European Banking Authority

EUROPEAN CENTRAL BANK
EUROSYSTEM

2025 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
SCT Inst	SEPA instant credit transfers
TRA	Transaction Risk Analysis

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 six reference periods H1 2022, H2 2022, H1 2023, H2 2023, H1 2024 and H2 2024 and analyses 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, in terms of both, value and volume.

The report provides 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. In addition, it comprises a box on instant credit transfers based on data collected under the ECB Regulation on payment statistics [Regulation (EU) No 1409/2013]. This edition builds on the report published in August 2024.

The report assesses payment fraud reported by industry across the European Economic Area (EEA), which amounted to EUR 4.2 billion in the year 2024. Most payment fraud by value arose from credit transfers and card payments, across all six reference periods analysed. More specifically, in 2024 the total value of fraudulent credit transfers sent by payment service providers (PSPs) in the EU/EEA amounted to EUR 2.5 billion, with a fraud rate of 0.001%, and the value of fraudulent card transactions in the EU/EEA amounted to EUR 1.3 billion, with a fraud rate of 0.033%. By volume, card transactions using cards issued in the EU/EEA accounted for the largest number of fraudulent transactions in 2024, while other payment types saw much lower figures.

Fraud involving card payments, credit transfers and e-money transactions predominantly occurred in remote transactions, while for cards the majority of 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.

In most card payment fraud transactions, fraudsters directly issued the payment order, often using stolen credentials for remote card fraud or lost/stolen physical cards for non-remote card fraud. Manipulation of the payer accounted for more than half of the total value of fraudulent credit transfers.

SCA was applied to the majority of electronic payments by value, especially for credit transfers (around 77%). However, electronically initiated card payments and e-money transactions were only SCA-authenticated in 40% and 38% of the number of transactions in 2024, respectively, influenced by contactless payments where SCA may not be applied, and which has become the standard in paying at the point of sale. In general, SCA-authenticated transactions showed lower fraud rates than non-SCA transactions, especially for card payments. For credit transfers, however higher fraud rates were observed for SCA-authenticated transactions, likely reflecting the fact that SCA is typically applied to higher-risk or higher-value payments. Furthermore, fraud rates for card payments were about

seventeen times higher when the counterpart was outside the EEA, where SCA may not be required, compared to domestic transactions. These findings suggest a beneficial impact of SCA requirements introduced under PSD2 on the security of electronic payments.

Losses due to fraud were distributed differently among liability bearers depending on the payment instrument, possibly, due to the divergent applicable liability regimes and the effectiveness of redress mechanisms available to payment service users (PSUs), among other reasons. In 2024, PSUs bore 38% of the losses that arose from card payments and 53% for both direct debits and cash withdrawals, while this share was 26% for e-money transactions. In contrast, PSUs endured around 85% of total fraud losses for credit transfers in 2024. Furthermore, the distribution of fraud losses between PSUs and PSPs diverged significantly across countries: in relation to card payments, in a significant number of countries, PSUs bore more than half of the fraud losses, at times even more than 87% of all losses, while in some other countries the share was as low as 12%.

Most payment transactions were domestic, but the majority of card payment fraud as well as a large share of credit transfer and direct debit fraud were cross-border. A notable share of fraudulent card payments (30% in value terms in 2024) was 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 SCA has had a positive effect on reducing fraudulent payments, especially within the EEA. Additionally, industry measures such as the global implementation of the EMV standard have also helped 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 PSUs 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 regulatory authority 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 apply as amended since 1 July 2020, 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 (NCBs), 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. In order to streamline this process and lessen the burden of reporting PSPs/NCAs/non-euro national central banks (NCBs), a Memorandum of Understanding (MoU) was set up for the reporting of payment fraud data that must be provided to the EBA and the ECB under article 96(6) of the PSD2. In particular, under this MoU the reporting process is streamlined by means of a single reporting of payment fraud data via the NCBs to the ECB, which then submits the data to the EBA.

The analysis presented in this report is based on semi-annual data for six reference periods – i.e. H1 2022, H2 2022, H1 2023, H2 2023, H1 2024 and H2 2024. Although some data under the EBA Guidelines has been reported since 2019, full coverage of EU/EEA countries only applies for the reference period H1 2022 onwards. The results are presented separately for the main means of payment, i.e. credit transfers, direct debits, card payments, cash withdrawals and e-money transactions. Presented figures for card payments are derived from an issuing, rather than acquiring, perspective.[2]

[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] 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.

Unless stated otherwise, all aggregate figures refer to the whole EU/EEA, excluding Liechtenstein[3], the Netherlands[4] for direct debits and Bulgaria[5] for the second semester of 2024 for credit transfers. 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 on payment fraud in the EU so far, 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 NCAs and/or NCBs and that may lead to additional retrospective data corrections when data will be 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 years, caution is advised when interpreting trends over time. Finally, because fraud data is subject to regular revisions, figures reported in different editions of this report should not be directly compared. Such revisions may be necessary to correct errors in preceding submissions from reporting entities, or to update data as a result of legal clarifications brought about over time. A recent such clarification is the ruling of the European Court of Justice in case C-661/22 on the definition of e-money[6] and the subsequent Q&A 2022_6336[7] of the European Commission, which may result in revisions in the future of data reported in the past under specific categories.

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/EEU 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.

The EBA and the ECB will continue to monitor fraud data and publish the aggregate data on an annual basis. The report focuses on a factual presentation of the data which is complemented by causal explanations of the data and observed trends, where available.

3 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 H2 2024 analysed in this report. In consequence, it was removed from the analysis included in this report.

4 Direct debits data for the Netherlands was excluded from the aggregate analysis due to confidentiality reasons.

5 Credit transfer data for H2 2024 from Bulgaria was excluded from the aggregate analysis due to a data quality issue that significantly impacted the readability of the affected charts.

6 See https://curia.europa.eu/juris/document/document.jsf?text=&docid=283050

7 See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2022_6336

2. Levels of payment fraud

The total value of fraudulent payment transactions reported by the industry across the European Economic Area (EEA) amounted to EUR 4.2 billion in 2024. This represents a year-on-year increase of EUR 602 million or 17% from 2023 to 2024. The total value of fraudulent transactions includes the sum of all fraudulent transactions reported for credit transfers, direct debits, card payments (from the issuer perspective), cash withdrawals and e-money[8] transactions (as per Chart 1a).

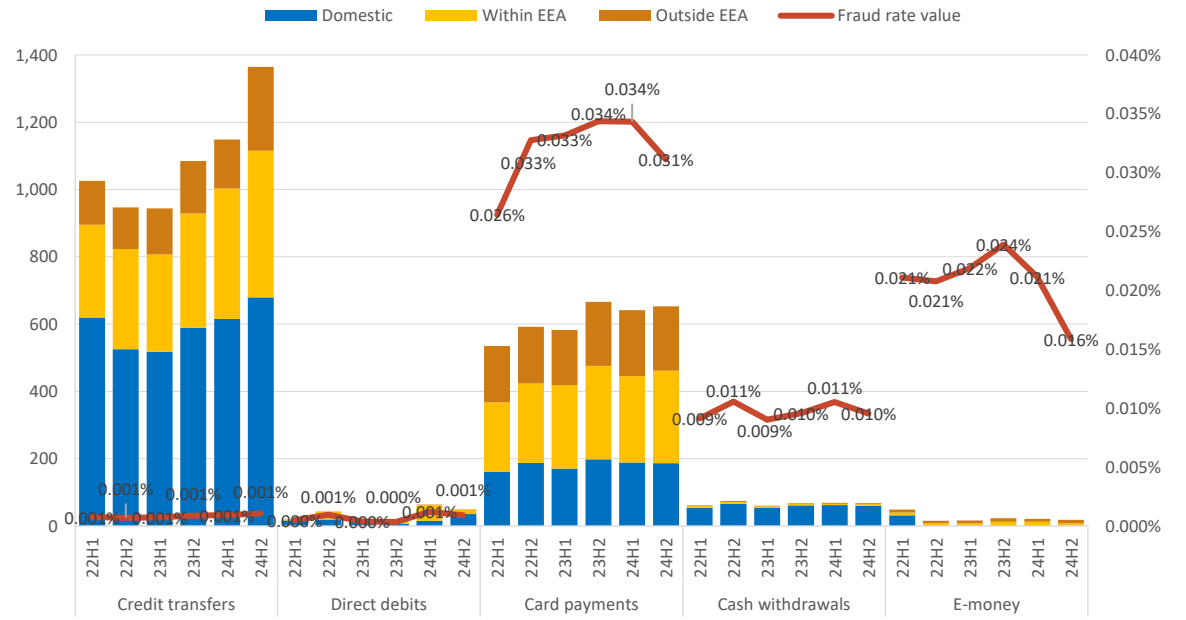
In absolute terms, between 2022 and 2024, fraud was higher for credit transfers and card payments. In 2024, the total value of fraudulent credit transfers reached EUR 2.5 billion (see Chart 1a), representing an increase of 24% compared to 2023. The values reported for card fraud show an increase of 4% from 2023 to 2024, with funds stolen using cards issued in the EU/EEA, totalling EUR 1.3 billion in 2024. The sum of the values of fraudulent direct debits, cash withdrawals and e-money transactions amounted to EUR 349 million in 2024, a year-on-year increase of 26%, mainly driven by the evolution of fraudulent direct debits that increased from EUR 36 million in 2023 to EUR 112 million in 2024. These absolute values may also reflect the impact of differing spending limits across payment instruments, (e.g. often lower for cards and higher for credit transfers and direct debits), which can influence the potential amount exposed to fraud per transaction.

Across all payment instruments combined, the annual fraud rate (i.e. measured as fraud relative to the total value of transactions in a calendar year), remained stable and low throughout the 2022–2024 period, at approximately 0.002%. Annual fraud rates for credit transfers, direct debits[9] and cash withdrawals (0.001%, 0.001% and 0.010% for 2024, respectively) are substantially lower when compared to card payments and e-money (0.033% and 0.018% for 2024, respectively).

8 Following a clarification regarding the definition of e-money that the EU Commission provided in Q&A 2022_6336, published in January 2025, stating that funds are only considered e-money if they are voluntarily accepted as a separate monetary asset by a natural or legal person other than the issuer, e-money fraud data that will be reported in the future may contain retrospective corrections for some Member States.

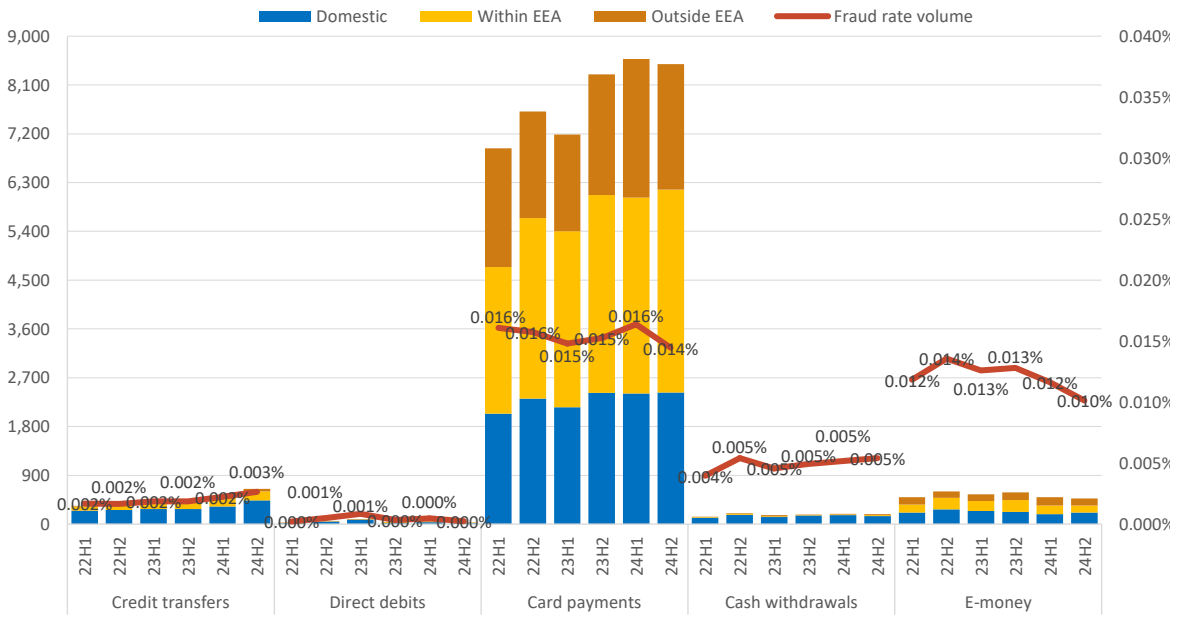
9 Reference is made to the EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) *"20. Regarding the reporting of fraudulent payment transactions in the context of direct debits, the EBA clarifies that refunds under eight weeks should not be automatically reported, as they do not always indicate fraud cases; such transactions should be reported only if they were subject to fraud and the reporting PSP was aware that this was the case, without implying any legal obligation to ask the payment service user whether this was the case."*

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)



As shown in Chart 1a, credit transfers have the lowest fraud rate. Given that credit transfers accounted for the highest share of fraud in value terms, that rate reflects the large overall value of this instrument and the fact that SCA is more often applied when using it. The annual fraud rates, while remaining considerably low, increased for credit transfers, direct debits and cash withdrawals, while decreasing for card payments and e-money, from 2023 to 2024.

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)



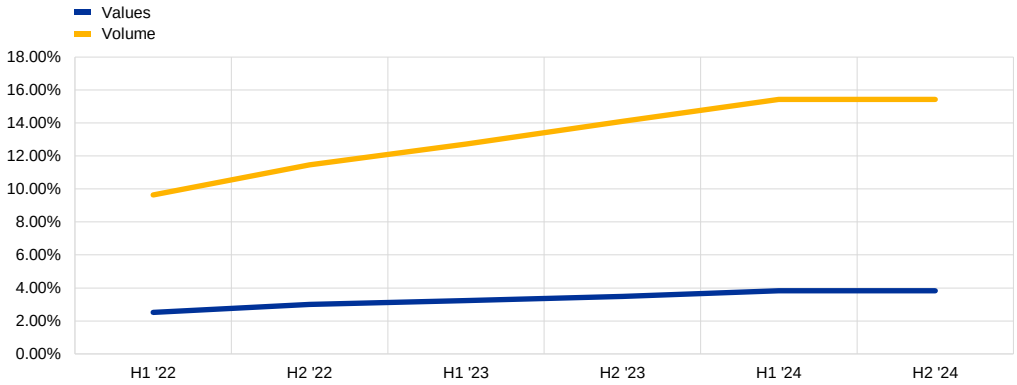
In relation to volumes, the number of reported fraudulent operations for all instruments increased by slightly over 1.8 million from 2023 to 2024 (a year-on-year increase of 10%) reaching 19.6 million transactions (see Chart 1b). Card payment fraud accounted for the largest number of fraudulent transactions across all reporting periods. The high number of fraudulent transactions in card payments may indicate fraudsters take advantage of low value transactions where strong customer authentication (SCA) may not be applied, leveraging on SCA exemptions. In 2024, around 17.06 million fraudulent card transactions were executed out of around 111.05 billion transactions initiated with cards issued in the EU/EEA. The annual fraud rate for card volumes accounted for 0.015% of the total number of card payments in 2024, practically the same as 2023. Overall, while still being the highest when compared to other instruments, fraud rates for card payments remained fairly stable and low in terms of volumes across all reporting periods analysed.

Box 1: Evolution of SEPA instant credit transfers

This box displays some recent developments in the use of instant payments in the EU[1], including some initial data on related fraud.

Instant payments are increasingly used by the public: the relative share of SEPA instant credit transfer (SCT Inst) volumes in comparison to SEPA credit transfers (SCT) has gradually grown over the past three years, from slightly below 10% to close to 16%. SCT Inst values in comparison to SCT are still at a low level, having increased from slightly above 2% to 4% and their growth rate also being slightly below volume growth (the higher average value of credit transfers also reflects the usage by corporate customers, while instant credit transfers were primarily used by retail customers over the reference periods).

Chart 1 - Volume and value of SCT instant in % of SCT transactions

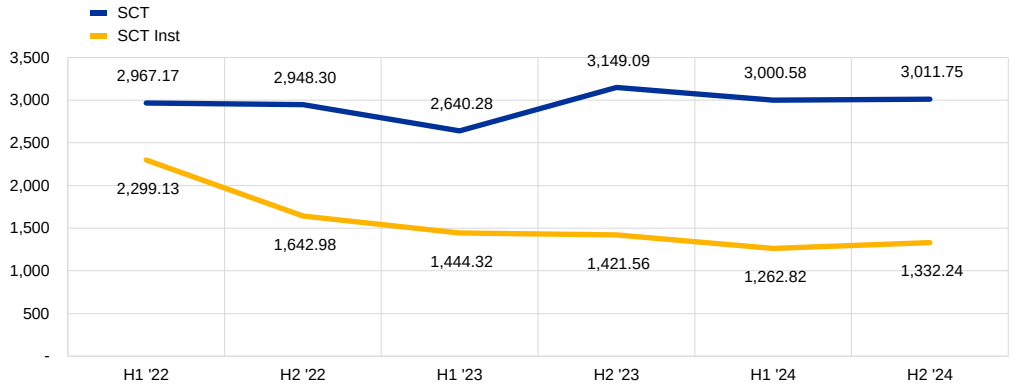


The average fraud amount for SCT traditional transactions[2] has slightly increased over the last three years, as a consequence of fraud values increasing by 33%, marginally more than corresponding fraud volumes over the same period (31%). The higher average fraud amounts per transaction may be connected to the increase in authorised push payment scams (APP scams) which cause high damages per fraudulent transaction. SCT Inst transaction values grew by 74%, outpacing the 59% growth in related fraud values, contributing to a reduction in fraud rates as well as a slight decrease in the loss value per fraudulent transaction. However, transaction volumes increased by 98%, while fraud volumes grew by 175%.

[1] The data used corresponds to EU without Bulgaria, Croatia, Czech Republic, Denmark, Hungary, Poland, Romania, Sweden, as for these countries data was not available over the entire period.

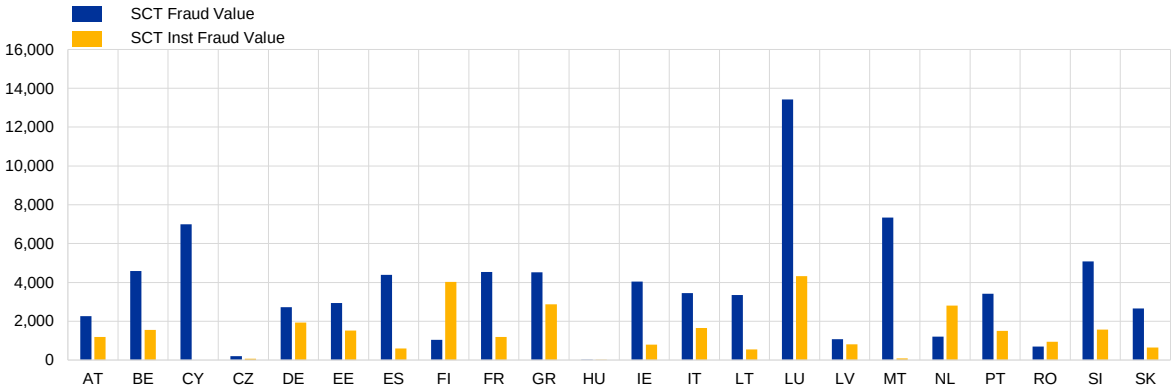
[2] This analysis distinguishes between traditional SCT transaction and SCT Instant Transactions. Together they would add up all SCT transactions.

Chart 2: Average value per fraudulent transaction
(average value (EUR))



On a country-by-country level, a high dispersion of average loss amounts per transaction can be observed. Besides the higher loss per transaction in traditional SCT transactions also a higher dispersion in average losses can be observed (from EUR 10 to EUR 13,430 with an average loss of EUR 3,632) compared to SCT Inst transactions (from EUR 74 to EUR 4,324 with an average loss of EUR 1,392) (See Chart 3). However, when interpreting these figures, it needs to be taken into account, that the use of SCT Inst is progressively expanding, as under Regulation (EU) 2024/886 (commonly referred to as the Instant Payments Regulation (IPR)), most PSPs will need to be able to send instant payments within the euro area as of 9 October 2025 (Payment Institutions and E-Money Institutions however have an extended deadline). The data also only partly reflect the potential use of additional safety measures such as Verification of Payee (VoP), which will become mandatory by the same date and may thus, looking ahead, contribute to containing fraud. Finally, it is important to take into account that the use cases of the SCT Inst instrument across countries can vary significantly due to users adoption preferences and country specific factors, which somewhat further limits the direct comparability of fraud data.

Chart 3: Average value of fraudulent SCT Inst by country[3,4]
(average value (EUR))



[3] Non-euro-area countries, average exchange rate between of 1 July and 31 December 2024
N/A data for SCT Inst displayed as zero
[4] At present, the value and respective fraud rate for SCT Inst and SCT in IT are under revision due to incorrect data submissions received from reporting entities. They will be corrected retrospectively when data will be reported for forthcoming reporting periods.

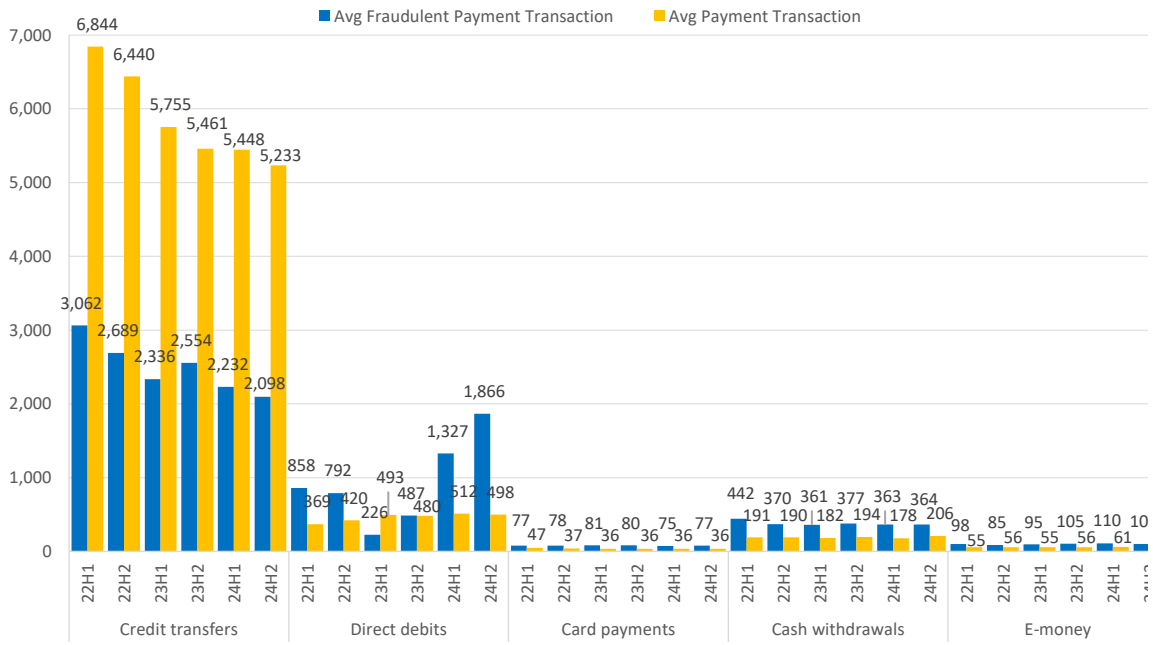
Direct debit transactions in 2024 displayed a larger share of all fraudulent transactions in terms of value (3%) than in terms of volume (0.4%), which could be explained by fraudsters successfully targeting high value transactions (see Chart 1b). Overall, 73,935 direct debit transactions were reported as fraudulent in 2024, which represents a year-on-year volume decrease of around 38% from 2023. The annual fraud rate of direct debit payments in 2024 confirmed the trend observed in the previous reporting years by being the lowest across all instruments at 0.0004%.

While the total amount of e-money fraudulent transactions in volume terms was the third lowest of all payment instruments, the annual e-money fraud rate, although continuing its decreasing trend, was still at a similar level as card payments and direct debits. The number of fraudulent e-money transactions amounted to around 969,000 transactions in 2024, which represents a relevant year-on-year decrease of 15% from 2023. The annual fraud rate in volume terms was around 0.011%, continuing the downward trend observed since 2022 where the fraud rate was around 0.013%.

Both in absolute and relative terms, the reported volumes of fraudulent credit transfers and cash withdrawals remained among the lowest of the five instruments included in the analysis. One possible explanation may be related to the limited opportunities for fraudsters to exploit situations where PSPs do not apply SCA. This means that large-scale, indiscriminate attacks are less effective, and fraud attempts tend to require a more tailored approach focussing on individual victims. As such, the numbers tend to be lower when compared with card payments, which are usually affected in the opposite way, by low value high frequency fraud. The total number of fraudulent credit transfers sent from PSPs in the EU/EEA in 2024 only amounted to around 1,166,000 transactions, with a fraud rate of 0.002%, the same rate as in 2023. From the total number of 7.07 billion cash withdrawals performed during 2024, only around 373,000 were fraudulent, which resulted in a fraud rate of 0.005% (remaining stable across all reference periods).

The average value of a fraudulent credit transfer in 2024 was still significantly higher compared to the majority of other payment instruments, followed by direct debits (as per Chart 2). The average value for a fraudulent credit transfer amounted to EUR 2,155 (a 12% decrease since 2023) which was lower than the average value of a credit transfer (EUR 5,370 in 2024). Direct debits and cash withdrawals show the following higher average values in a fraudulent transaction with an average of EUR 1,516 and EUR 363, respectively, in 2024. Unlike other payment instruments, the average value of fraudulent direct debits and cash withdrawals were significantly higher than the overall average transaction values (EUR 504 and EUR 191, respectively, in 2024). Both average values are significantly higher compared to the remaining instruments (e-money, and card payments amounted to EUR 105, and EUR 76, respectively). These differences may reflect both the nature of the instruments and potential fraud strategies. For instance, lower-value fraud in card and e-money transactions could be linked to attempts to avoid detection or SCA requirements.

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



3. Main fraud types

This chapter provides an analysis of the data based on the type of fraud and the initiation channel used. Section 3.1 focuses on electronically initiated credit transfers, card payments and e-money transactions and corresponding fraud, with additional distinction between non-remotely initiated transactions and remote transactions. Section 3.2 assesses the main fraud types under PSD2 observed for each kind of payment.

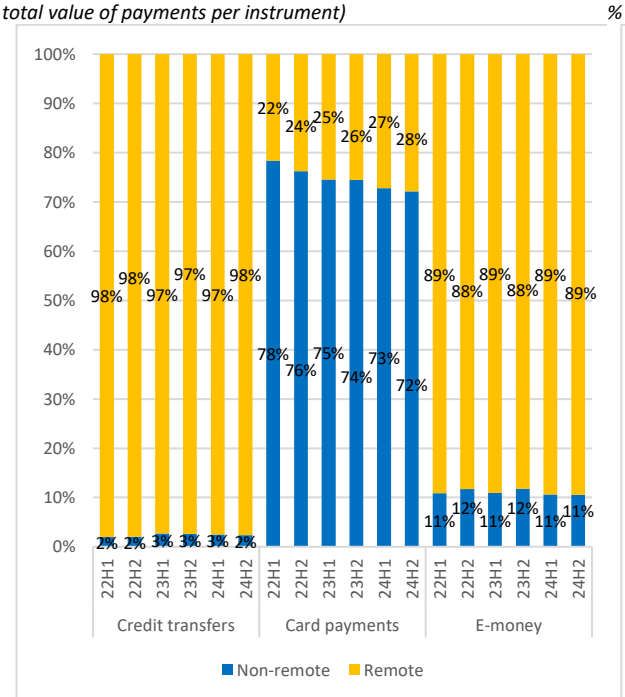
3.1 Remote versus non-remote transactions and fraud

The majority of electronically initiated credit transfers are initiated remotely, both with respect to overall transactions and fraudulent transactions. In the six periods analysed, around 98% of the total value of electronically initiated credit transfers and more than 99% of the value of corresponding fraudulent credit transfer 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 is 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)

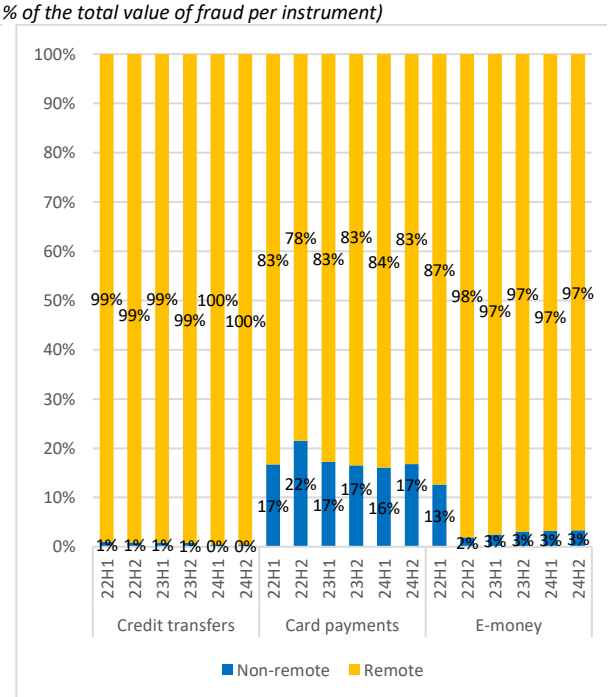
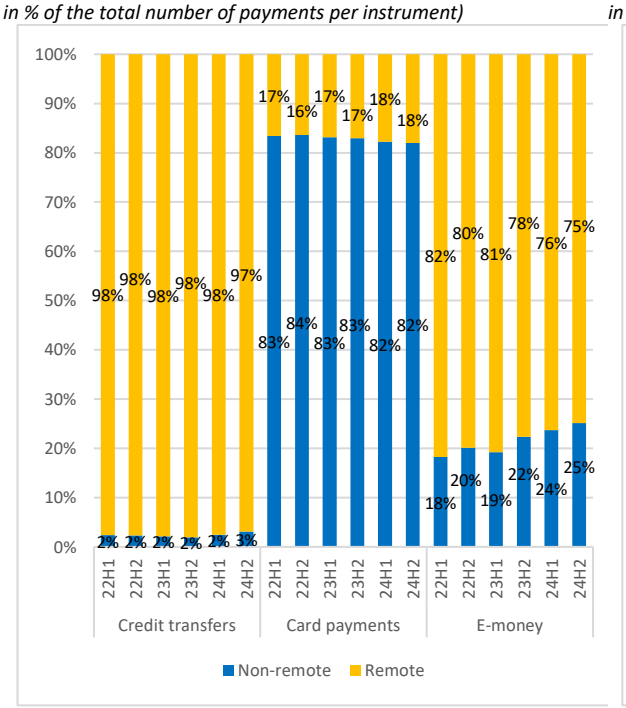


Chart 4: Volume shares of non-remotely versus remotely initiated payment transactions and fraud

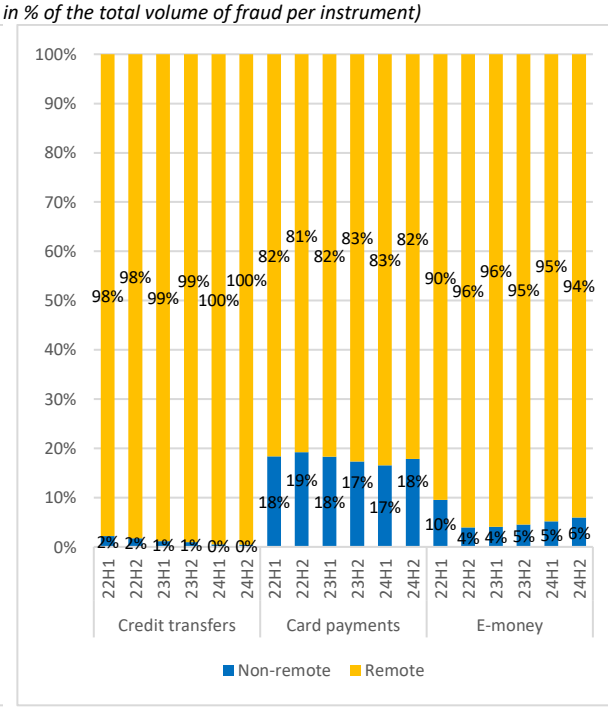
a) Volume of payment transactions by instrument

(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)



Credit transfers were mainly initiated remotely by users. When analysing fraudulent transactions (see Charts 3b and 4b), remote initiation is even more prevalent when comparing to the non-fraudulent transactions (see Charts 3a and 4a). However, in terms of fraud rates, figures are so low that differences between remote and non-remote transactions are not significant (in 2024, annual fraud rates for credit transfers initiated remotely were 0.001% and 0.003%, in value and volume terms, respectively, while the ones initiated non-remotely were even lower than that).

For e-money payments, most reported transactions, including fraudulent transactions, were remotely initiated. Since 2022, overall e-money transactions initiated remotely have been around 90% and 80%, in value and volume terms, respectively. In terms of fraud, the data shows a very similar pattern in the last 2 years (2023-2024): around 97% of all e-money fraudulent transactions in terms of value were initiated remotely (around 95% in volume terms). Also, e-money transactions showed higher annual fraud rates in the last year for remote (0.020% in values; 0.014% in volumes) compared to non-remote payments (0.006% in values; 0.003% in volumes).

In contrast, while most card payment transactions were initiated non-remotely, card fraud was mainly reported in remotely initiated payments. Remote card payment fraud in value and volume terms accounted for around 83% of all card fraud in 2024, while remotely initiated payments' share of the total value and volume of overall card transactions were only around 28% and 18%, respectively. These shares seem to indicate that while most card-based payments continue to be physical at the point of sale, card payments initiated remotely are the preferred option to steal/misuse funds possibly via stolen credentials.

In line with the above, the annual fraud rate in 2024 was 13 times higher in value, and 22 times higher, in volume, for remote (0.091% in values; 0.068% in volumes) when compared to non-remote card payments (0.007% in values; 0.003% in volumes).

The evident preference of fraudsters for remote transactions as initiation method, which is shown across all instruments, including in instruments that are primarily used in a non-remote environment, supports the legislators' focus on enhancing the security for such payments. In this respect, the introduction of dynamic linking as an additional requirement for SCA in the PSD2, ensures that the authentication code generated by a strong customer authentication is specific to the amount and to the payee specified by the payer when initiating a remote transaction.

3.2 Fraud types by channel

In the vast majority of fraudulent card payment transactions, cash withdrawals and e-money transactions, the payment order was issued by the fraudster (see Chart 5). In the six reference periods analysed, more than 90% of the total value was related to this type of fraud with the exception of 2024 for e-money, where the issuance of payment orders by the fraudster fell below this threshold. In volume terms, this same fraud type averages around 97% of card, e-money and cash withdrawals fraud (see Chart 6).

By contrast, the largest share of fraudulent credit transfer, both in value and volume terms, was due to the manipulation of the payer to initiate a transaction. This type of fraudulent payment transactions followed an increasing trend, from 65% to 74% in value terms and 55% to 71% in volume terms, from 2023 to 2024, respectively. (see Charts 5 and 6).

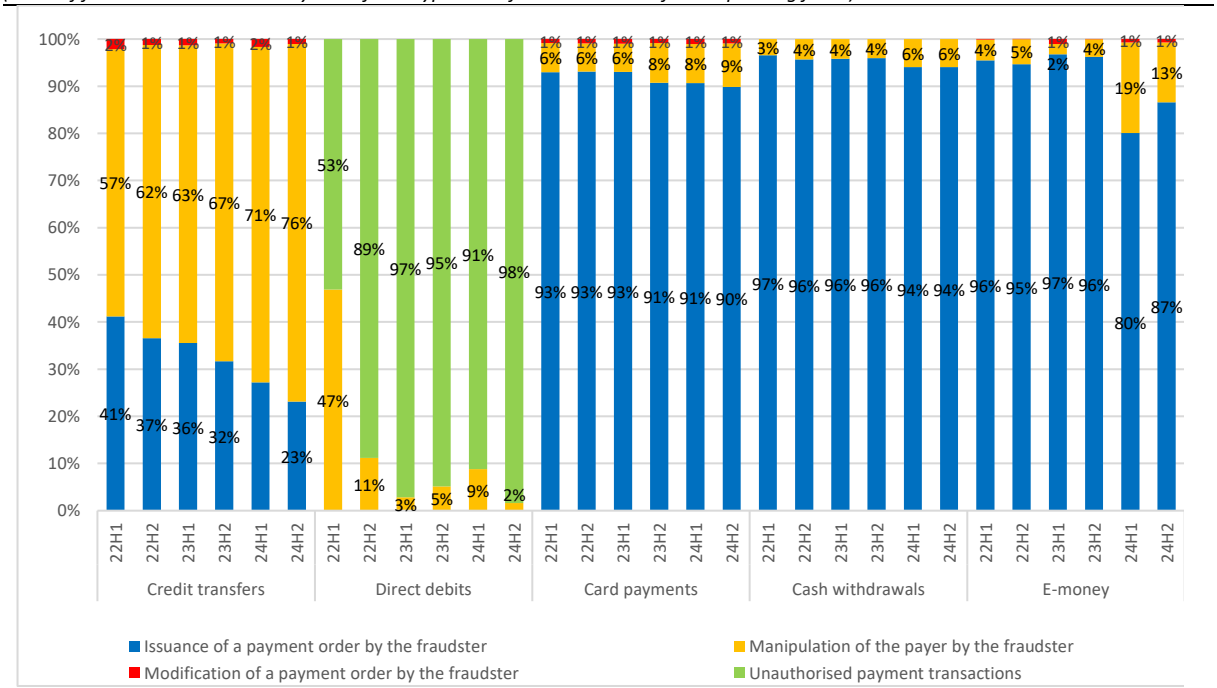
This clearly shows a significant growth of fraud based on the manipulation of the payer into initiating a transaction that goes against their own self-interest, appearing therefore to be the preferred fraud type by fraudsters for credit transfers. This fraud type includes impersonation fraud and other frauds supported by phishing/smishing/vishing techniques that aim, not only at preparing more technical attacks, but also at persuading the payer to initiate a transaction for the benefit of the fraudster. In this context, social networks play an important role, often used as both a vector to interact with potential victims to build up, extract information and groom the victim through tailor-made attacks on specific individuals.

For e-money transactions, the increase of the share of manipulation of the payer fraud in 2024 was, possibly, due to the increase in the overall value of e-money transactions, which might made e-money more attractive for fraudsters resulting in more targeted attacks on this payment method.

Finally, most cases of direct debit fraud in value terms were accounted for unauthorised[10] payment transactions, with the exception of the first semester of 2022 where the manipulation of the payer by the fraudster to consent to a direct debit accounted for almost half of the cases. A greater volatility could be observed in volume terms (i.e. 25%, 67% and 45% of the total volume of direct debit fraud in H1 2022, H2 2023 and H1 2024, respectively, were related to manipulation of the payer). This volatility is partly due to the relatively low number of fraud cases (approximately 74,000 in 2024), which makes the data more susceptible to the influence of outliers.

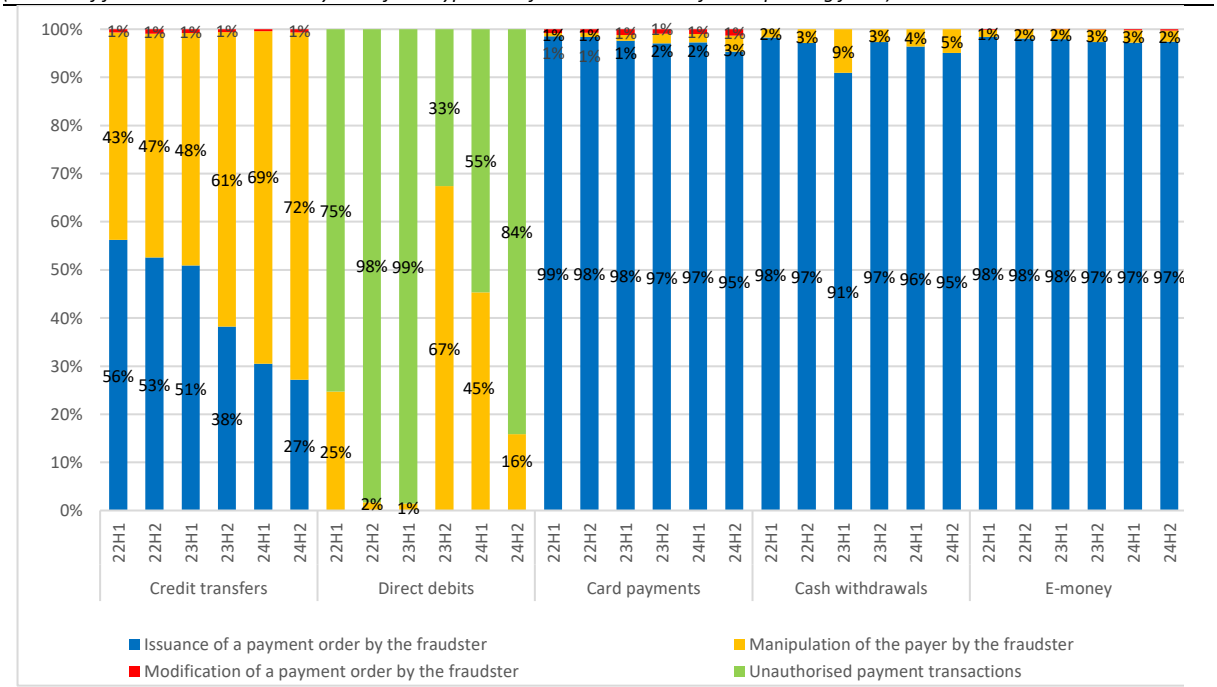
Chart 5: Composition of the value of fraud by main types of fraud

(value of fraudulent transactions by main fraud type in % of the total value of corresponding fraud)



[10] As in the previous year, 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.

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)



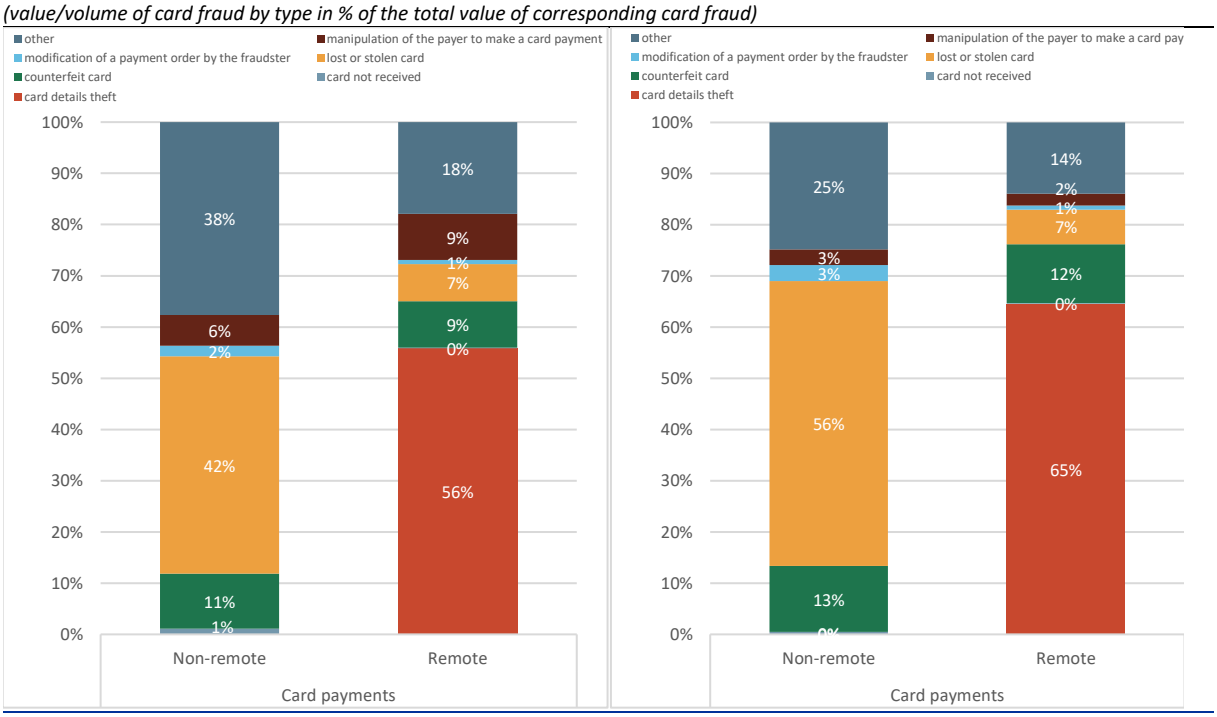
In addition to the previous and more high-level analysis, card payment fraud data (see Chart 7) contains additional breakdowns in terms of the fraud types under the umbrella category of issuance of a payment order by the fraudster, with the largest share of remote card fraud being due to card details theft. In 2024, the theft of card details in remotely initiated fraudulent card transactions accounted for more than 56% of the total value (around 65% in volume terms). Counterfeit card fraud accounted for 9% of remote card fraud in value and 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 14% 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 around 9% in value and 2% in volume terms. This may be related to fraudsters trying to exploit instances where SCA was not necessarily applied, e.g. purchases outside the EEA, and testing large volumes of card numbers trying to bypass the need to engage or deceive users directly, as the attack targets the infrastructure rather than individuals.

Conversely, lost or stolen cards is the most relevant type of fraud in non-remote card payment fraud. In 2024, lost or stolen cards accounted for 42% of the value of non-remote card fraud and for 56% of the fraudulent volume of these payments. Additionally, a large share of non-remote card fraud (38% in value terms and 25% in volume terms) was attributed to the category “other issuance of payment orders by fraudsters”. Also, similarly to remote card payments, data in fraud using counterfeit cards shows a lower percentage in this kind of payments, accounting for 11% of the value of non-remote card fraud and 13% in volume terms.

In non-remote card payment fraud, fraudsters using lost or stolen cards is still the preferred type of fraud. However, the category “other” maintains a relevant share throughout all periods. Based on that, there could be merit in trying to understand the types of fraud being reported under this category or to clarify if this category is chosen in cases of doubts regarding the categorisation.

Chart 7: Composition of the value (left) and volume (right) of card fraud by initiation channel and fraud type (2024)

(value/volume of card fraud by type in % of the total value of corresponding card fraud)



4. The impact of strong customer authentication (SCA)

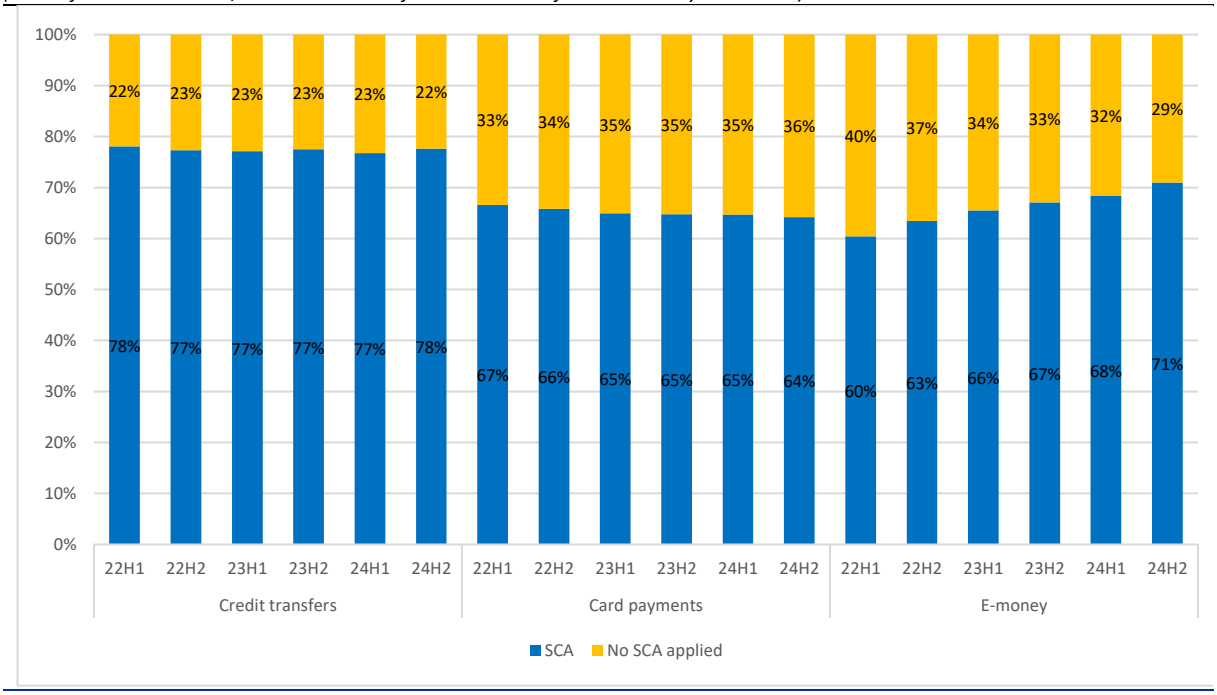
The application of strong customer authentication (SCA), as defined in Delegated Regulation 2018/389 on Regulatory Technical Standards (RTS) for SCA and secure communication (RTS on SCA and common and secure communication (CSC)), has proven to be one of the most effective tools in reducing fraud. Designed to balance security and customer convenience, the RTS outline specific exemptions where payment service providers (PSPs) may choose not to apply SCA, based on factors such as risk level, transaction amount, frequency, and payment channel. In such cases, PSPs assume liability for any unauthorised transactions. This chapter provides:

- an overview of SCA usage for electronic payments (section 4.1),
- a comparison of fraud rates for transactions with and without SCA (section 4.2), and
- a detailed look at the exemptions defined under the RTS (section 4.3).

4.1 Use of SCA for electronically initiated payments

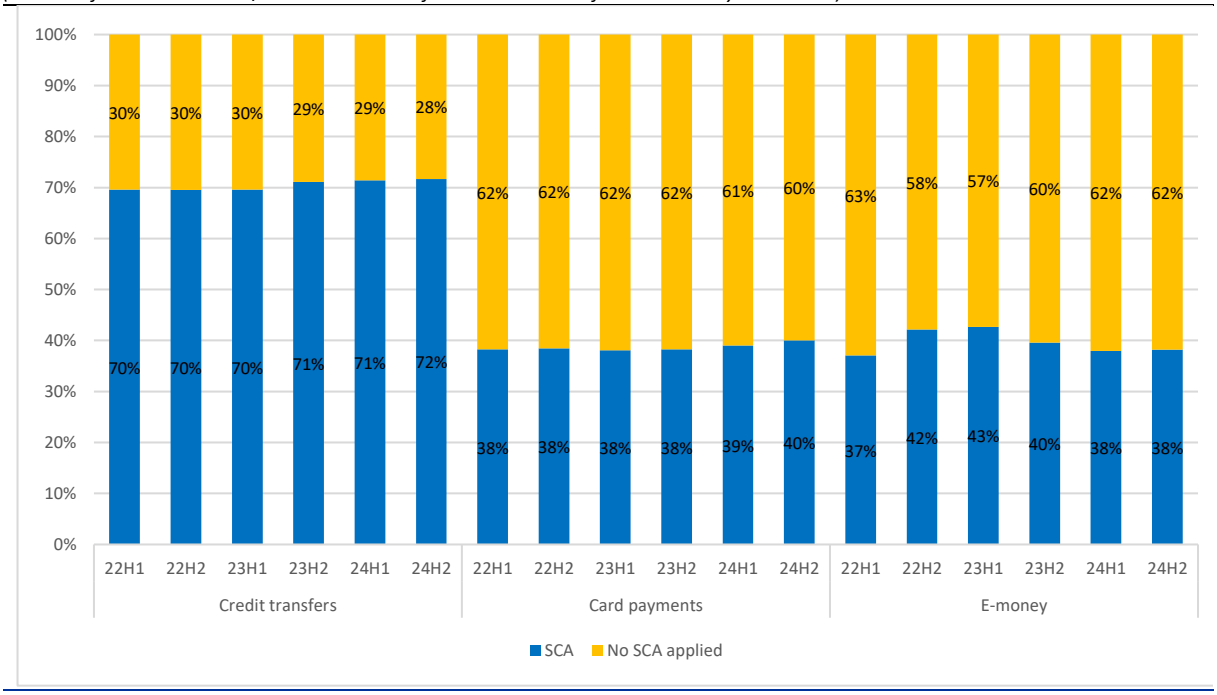
SCA was applied to the majority of electronic payments included in the scope of this report in value terms, with percentages ranging between 77-78% for all six reporting periods. While several exemptions to the use of SCA were provided in the RTS on SCA and CSC with an aim of supporting seamless and innovative means of payment while taking into account the need to ensure the safety of customers' funds and personal data, payment transactions being executed via SCA have become the standard. In 2024, transactions authenticated via SCA accounted for 77% of all electronically initiated credit transfers in value terms (see Chart 8). For electronically initiated card payments using cards issued in the EU/EEA, the percentage is slightly lower, with around 64% of the total value authenticated via SCA. The share of e-money transactions authenticated via SCA was still increasing and amounted for around 70% in 2024, which represents an 8 p.p. increase since 2022.

Chart 8: Share of SCA vs 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)



In terms of volume, while most electronically initiated credit transfers were authenticated with SCA and remained stable at around 71% across all periods, the share of card payments and e-money transactions without SCA was significantly higher (see Chart 9). In 2024, electronically initiated card payments and e-money transactions were only SCA authenticated in 40% and 38% of the transactions, respectively. For card payments, this lower percentage can mostly be explained by the use of these instruments at the point of sale where exemptions like the ones foreseen for contactless payments and transport fares, inter alia, are more prevalent and have become the standard for paying at the point of sale.

Chart 9: Share of SCA vs 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 and geographical location

Fraud rates for transactions within the EEA, where it is mandatory to apply either SCA or one of the exemptions provided in the RTS on SCA and CSC, remained lower compared with transactions where the counterpart PSP was outside the EEA, where SCA may not be mandatory (see Chart 10 and 11). This was observed for credit transfers, card payments and e-money transactions 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 seems to indicate that the overall fraud mitigation requirements, notably SCA for all electronically initiated transactions and EMV in particular for non-remote transactions, have limited the opportunities to use counterfeit instruments and thus keep having the desired beneficial impact on fraud levels within the EEA.

The fraud rates for card payment transactions authenticated with SCA were consistently and substantially below fraud rates for card transactions without SCA. This pattern was especially evident for transactions involving cards issued in the EU/EEA and acquired outside of the EEA, where SCA may not be mandated by law; this pattern was also observed with regard to card payments acquired within the EEA (see Charts 10 and 11). In 2024, fraud rates for card transactions without SCA within the EEA were twice as high in both value and volume terms than transactions with SCA within EEA, while for transactions outside the EEA they were three times higher in value and four times higher in volume terms.

Fraud rates for credit transfers were generally low, irrespective of the application of SCA or the geographical location of the receiving PSP, both in terms of value and volume. Interestingly, the data shows higher fraud rates for SCA authenticated credit transfers compared to those exempted from SCA. This does not imply that SCA is less effective; rather, it reflects the nature of the transactions involved. SCA is typically applied to higher-value or higher-risk transactions, which are more attractive targets for fraudsters. Besides, many types of exempted transactions, such as "payments to self" or those using secure corporate protocols, are less likely to be targeted by fraud, resulting in lower observed fraud rates. Therefore, the higher fraud rates for SCA-authenticated transactions are likely due to fraudsters focusing their efforts on transactions where SCA is applied, rather than attempting to circumvent SCA requirements.

From 2023, fraud rates for e-money payments within the EEA were lower for transactions authenticated via SCA in value terms. In terms of volumes, transactions without SCA constantly had higher fraud rates from 2022 to 2024. Outside the EEA, the fraud rate for transactions with SCA were lower in 2024 in terms of transaction values and volumes.

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

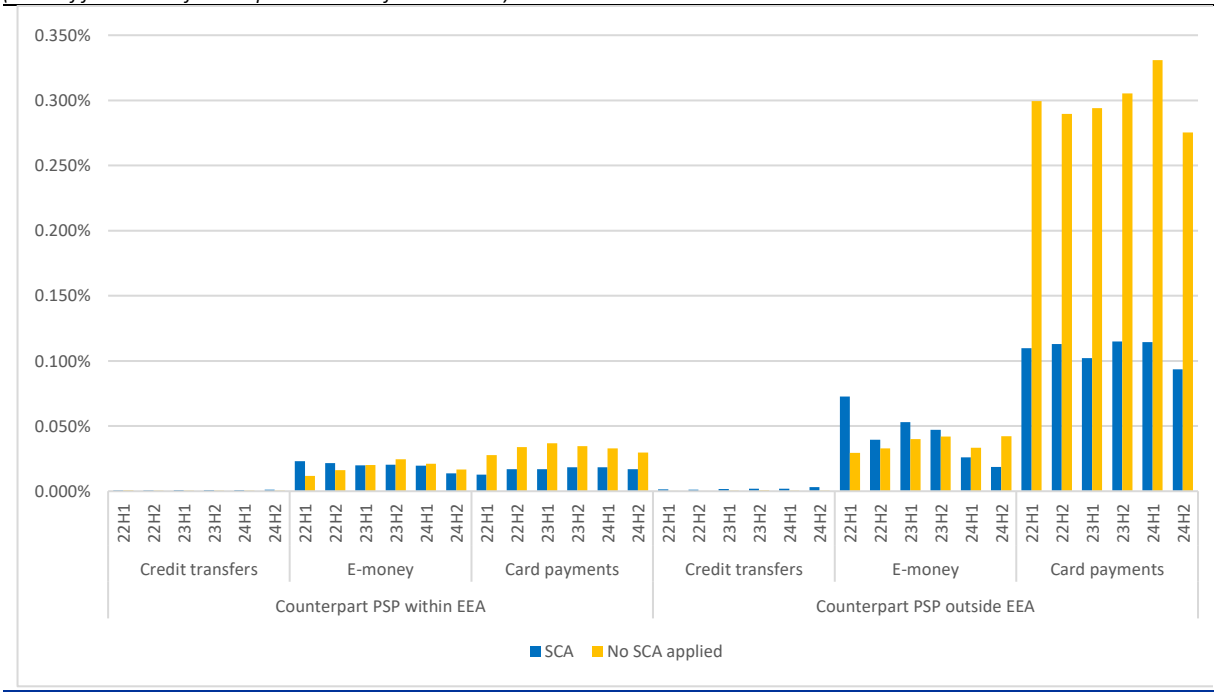
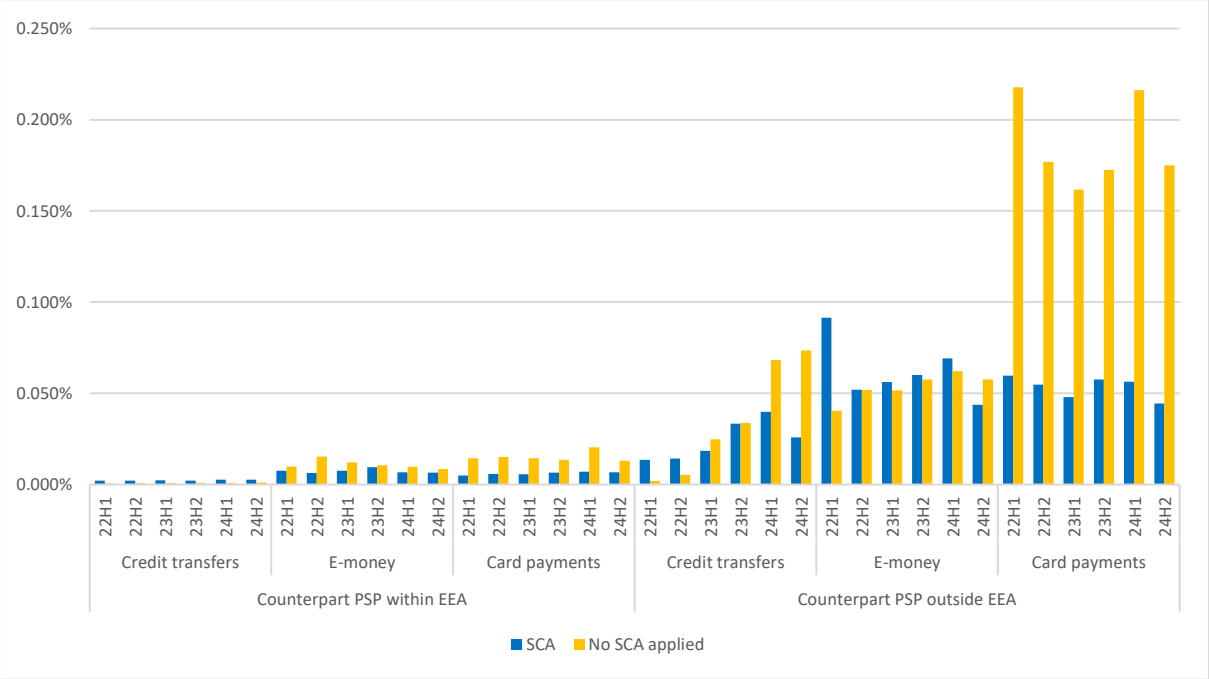


Chart 11: Fraud rates for SCA vs non-SCA-authenticated transactions by payment instrument and geography (in volumes)
(volume of fraud in % of the respective value of transactions)



4.3 Transactions not authenticated via SCA

Generally, non-SCA authenticated transactions exhibit higher fraud rates compared to SCA-authenticated ones. Charts 12, 14, and 15 present the breakdown of non-SCA transactions by exemption type or reason for not applying SCA, segmented by payment instrument—credit transfers, card payments and e-money—and by channel (remote vs. non-remote). Charts 13, 16, and 17 display the corresponding fraud rates for each exemption or rationale.

In accordance with the PSD2 mandate, the RTSs on SCA and CSC define specific exemptions to SCA. These exemptions aim to balance enhanced payment security with usability and accessibility, and are based on factors such as transaction risk, amount, recurrence and channel.

Key exemptions include:

- Articles 11 and 16: Contactless payments at point of sale and low-value transactions, respectively, based on thresholds for transaction count or cumulative value.
- Article 12: Unattended terminals (e.g., toll gates), where SCA may be impractical due to operational constraints.
- Articles 13 and 14: Trusted beneficiaries and recurring transactions, both involving repeated payments previously authorised via SCA.
- Article 15: Credit transfers between accounts held by the same individual or entity within the same payment service provider (PSP).

- Article 17: Transactions by non-consumers using secure corporate payment protocols that offer equivalent security to SCA.

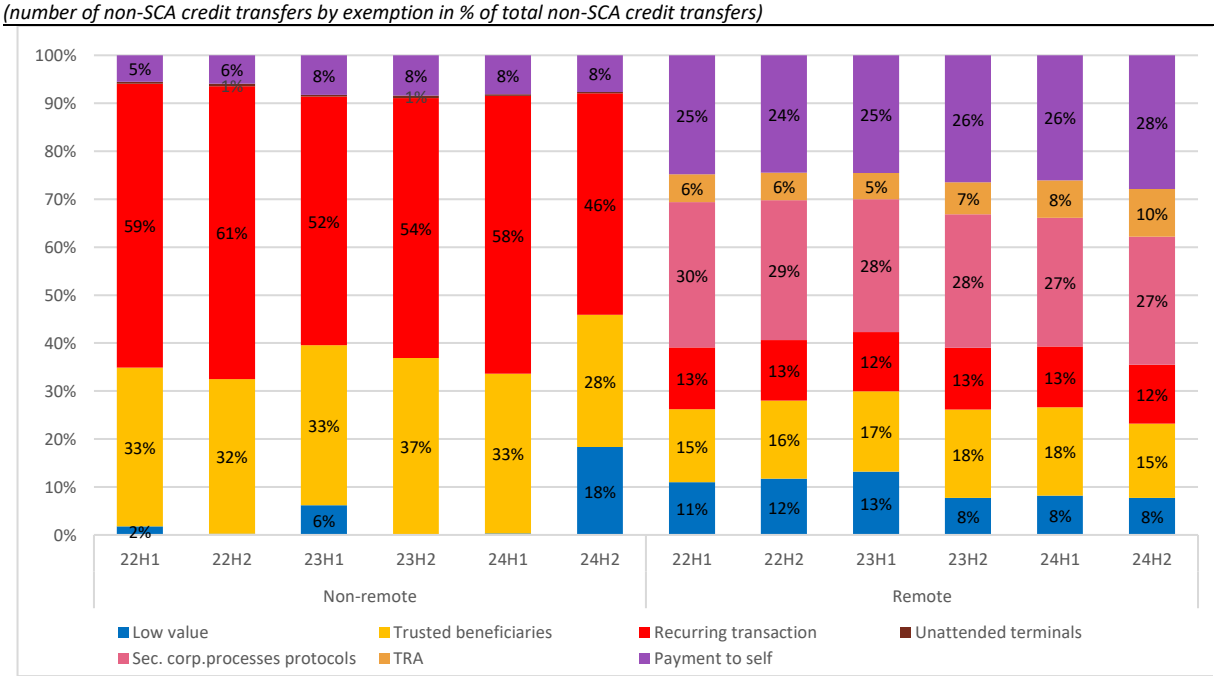
- Article 18: Remote transactions deemed low-risk following a transaction risk analysis (TRA).

Some payment transactions are not in the scope of SCA. This is for example the case for merchant-initiated transactions[11] that are not initiated by the payer but by the payee only (referred as MIT in the charts) or "other" in the chart (e.g. one leg-out transactions).

For remote credit transfers, the most frequently used exemption by PSPs was for secure corporate processes and protocols under Article 17 of the RTS on SCA and CSC. This was closely followed by transfers between accounts owned by the same user ("payment to self") under Article 15 (as per Chart 12). These two exemptions, along with trusted beneficiaries, consistently accounted for approximately 70% of all exemptions applied to remote transactions, a pattern that remained stable over time. In contrast, the Transaction Risk Analysis (TRA) exemption, which allows PSPs with low fraud rates to bypass SCA for remote payments up to €500, was rarely used, although increasing over time. This limited use may reflect a cautious approach by PSPs, prioritising security over customer convenience.

With non-remote credit transfers, the distribution of exemption shifts. Exemptions, such as recurring transactions and trusted beneficiaries, are more prominent. In particular during the second semester of 2024, the share of low-value exemption grew substantially, possibly due to point-of-sale solutions based on credit transfers becoming more widely used across Europe (contactless physical purchases using NFC or QR codes.).

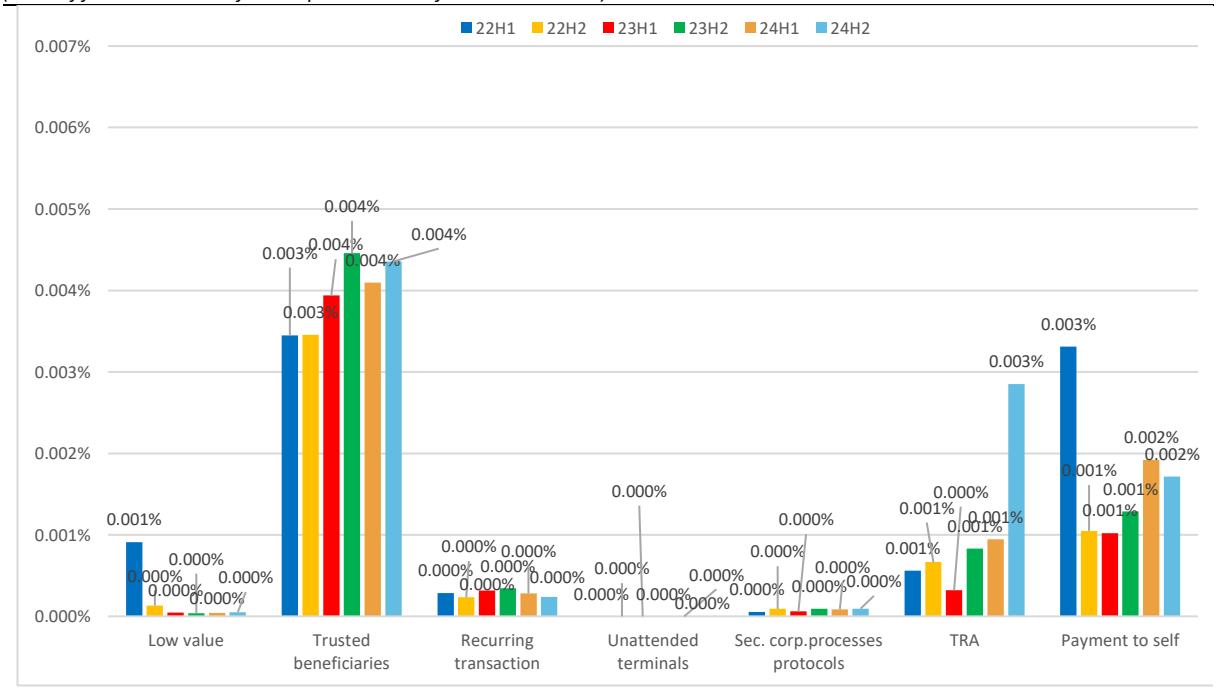
Chart 12: Composition of the volume of electronic credit transfers without SCA by exemption type
(number of non-SCA credit transfers by exemption in % of total non-SCA credit transfers)



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.

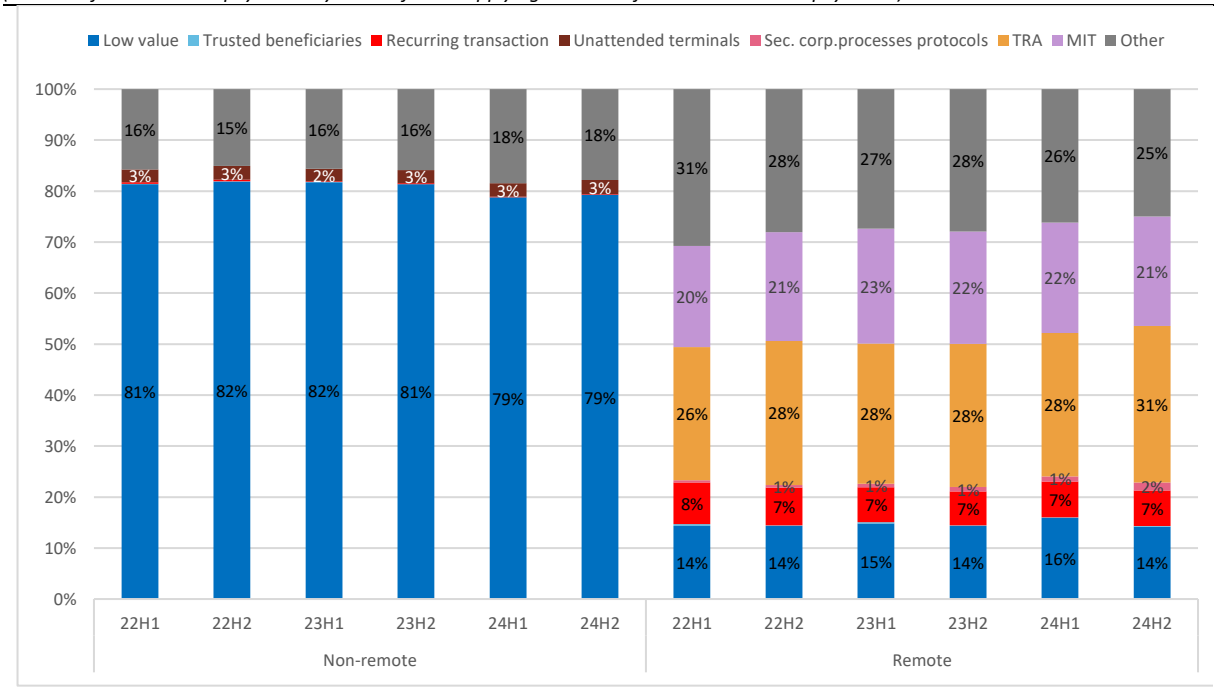
[11] MIT refers to card-based payment and e-money transactions that meet the conditions specified by the Commission in Q&A 2018_4131 and Q&A 2018_4031 and which are, as a result, considered as payee-initiated and not subject to the requirement in Article 97 of PSD2 to apply SCA.

Chart 13: Fraud rates of credit transfers without SCA by reason for not applying SCA (in value)
(value of fraud as a share of the respective value of total transactions)



Fraud rates for SCA-exempted credit transfers, while overall low, were higher, in value terms, for trusted beneficiaries, which is an exemption that involves the application of SCA to add a payee to a list prior to the execution of a credit transfer, and payments between accounts owned by the same user held in the same PSP. The most often applied exemption, regarding secure corporate processes and protocols (Art. 17) resulted in low fraud rates, around 0.0001%. While the annual credit transfer fraud rate is low (0.001%), the exemptions for trusted beneficiaries and, at times, the exemptions for payments between accounts owned by the same user and TRA, had a higher fraud rate than for all credit transfers.

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 reason for not applying SCA in % of total non-SCA card payments)



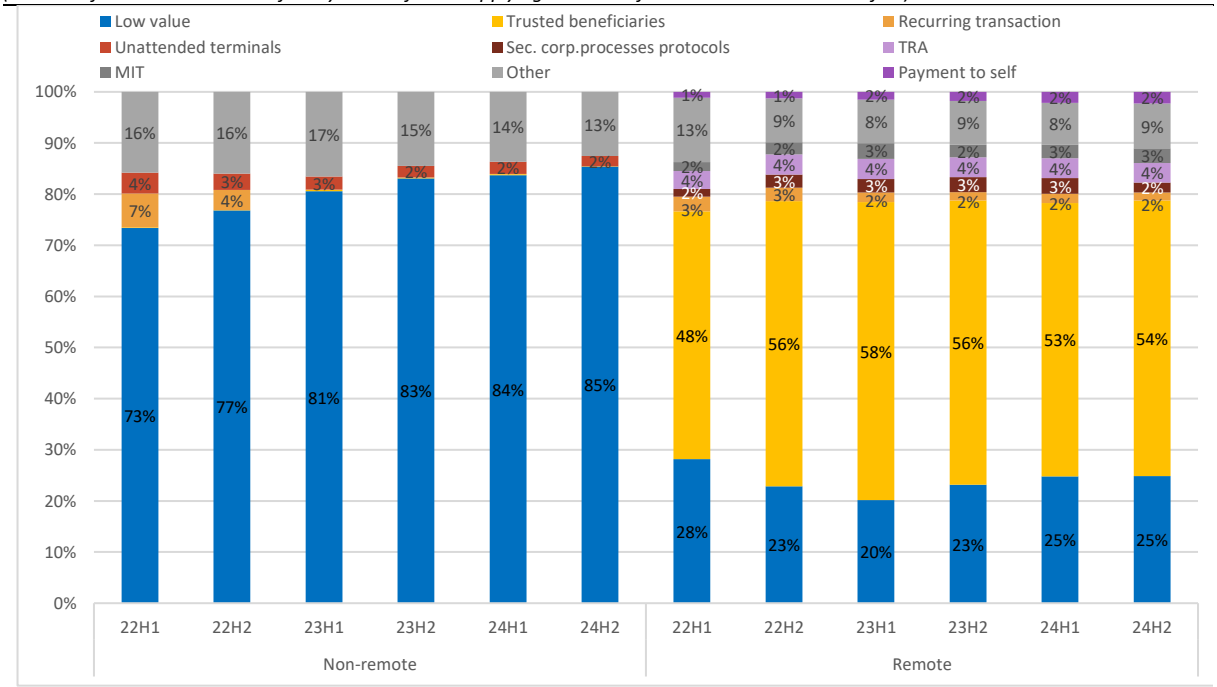
Note: the category of 'low value' exemption shown in this graph refers to exemptions under Art. 11 of the RTS on SCA and CSC on contactless payments for non-remote transactions and to exemptions under Art. 16 for remote transactions.

Contactless payments have become the standard initiation method used at the physical point of sale, representing the majority of non-remote card payments and e-money transactions where SCA was not applied. This exemption, which is often based on NFC technology or the reading of QR-codes, accounted for around 79% of the total volume of non-SCA card payments in 2024, and for 85% of non-SCA e-money transactions that were initiated non-remotely in 2024 (see Charts 14 and 15).

For remote card payments, the most often applied exemption to transactions in scope of SCA was the TRA, which entails that such transactions were evaluated and considered to be low risk in regard to the behavioural pattern of the payer (e.g. known fraud scenarios or abnormal location of the payer). In 2024, around 29% of remote card payments without SCA were exempted under TRA. The next most prevalent reason for not applying SCA to remote card transactions relates to merchant-initiated transactions (MIT), which entail the existence of a previously existing mandate that requires the application of SCA when the mandate is granted, which amounted to 22% in 2024. In 2024, 26% of remote transactions were reported as being outside the scope of SCA requirements under PSD2. This figure remains high despite the clarifications provided in the EBA Q&As[12], which clarified that card-based payment transactions qualify as electronic payment transactions and are initiated by the payer through the payee and thus cannot be considered out of scope of the SCA requirement; this warrants further investigation as to whether SCA requirements under PSD2 have been applied correctly.

[12] For example, mail order and telephone order (MO-TO) transactions are out of scope of SCA requirement and should hence not be reported as exempted from SCA under the category of other reasons for not applying SCA (see EBA Q&As 2019_4788 and 2019_4790).

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 reason for not applying SCA in % of total non-SCA credit transfers)



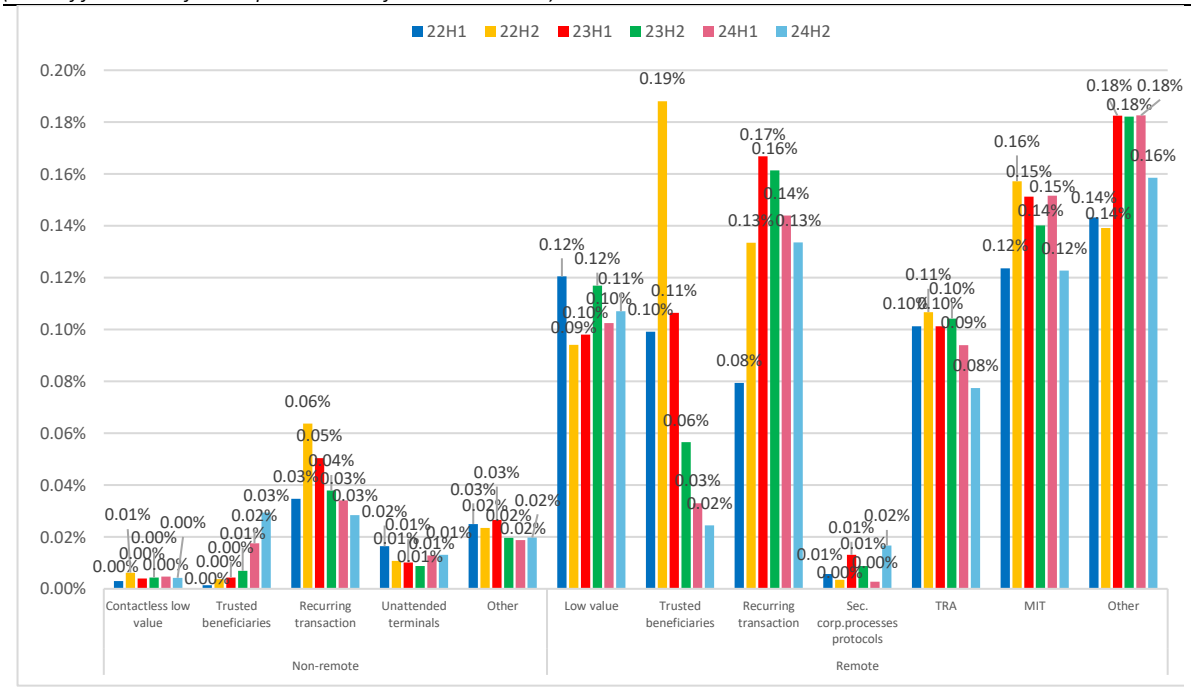
Note: the category of 'low value' exemption shown in this graph refers to exemptions under Art. 11 of the RTS on SCA and CSC on contactless payments for non-remote transactions and to exemptions under Art. 16 for remote transactions.

In 2024, regarding remote e-money transactions, the two most prevalent exemptions, "trusted beneficiaries" and "low value" accounted for around 79% of the transactions where SCA was not applied. These two exemptions were the most relevant for all reported periods and maintained a similar share of the exempted remote e-money transactions. Although to a lesser extent, a significant share of remote e-money transactions was exempted due to "other" reasons, requiring further follow-up investigations.

Fraud rates for SCA-exempted remote card payments were generally above the overall card payment fraud rate (0.033% in 2024) with the exception for secure corporate processes across all periods and for protocols and trusted beneficiaries in 2024. This could suggest that fraudsters adapt their attacks by aiming at transactions that could fall into commonly used exemptions. In general, exemptions are more widely applied to card payments than to other instruments like credit transfers.

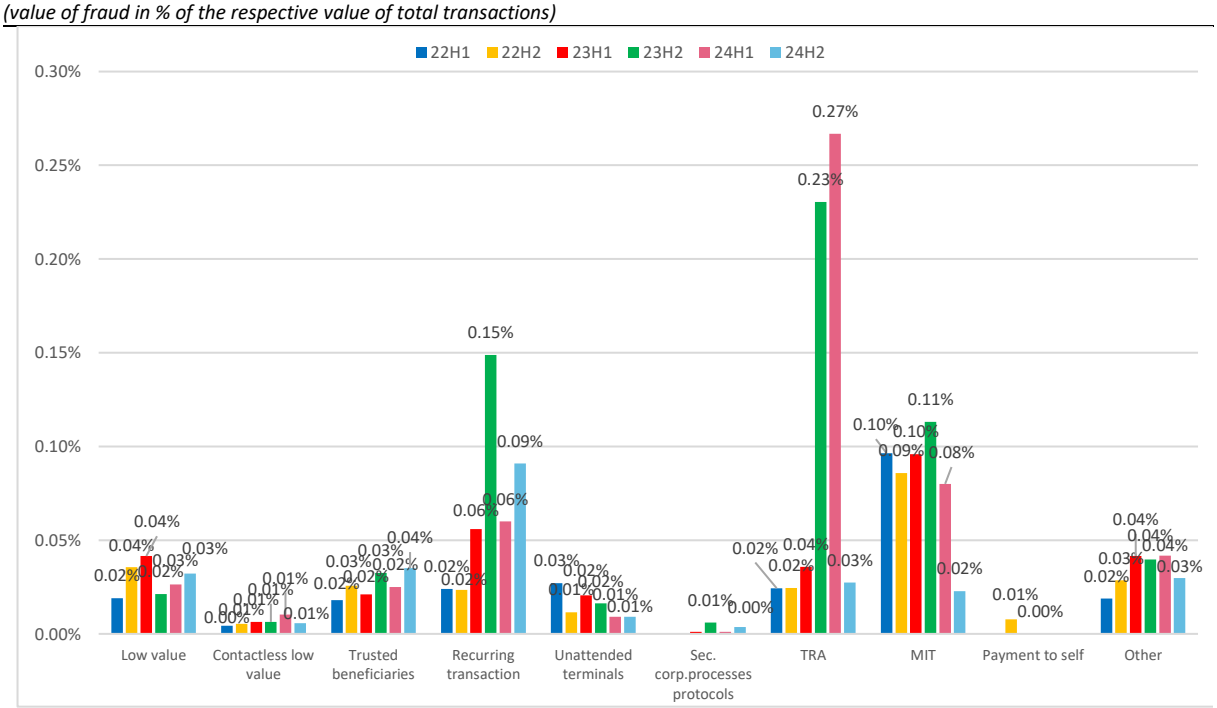
In this context, in 2024, fraud rates for remote card payments without SCA ranged between 0.01% and 0.17% of the corresponding total value of respective card payments, which could be significantly higher than the overall fraud rate for cards, that was of 0.033% in the same period. This applies to both exemptions defined under PSD2 and to transaction outside the scope of the PSD2 SCA requirements (see Chart 16). Contrary to this, fraud rates related to SCA-exempted non-remote card payments were generally lower than remote transactions and often below the overall fraud rate for this instrument.

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)



In 2024, for remote e-money transactions where SCA was not applied, the annual fraud rates for TRA, MIT and recurring transactions (0.142%, 0.049% and 0.074% in 2024, respectively) were considerably higher than the overall fraud rate for e-money transactions (0.018% in 2024). In contrast, transactions exempted based on secure corporate processes and protocols were generally lower (see Chart 17). For the two more often used exemptions in remote and non-remote transactions, trusted beneficiaries and low-value, respectively, the annual fraud rates were 0.023% and 0.014% in 2024, respectively. Fraud rates for e-money transactions without SCA were generally low for non-remote transactions, with the higher fraud rates, although with a decreasing trend, being related to recurring transactions (0.026% in 2024) and for paying transport fares and parking fees in unattended terminals (0.009% in 2024). The most used exemption for contactless payments, observed a low fraud rate, around 0.007% during the six reporting periods.

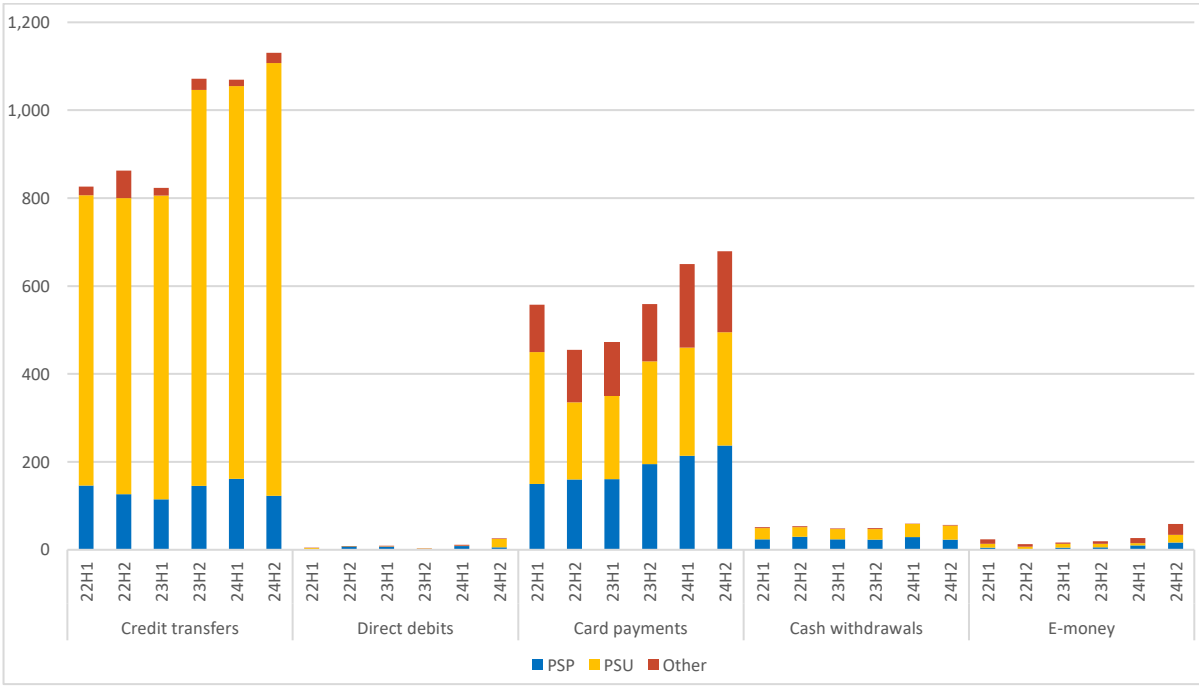
Chart 17: Fraud rates for e-money transactions without SCA by reason for not applying SCA (in value)
(value of fraud in % of the respective value of total transactions)



5. Losses due to fraud

Further information is reported on losses due to fraud. This refers to the losses borne by the reporting PSP, its payment service user (PSU) or others (e.g. the PSP counterpart to the respective transaction), and therefore identifies the party that bears the financial impact of fraud. 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.[13]

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



Across all periods, the highest overall losses due to fraud were reported for credit transfers and card payments, with EUR 2.200 billion and EUR 1.329 billion, respectively, for 2024. PSUs across all instruments were the most affected party and had to bear, in 2024, a total loss of around EUR 2.485 billion, with the reporting PSP and others bearing the remaining EUR 829 million and EUR 454 million, respectively.

For 2024, the overall losses for credit transfers were EUR 2.200 billion (a year-on-year increase of 16%), EUR 1.329 billion for card payments with cards issued in the EU/EEA (a year-on-year increase of 29%) and EUR 239 million for direct debits, cash withdrawals and e-money (a year-on-year increase of 64%) (see Chart 18). Considering that the total value of fraudulent transactions showed a year-on-year

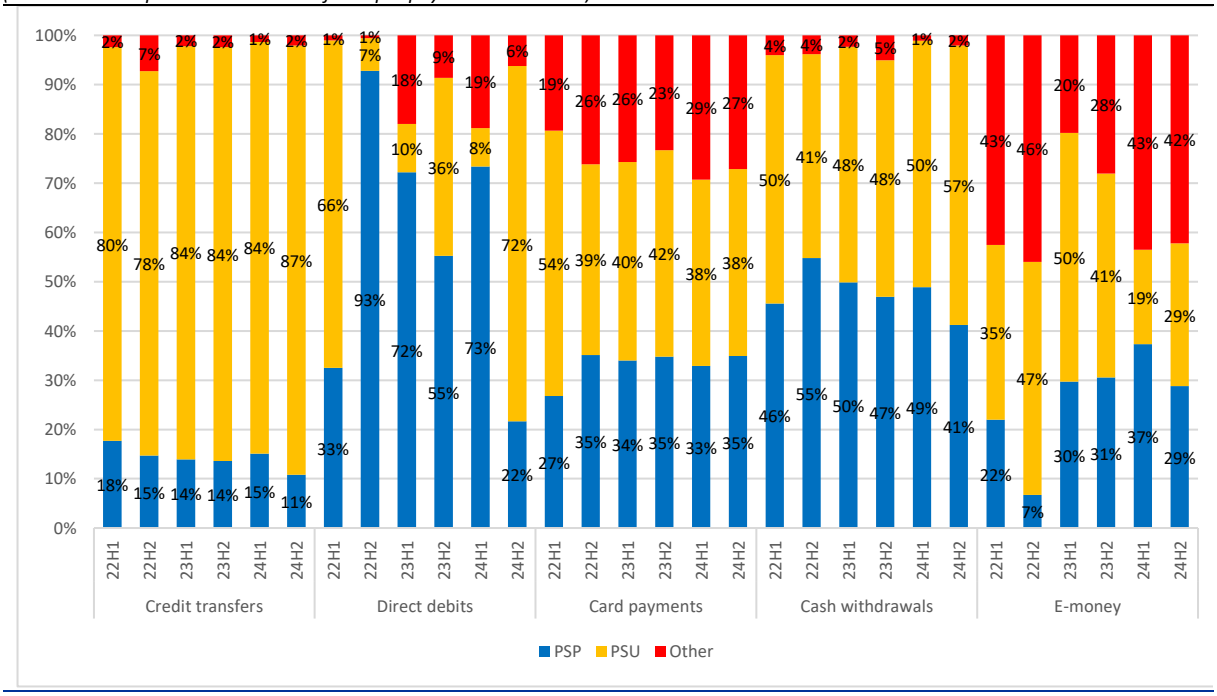
[13] Reported loss figures do not take into account refunds by insurance agencies because they are not related to fraud prevention for the purposes of PSD2.

increase of 17% (see chapter 2), the increase of 23% of financial losses across all instruments seems to indicate that PSPs were less effective in recovering stolen funds compared to the previous year.

Substantial shares of reported financial losses resulting from fraudulent attacks seem to be borne by PSUs, especially in relation to credit transfers, underscores the need for enhanced consumer protection measures and more effective liability frameworks. It also raises questions about the effectiveness of redress mechanisms available to PSUs in cases of fraud and may suggest that national restrictive interpretations of the concepts of 'authorisation' and 'gross negligence' are contributing to PSUs bearing a high share of the losses. In 2024, with the exception of direct debits and e-money (with a share of 19% and 29% for the first and second half of 2024, respectively), the largest share of the reported losses across all of the remaining instruments were borne by PSUs.

More specifically, for credit transfers most losses were borne by PSUs respectively, with around 85% of the annual losses (see Chart 19). This is especially relevant considering credit transfers represent the largest value of funds stolen, at EUR 2.200 billion in 2024. The distribution of the reported losses for card payments and cash withdrawals, in 2024, were more evenly distributed between PSUs and the other two parties, with PSUs bearing around 38% and 53% of the respective losses. Losses resulting from e-money transactions, across all periods, are mainly borne by the reporting PSP and others (between 63% and 93%). In direct debits, the distribution of losses varies significantly between observation periods, with some periods where PSUs (i.e., the payee in this instrument) bear the majority of losses, and others, where the payee's PSP bears the larger share.

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



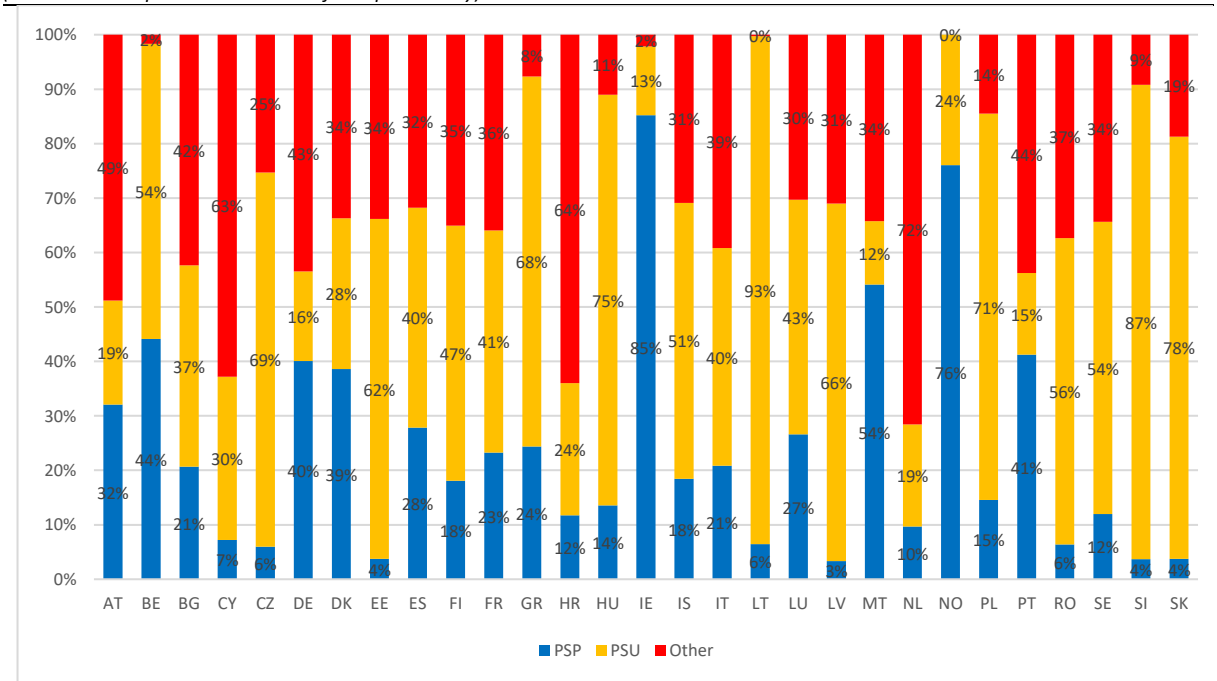
The distribution of fraud losses between PSUs and PSPs diverges significantly across the EEA. Multiple underlying reasons could help explain these disparities including divergent liability regimes across the EEA or divergent interpretations of key concepts under PSD2, such as the concepts of 'authorisation' of transactions and 'gross negligence', variations in the availability and effectiveness of dispute resolution mechanisms, consumer awareness and digital literacy, differences in national payment habits, and potential inconsistencies in reporting practices.

Moreover, with regard to the share of losses per country, it is important that the data is assessed jointly with the fraud levels, given that the outcome may be significantly influenced by countries with very low number of fraud cases.

In card payments for 2024, PSUs bore the overwhelming majority of losses (see Chart 20), often exceeding 70%, in countries like Slovakia, Slovenia, Hungary and Lithuania. Conversely, Ireland and Norway stand out for their high PSP liability, with PSPs covering more than three-quarters of fraud losses, over 80% in Ireland's case.

In several countries, notably Cyprus, Croatia and Netherlands, a large share of losses is attributed to the "Other" category. This suggests that liability is frequently assigned to the counterpart PSPs, among other parties, possibly reflecting more complex shared liability arrangements. Meanwhile, countries like France and Denmark show a relatively balanced distribution of losses across PSUs, PSPs.

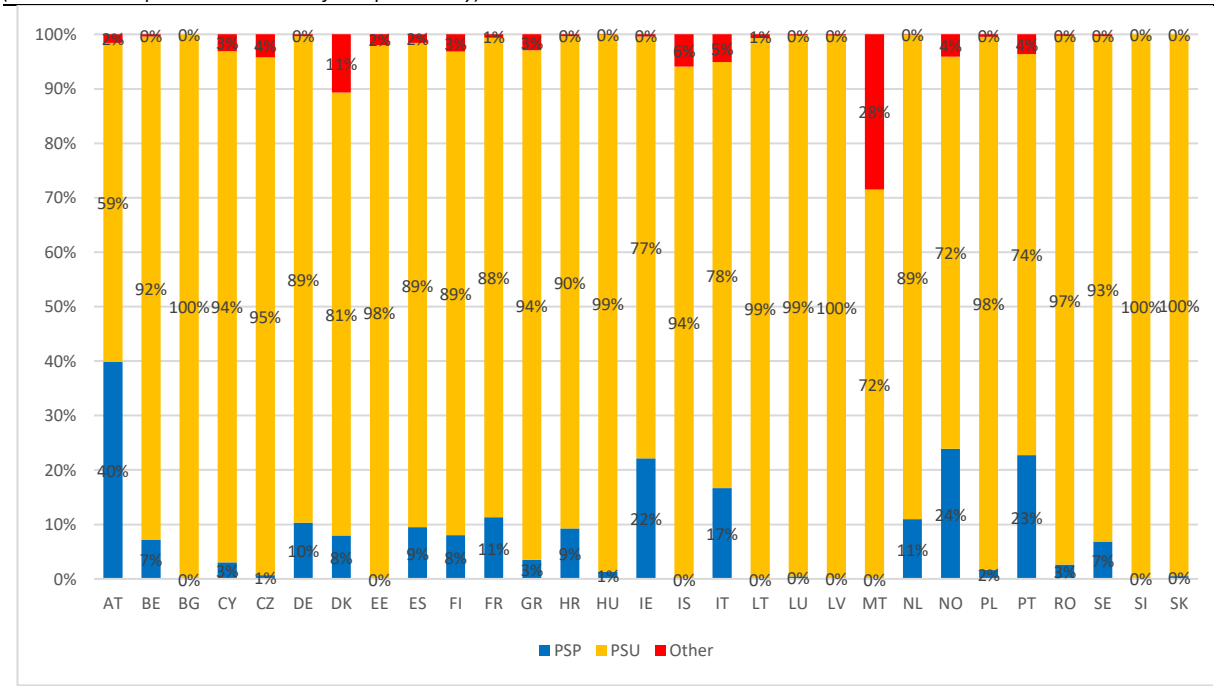
Chart 20: Composition of losses for card payments by liability bearer and country
(share in total reported losses due to fraud per country)



For credit transfers, in 2024, PSUs consistently bore the majority of losses across most countries (see Chart 21). Notably, all countries except Austria, Ireland, Italy, Malta, Norway and Portugal report PSU shares exceeding 80% of total fraud losses with this instrument. This suggests that in most countries the modus operandi of fraud with credit transfers, e.g. often with transactions being SCA authenticated, is particularly punishing to users who were held responsible for the losses related to credit transfers. Specifically, the possible consideration of all SCA authenticated transactions as authorised, could be a relevant reason behind those shares.

Austria is an outlier in this regard: PSPs bear approximately 40% of the total fraud losses, while PSUs account for around 59%. Only about 1.2% of losses are attributed to other entities, such as counterpart PSPs.

Chart 21: Composition of losses for credit transfer by liability bearer and country
(share in total reported losses due to fraud per country)



Fraud losses related to direct debits in 2024 were reported by only a limited number of EEA countries, and the distribution of liability among them varies significantly (as per Chart 22). Portugal and Slovakia stand out for assigning all reported fraud losses to "Other" entities, which may include the PSP counterpart. In contrast, Belgium reported all losses as being borne by PSPs. Czech Republic, Ireland and Luxembourg place the burden entirely on PSUs. France, Italy and Poland show a more mixed model distributing the losses among the three categories.

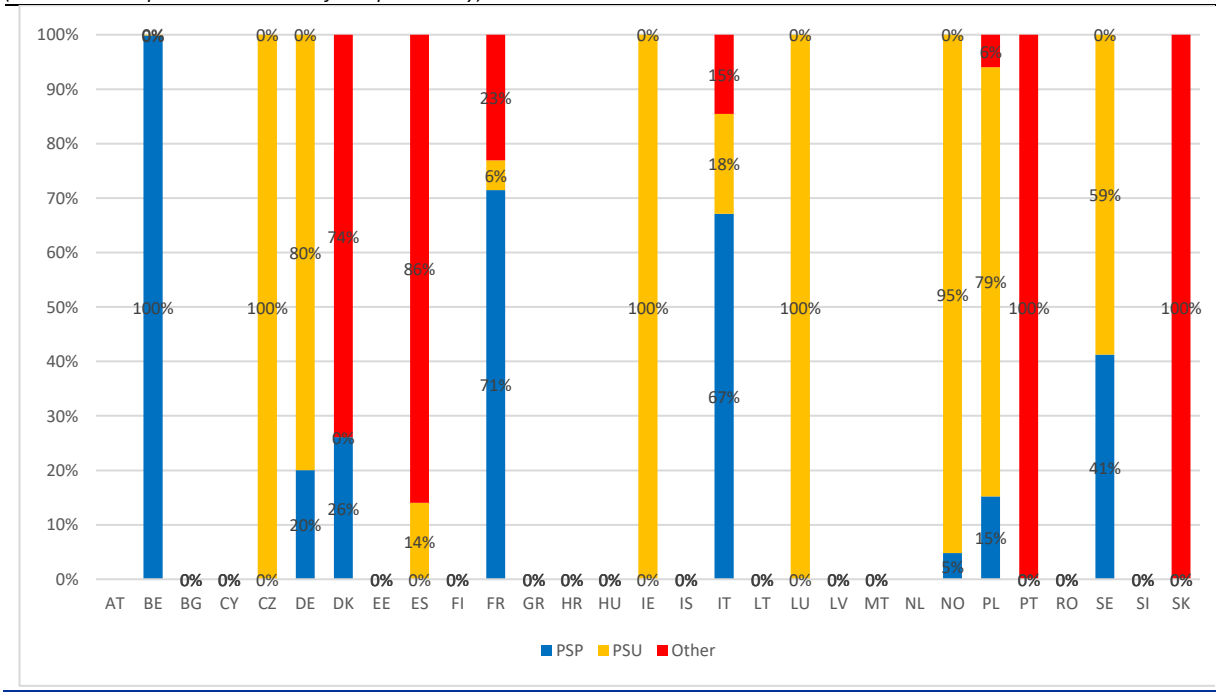
Direct debits differ from the other instruments in this matter as the "PSP" is the service provider of the payee instead of the service provider of the payer, and the "PSU" is the payee instead of the payer. This last part may help explain why in some countries, the PSUs, i.e. payees, bear the majority of losses, considering the protective measures the payers are entitled to with this instrument, particularly, the unconditional right to request the return of funds debited from their accounts within eight weeks[14].

[14] In case the direct debit is processed under the European Payment Council's SDD Core Scheme

However, significant divergencies are observed among the reporting countries, which might be due to differences in the use of this payment method across the EEA.

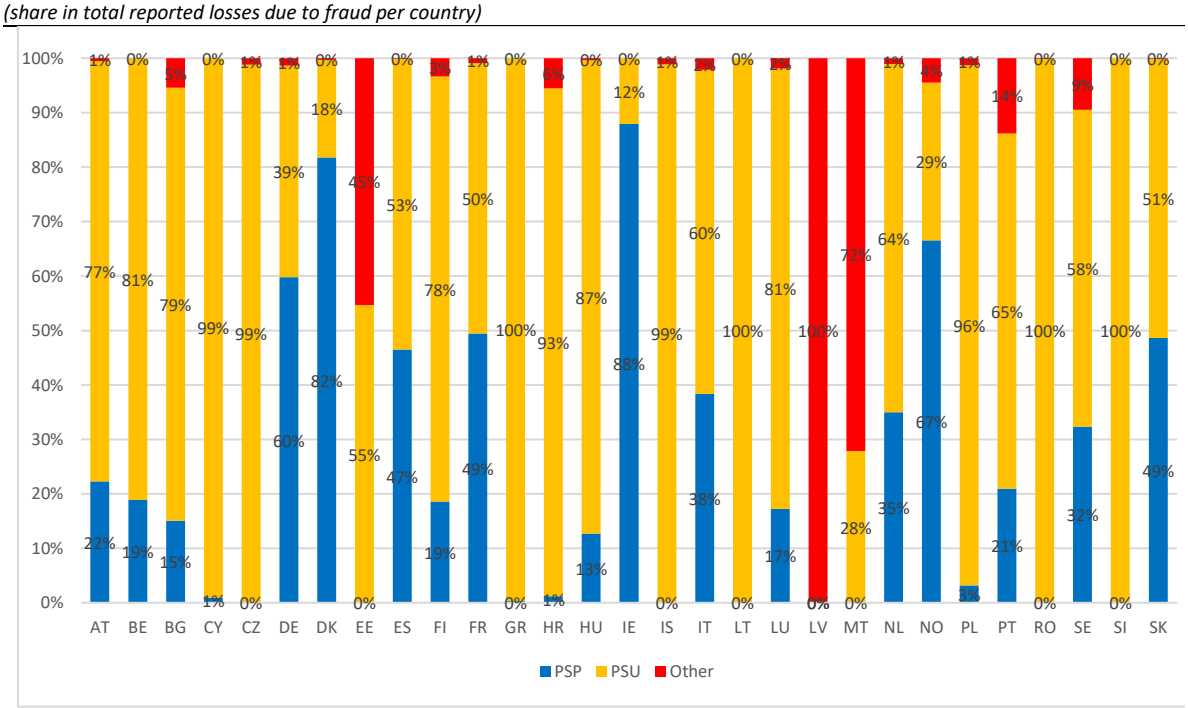
Moreover, a large number of EEA countries reported no data at all on fraud losses for direct debits. This may be linked to the unconditional refund rights for direct debits and the fact that under the EBA Guidelines PSPs are not required to investigate whether a refund for a direct debit was due to fraud. As a result, if a fraudulent transaction is refunded within the eight-week window and not explicitly flagged as fraud, it may go unreported in fraud statistics. In addition, the already mentioned low usage of direct debits in some countries may also explain in part this finding.

Chart 22: Composition of losses for direct debits by liability bearer and country
(share in total reported losses due to fraud per country)



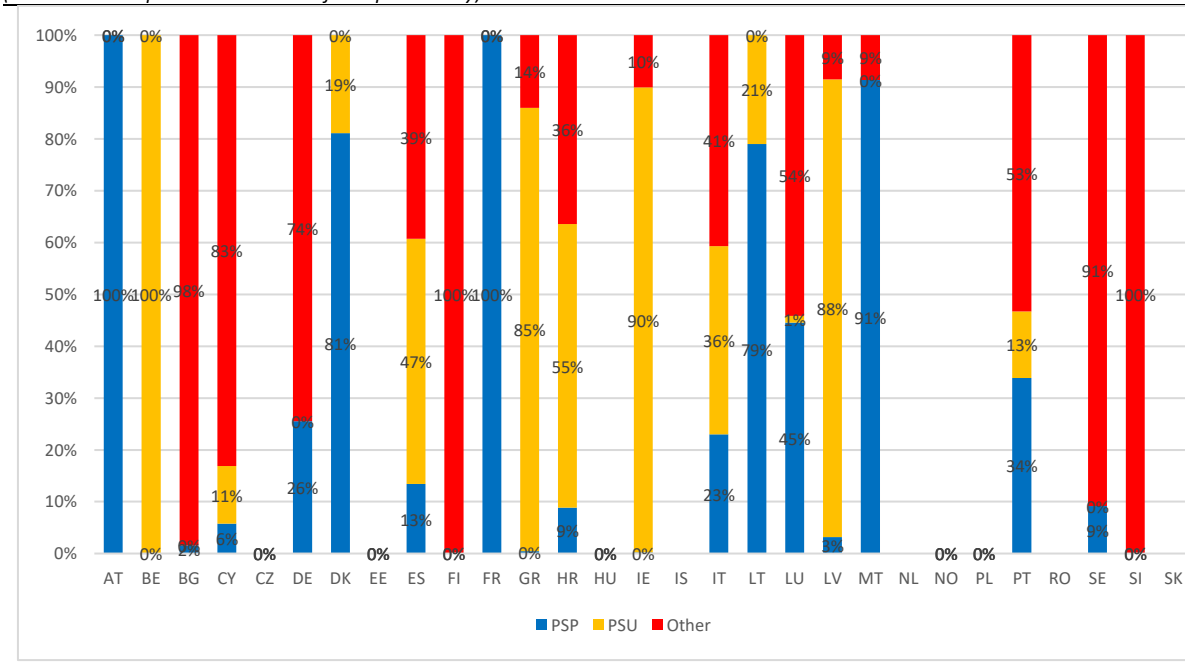
For cash withdrawals, in 2024, PSUs bore more than 70% of the reported fraud losses in more than half of the reporting countries (see Chart 23), namely Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Finland, Greece, Croatia, Hungary, Iceland, Lithuania, Luxembourg, Poland, Romania and Slovenia. In many of these, such as Greece, Lithuania, Romania, and Slovenia, PSUs had to bear the entirety of reported losses. In contrast, Denmark and Ireland stand out with PSPs covering over 85% of fraud losses in both cases. Only Latvia reports a case where all losses are attributed to “Other” entities, which may reflect unique reporting practices or liability arrangements involving third parties. Finally, Spain and France were the countries with a relatively balanced distribution of liability, where PSUs and PSPs each account for around 50% of losses.

Chart 23: Composition of losses for cash withdrawals by liability bearer and country
(share in total reported losses due to fraud per country)



Finally, for e-money, the distribution of losses between parties in 2024 varied significantly between countries (see Chart 24). In some countries, PSUs bore nearly all reported losses. Belgium, Greece, Ireland and Latvia are clear examples, with PSU shares exceeding 85%. Several countries report a more balanced distribution. Croatia and Spain each show even shares between PSUs and "Others", while Italy presents a three-way split with PSPs, PSUs, and "Others" all contributing substantially to the total. In contrast, some countries place the burden almost entirely on PSPs. Austria, Denmark, France and Malta report PSP shares ranging from 80% to 100%.

Chart 24: Composition of losses for e-money by liability bearer and country
(share in total reported losses due to fraud per country)



Assigning the majority of losses to “Other” entities is notable in a few countries, Bulgaria, Cyprus Sweden and Slovenia report “Other” shares ranging from 81% to 100%. Notably, many countries, including Czech Republic, Estonia, Hungary, Norway and Poland, report no data at all. This absence may reflect the lack of solutions offered on those countries and/or limited use of the ones that exist.

6. The geographical dimension of fraud

From a geographical perspective, although most payment transactions were domestic[15], fraud rates were significantly higher for cross-border[16] payments. During 2022-2024, the value of domestic credit transfers and card payments was between 73% and 82% of the total value of both (see Chart 25a); in volume terms, the shares of domestic in total transactions were around 96% for credit transfers and 80% for card payments (see Chart 26a).

However, in all periods analysed, around 70% of card payment fraud was related to cross-border transactions in terms of both value and volume (see Charts 25b and 26b). Also, high levels of fraudulent credit transfers are observed with the beneficiary being located in a different country, both within the EEA as well as outside. While only around 20% of the value of credit transfers were cross-border (around 4% in volume terms) across all periods, the share of fraud for this instrument ranged between 40% and 50% of the total value of credit transfers and 13% and 21% in volume terms. A notable share of fraudulent card payments (30% in value terms in 2024) was related to cross-border transactions outside the EEA.

The high levels of fraud in cross border credit transfers and card payments may be due to insufficient cooperation among PSPs and other market actors to deal with criminal activities between countries.[17] Also, for cross-border card payments that involve a PSP outside the EEA (one-leg out transactions), the application of SCA is inconsistent or absent, increasing vulnerability and impacting the fraud rates, as explained in a previous section.

Whereas most direct debit transactions were domestic, cross-border fraud was, at times, predominant. In 2024, cross-border direct debits accounted for 23% of the overall transactions in value terms. In the same period, fraudulent direct debits transacted cross-border accounted for 54% of total value.

By contrast, the majority of fraudulent cash withdrawals were domestic (90% in value and 84% in volume terms in 2024). Concerning e-money, domestic transactions accounted for 62% of the total value of fraud, while the share of cross-border fraud appeared higher than the domestic ones in volume terms (59% for 2024).

[15] Domestic payment transactions 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 Member State.

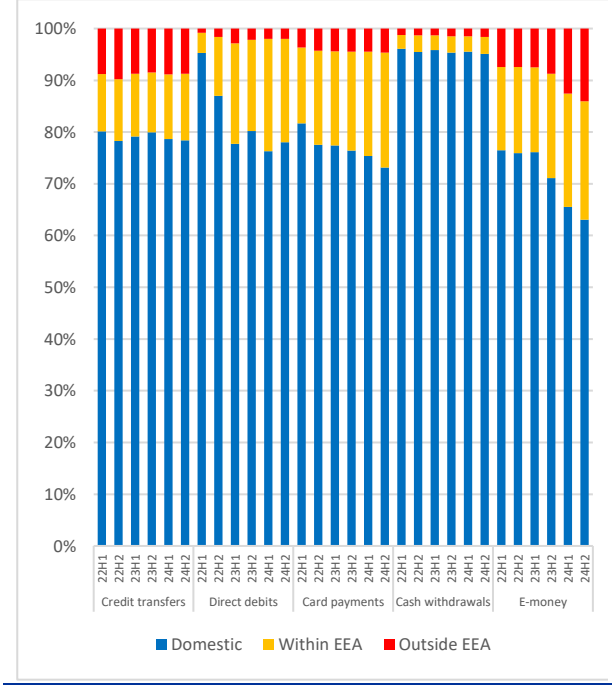
[16] Cross-border payment transactions encompass transactions where the sending and receiving PSP (or for non-remote card payments, the location of the point-of-sale terminal or ATM) are located in different Member States, either they are within or outside the EEA.

[17] See also EBA Opinion on new types of payment fraud and possible mitigants

Chart 205: 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)

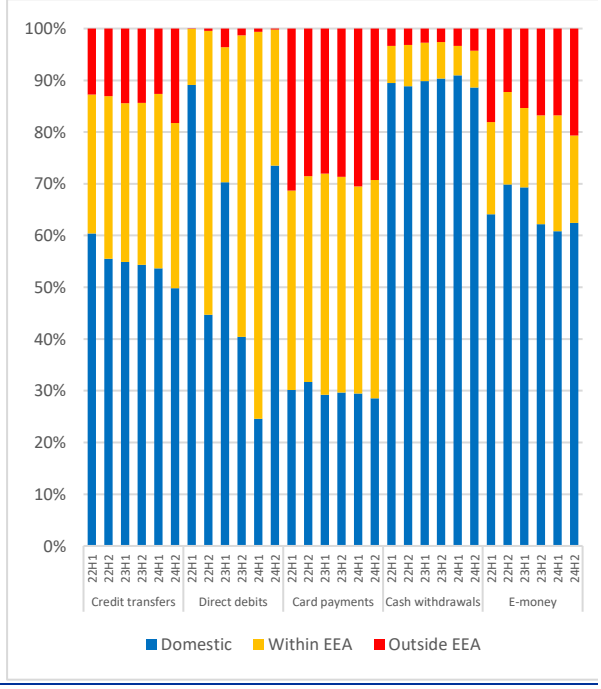
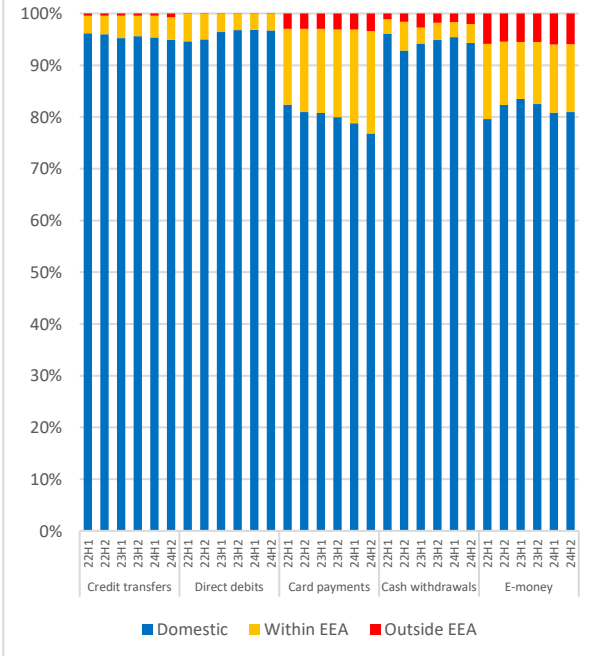


Chart 216: Composition of payment transactions and fraud by instrument and geographical dimension II

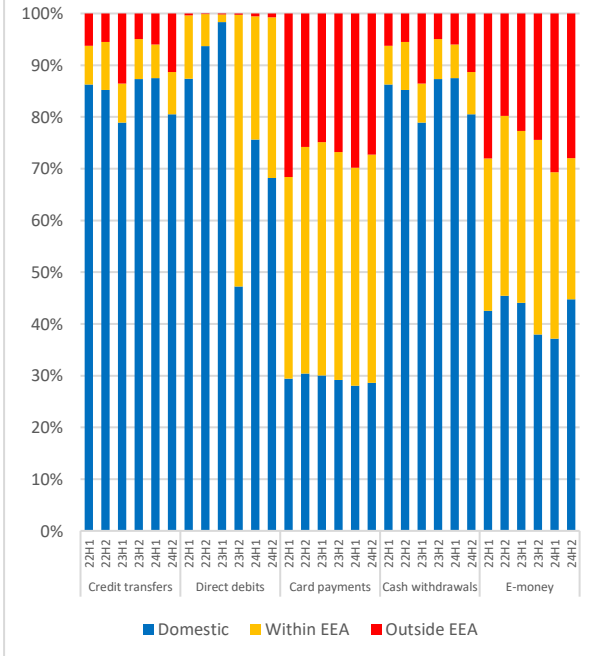
a) Volume of payment transactions

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



b) Volume of fraudulent payment transactions

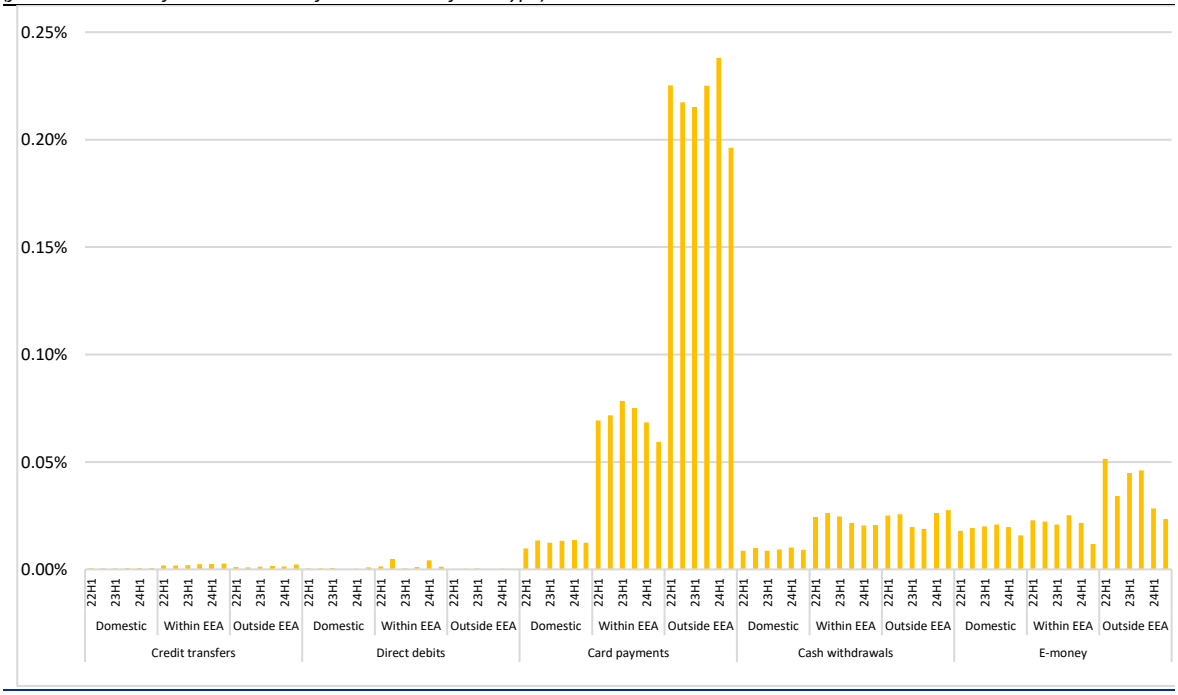
(volume of fraudulent transactions by geographical dimension in % of total fraud for each instrument)



Moreover, fraud rates for cross-border transactions within and outside EEA, are generally higher than for domestic transactions, with respect to all types of payments. Specifically, in 2024, the cross-border card payment fraud rate was more than seven times higher than for domestic transactions. This disparity was even greater for transactions limited to non-EEA counterparts,

where fraud rates were 17 times higher, potentially due to the absence of SCA requirements. Across all instruments, the comparison between fraud rates for domestic transactions with cross-border, both within and outside the EEA, were still significantly higher in credit transfers (more than three times higher), direct debits (more than twenty five times higher), cash withdrawals (more than twice higher), and, to a lesser extent, e-money payment transactions (1.11 higher, see Chart 27).

Chart 27: Relative fraud levels by instrument and geographical dimension (in value)
(fraud as a share of the total value of transactions of that type)



7. A country-by-country perspective on fraud

On a country-by-country basis, while absolute fraud levels will be naturally influenced by the overall value and volumes of the respective payment transactions, relative fraud rates vary considerably. Tables 1 and 2 provide an overview of the total value and volume of fraud in both absolute and relative terms by country and payment instrument, for the reference period 2024.

With respect to **credit transfers**, relative fraud rates in terms of value and volume continue to remain low across all countries. The lowest absolute level of fraud was observed for Liechtenstein (amounting to 8 fraudulent transactions with a value of EUR 174,415). Regarding fraud rates, the highest was observed for Slovenia at 0.006% in value terms, while Lithuania accounted for the highest fraud rate in terms of volumes (0.015%[18]).

Similarly, in **direct debits**, low fraud rates were observed across nearly all countries, with the exception of Slovakia. In fact, thirteen countries reported zero fraud in this payment instrument. As previously mentioned, this could be explained by the fact that, under the EBA Guidelines, PSPs are not always required to investigate whether a refund for a direct debit was due to fraud. Consequently, many fraudulent direct debits may go unreported if they are refunded within the eight-week window and not explicitly flagged as fraud. The highest fraud levels were reported for France, with over 52,000 fraudulent transactions, in volume terms, and Germany totalling EUR 72.2 million, in value terms. In relative terms, Slovakia experienced the largest fraud rate by volume (0.011%) and the highest fraud rate by value (0.044%).

Fraudulent card payments reported by issuing PSPs located in the EU/EEA were the lowest in Latvia (22,489 transactions) and the highest in France (over 7.1 million transactions) in volume terms. France also reported the highest card fraud value, amounting to EUR 484 million, and recorded the highest fraud rates in both value and volume terms (0.057% and 0.034%, respectively).

Cash withdrawals showed generally low fraud rates across all EU/EEA countries in 2024, with some exceptions. The highest fraud rates in value terms were observed for Denmark (0.070%) and France (0.033%). In contrast, very low levels of fraud and corresponding fraud rates were observed for Romania and Liechtenstein, both reporting 0.000%. In volume terms, the highest fraud rates were recorded for France (0.012%), Lithuania (0.011%), and Estonia (0.002%).

Fraudulent e-money transactions in 2024 appeared to be concentrated in countries where e-money payments were more prevalent. In absolute terms, Luxembourg reported the highest value of fraudulent payment transactions (EUR 45.3 million), while Italy recorded the highest volume (over 447,000 transactions). In relative terms, Poland showed the highest fraud rate by value (0.111%), and Greece had the highest fraud rate by volume terms, with 0.028%.

[18] Based on corrected data submitted after the deadline, the associated fraud rates for credit transfers in terms of value changed considerably and is likely not the highest anymore.

Table 1: Absolute and relative levels of payment fraud in value terms (2024, 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	65,989,654	0.001%	-	-	19,645,025	0.024%	391,268	0.001%	2,632	0.000%
BE	216,038,048	0.002%	87,797	0.000%	53,094,226	0.032%	3,132,304	0.012%	0	0.000%
BG	5,559,385[19]	0.001%[19]	0	0.000%	4,736,123	0.023%	156,931	0.001%	31,636	0.002%
CY	2,718,484	0.001%	0	0.000%	2,251,185	0.015%	26,752	0.001%	42,287	0.001%
CZ	46,881,891	0.001%	65	0.000%	20,880,548	0.029%	1,989,939	0.005%	0	0.000%
DE	474,164,942	0.001%	72,217,429	0.001%	124,544,539	0.022%	27,056,899	0.008%	54,673	0.008%
DK	38,076,399	0.001%	322,306	0.000%	32,231,557	0.038%	3,122,679[20]	0.070%	94,178	0.014%
EE	10,407,273	0.003%	0	0.000%	2,229,503	0.020%	891,653	0.014%	0	0.000%
ES	153,027,315	0.001%	4,132,440	0.001%	140,967,863	0.038%	17,360,834	0.014%	2,787,720	0.019%
FI	64,162,532	0.002%	0	0.000%	14,780,971	0.020%	341,887	0.005%	34,912	0.008%
FR	350,992,884	0.001%	30,365,272	0.001%	484,039,292	0.057%	44,499,471	0.033%	95,876	0.008%
GR	12,168,897	0.001%	0	0.000%	11,327,082	0.017%	1,132,598	0.003%	265,648	0.055%
HR	12,572,657	0.002%	0	0.000%	5,751,537	0.025%	153,261	0.001%	220,908	0.011%
HU	69,801,157[20]	0.002%	0	0.000%	25,931,597	0.052%	1,300,893	0.006%	0	0.000%
IE	67,407,748	0.001%	9,534	0.000%	45,112,633	0.029%	752,580	0.005%	25,633,955	0.029%
IS	3,394,366	0.001%	**0**	0.000%	3,146,347	0.030%	161,349	0.032%	-	-
IT	158,958,560	0.002%	2,036,264	0.000%	79,260,954	0.021%	18,787,508	0.010%	18,539,276	0.024%
LT	74,935,781[21]	0.005%	2,296[21]	0.000%	36,735,019[21]	0.048%	2,578,891[21]	0.017%	6,585,231[21]	0.026%
LU	70,847,579	0.002%	177,376	0.002%	10,450,124	0.046%	678,971	0.017%	45,278,657	0.017%
LV	9,898,590	0.001%	0	0.000%	1,815,118	0.018%	862,967	0.019%	0	0.000%
MT	3,173,477	0.003%	0	0.000%	2,291,362	0.030%	22,309	0.001%	427,691	0.001%
NL	142,036,059	0.000%	-	-	37,812,516	0.019%	5,798,657	0.016%	-	-
NO	68,180,939	0.001%	0	0.000%	37,048,829	0.035%	606,633	0.005%	49,529	0.015%
PL	163,627,757	0.001%	346	0.000%	21,698,379	0.013%	1,450,148	0.002%	8,638	0.111%
PT	15,766,916	0.001%	106,100	0.000%	26,297,692	0.018%	601,573	0.002%	29,726	0.001%
RO	63,871,808	0.002%	0	0.000%	9,997,143	0.015%	207,488	0.000%	-	-
SE	116,142,017	0.002%	9,099	0.000%	28,731,117	0.025%	1,390,380	0.009%	1,404,167	0.025%
SI	21,825,505	0.006%	89	0.000%	3,943,079	0.029%	88,862	0.001%	18,812	0.011%
SK	13,447,033	0.001%	1,982,072	0.044%	7,477,633	0.025%	196,852	0.001%	-	-
EU total	2,516,075,653	0.001%	112,096,314	0.001%	1,294,228,994	0.033%	135,742,538	0.010%	101,942,164	0.018%

("-" represents datapoints deleted for confidentiality reasons)

[19] Revised data points have exceptionally been included for Bulgaria for the purpose of this specific table.

[20] At present, this value and respective fraud rate are underreported due to incorrect data submissions received from reporting entities. They will be corrected retrospectively when data will be reported for forthcoming reporting periods.

[21] At present, this value and respective fraud rate are overreported due to incorrect data submissions received from reporting entities. They will be corrected retrospectively when data will be reported for forthcoming reporting periods.

Table 2: Absolute and relative levels of payment fraud in volume terms (2024)

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	32,745	0.004%	-	-	179,124	0.009%	976	0.000%	81	0.000%
BE	87,235	0.004%	97	0.000%	461,738	0.012%	5,712	0.004%	0	0.000%
BG	1,769	0.001%	0	0.000%	82,039	0.014%	1,150	0.001%	197	0.001%
CY	360	0.001%	0	0.000%	23,647	0.010%	81	0.001%	1,088	0.009%
CZ	26,072	0.002%	1	0.000%	232,448	0.008%	1,686	0.001%	0	0.000%
DE	153,909	0.002%	1,520	0.000%	1,358,683	0.010%	82,332	0.006%	529	0.002%
DK	10,310	0.001%	23	0.000%	296,256	0.013%	5,453	0.002%	88	0.000%
EE	5,496	0.002%	0	0.000%	24,276	0.005%	990	0.002%	0	0.000%
ES	86,382	0.003%	12,403	0.001%	2,579,585	0.022%	53,999	0.009%	58,738	0.021%
FI	21,680	0.002%	0	0.000%	147,977	0.006%	1,216	0.002%	462	0.004%
FR	132,298	0.002%	52,718	0.001%	7,112,201	0.034%	126,078	0.012%	3,232	0.003%
GR	5,032	0.001%	0	0.000%	211,974	0.009%	2,363	0.002%	8,509	0.028%
HR	4,923	0.001%	0	0.000%	79,957	0.011%	650	0.001%	5,315	0.008%
HU	18,145[22]	0.004%	0	0.000%	202,574	0.010%	4,281	0.005%	0	0.000%
IE	30,168	0.003%	89	0.000%	453,313	0.015%	2,762	0.003%	37,058	0.009%
IS	586	0.001%	**0**	0.000%	21,114	0.010%	121	0.006%	-	-
IT	121,218[23]	0.005%	2,824	0.000%	988,473	0.012%	40,329	0.005%	447,039	0.018%
LT	96,167[23]	0.015%	14[23]	0.000%	488,203[23]	0.016%	9,952[23]	0.011%	2,341[23]	0.002%
LU	2,867	0.002%	14	0.000%	87,787	0.020%	1,393	0.008%	392,671	0.008%
LV	8,161	0.003%	0	0.000%	22,489	0.004%	1,298	0.005%	0	0.000%
MT	1,950	0.009%	0	0.000%	20,817	0.017%	102	0.001%	6,215	0.007%
NL	95,096	0.002%	-	-	410,947	0.006%	11,837	0.007%	-	-
NO	17,614	0.001%	0	0.000%	222,971	0.007%	2,246	0.010%	51	0.000%
PL	124,090	0.002%	12	0.000%	335,471	0.004%	5,997	0.002%	11	0.015%
PT	5,737	0.001%	421	0.000%	555,738	0.019%	4,060	0.001%	1,550	0.002%
RO	25,075	0.003%	0	0.000%	122,471	0.005%	793	0.000%	-	-
SE	39,709	0.001%	54	0.000%	233,902	0.006%	4,936	0.005%	1,004	0.024%
SI	2,991	0.002%	4	0.000%	40,114	0.010%	233	0.001%	81	0.002%
SK	8,201	0.002%	3,720	0.011%	62,874	0.006%	528	0.001%	-	-
EU total	1,164,217	0.002%	73,935	0.013%	17,059,163	0.015%	373,554	0.005%	968,945	0.011%

("-" represents datapoints deleted for confidentiality reasons)

[22] At present, this value and respective fraud rate are underreported due to incorrect data submissions received from reporting entities. They will be corrected retrospectively when data will be reported for forthcoming reporting periods.

[23] At present, this value and respective fraud rate are overreported due to incorrect data submissions received from reporting entities. They will be corrected retrospectively when data will be 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), which only need to 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 been collected in most EEA countries 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 responsible NCB and provided in aggregated form 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[24]). The reporting periods covered by the present analysis include H1 2022, H2 2022, H1 2023, H2 2023, H1 2024 and H2 2024. The data used as the basis for this report has a cut-off date of 11 July 2025 with respect to data reported to the ECB in accordance with the ECB Regulation on payments statistics and 7 October

[24] 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. Credit transfer data for H2 2024 from Bulgaria was excluded from the aggregate analysis due to a data quality issue that significantly impacted the readability of the affected charts.

2025 with respect to data for the remaining EU/EEA countries reported to the EBA under the EBA Guidelines on fraud reporting under PSD2.

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 CAs and/or NCBs 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.


eba
European
Banking
Authority


EUROPEAN CENTRAL BANK
EUROSYSTEM