statistics is used to extract relevant aggregates in accordance with the requirements under the EBA Guidelines and subsequently shared with the EBA. Where this applies, the corresponding data was used as the basis for the present analysis.

Scope of the data

The data considers three types of PSPs, namely credit institutions, payment institutions and electronic money institutions. The data used for this report covers credit transfers, direct debits, card payments, cash withdrawals and e-money transfers. The geographical coverage refers to all EU Member States plus two non-EU EEA countries (Iceland and Norway[23]). The reporting periods covered by the present analysis include H1 2022, H2 2022 and H1 2023. The data used as the basis for this report has a cut-off date of 19 January 2024 with respect to data reported to the ECB in accordance with the ECB Regulation on payments statistics and 6 June 2024 with respect to data for the remaining EU/EEA countries reported to the EBA under the EBA Guidelines on fraud reporting under PSD2.

[23] Liechtenstein only reported data from H2 2022 onwards. As this does not cover the whole time series analysed in this report (i.e. H1 2022 to H1 2023), data for Liechtenstein was removed from the analysis.

Data quality and integrity

Data quality and integrity are key in the reporting process. The EBA in collaboration with the ECB has established a comprehensive set of validation rules to ensure the data reported by PSPs is accurate and reliable. These are published in the EBA Guidelines on fraud reporting under PSD2 and in the EBA reporting framework 2.10 package. In addition, data collected under the ECB Regulation on payments statistics is subject to an encompassing set of data quality checks defined under a corresponding data quality framework, in order to ensure the formal validity, consistency and plausibility of the data. Finally, NCAs and NCBs also already perform relevant data quality checks on the information received from reporting agents at national level.

Data limitations and qualifications

The data reported still contains several data limitations such as some incomplete data submissions or methodological misclassifications on the side of reporting agents. Several data quality findings are currently still being investigated by the respective competent authorities and/or national central banks together with the reporting agents. As a result, several reporting errors have already been identified, which are expected to be resolved with subsequent data submissions and corrections and will be reflected in future editions of the present report. Where identified and considered relevant, quality disclaimers have been added throughout the report.

Due to the short time series considered for the present analysis, caution should be exercised when interpreting trends over time.


eba
European
Banking
Authority


EUROPEAN CENTRAL BANK
EUROSYSTEM