Box 2.7

EVOLUTION OF FRAUD IN PAYMENT OPERATIONS

Since 1 January 2020, payment service providers (PSPs) have been required to provide their national competent authority with statistical data on fraud relating to the various means of payment, under the PSD2 regulatory framework and its subsequent developments. The European Central Bank (ECB) Regulation on payment statistics also requires PSPs to report this information. With regard to Spanish PSPs, the Banco de España has been monitoring fraud reporting with a view to gradually improving the quality of the data provided by supervised institutions and being able to assess their evolution more effectively.

The collection of these data facilitated the publication in 2024 of a joint report by the ECB and the European Banking Authority,[1] which is to date the most comprehensive publication on payment fraud within the European Union (EU).

Chart 1
Evolution of fraud rates with and without SCA in credit transfers and card transactions by number of transactions

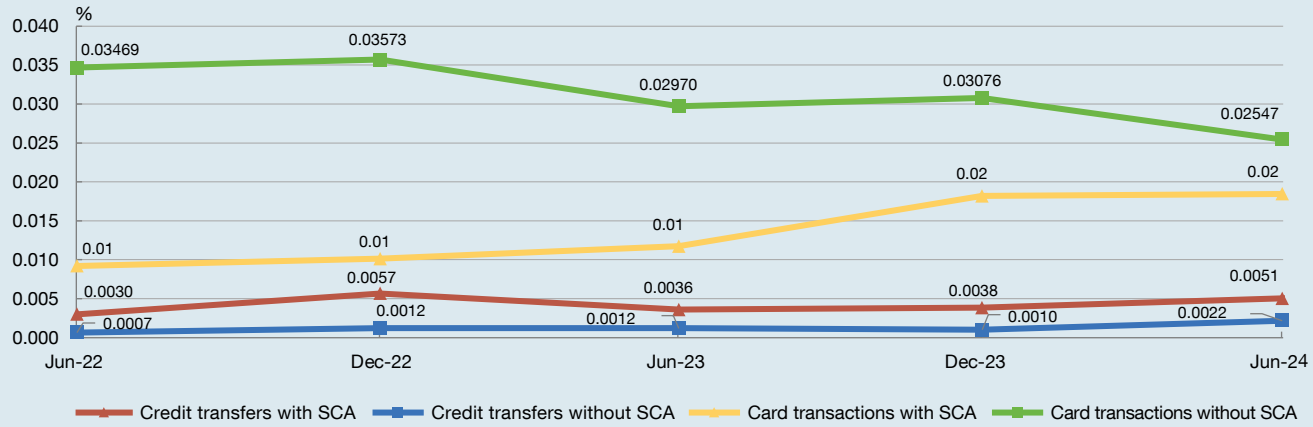


Chart 2
Causes of fraud in card transactions

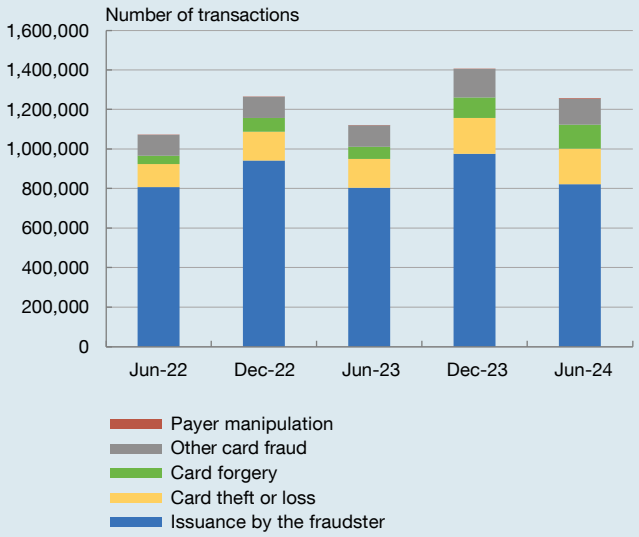
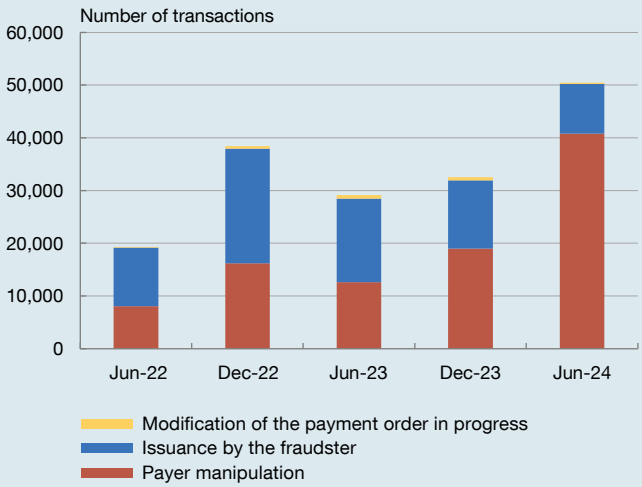


Chart 3
Causes of fraud in credit transfers



SOURCE: Compilation of payment and fraud statistics based on the requirements of Regulation (EU) No 1409/2013 of the European Central Bank, amended by Regulation (EU) No 2020/2011 of 1 December 2020 on payment statistics, which establishes the framework for the collection of statistics on payments by the European System of Central Banks.

1 Banco de España press release dated 1 August 2024.

Box 2.7
EVOLUTION OF FRAUD IN PAYMENT OPERATIONS (cont'd.)

At the national level, the evolution of data for the last two years does not diverge greatly from the findings of the aforementioned European report. Credit transfers and card transactions are the payment methods with the highest number and value of fraudulent transactions. By way of example, the data from the joint report by the ECB and the European Banking Authority show a fraud rate in terms of number of transactions in the European Economic Area in the first half of 2023 of 0.003% for credit transfers and 0.015% for card transactions, while at the domestic level, these rates are 0.002% and 0.023%, respectively.

Among the breakdowns required by the regulation, the application of strong customer authentication (SCA) in payment transactions is an essential source of information on the role of this measure in mitigating the fraud risk.

Chart 1 shows the effect of SCA on card transactions and credit transfers, revealing that, in contrast to what might be expected, in both cases the fraud rate appears to be rising in transactions with SCA.

This fact is brought about by fraudsters seeking new ways to operate despite SCA, mainly through customer manipulation and identity theft, which lead customers to correctly authenticate transactions (even by applying SCA) that are actually fraudulent.

Payer manipulation and identity theft occur in transactions that are generally high value, through techniques such as phishing, vishing, spoofing or similar, known as "social engineering fraud techniques". However, the implementation of SCA has helped keep the fraud rate at relatively low levels, although it will be necessary to pay attention to the effects of the greater use of instant credit transfers in the future, where fund movements are almost instantaneous.

In this regard, Chart 3 shows how, in the case of credit transfers, fraud involving the manipulation of the payer by the fraudster is gaining relative weight each year (particularly due to so-called "CEO fraud") and now accounts for almost 80% of the number of fraudulent transactions. In the case of card transactions (see Chart 2), the theft of personal security credentials for issuing orders by fraudsters has been declining, as a result of the greater complexity introduced by the increasingly widespread use of SCA.

The above data would seem to show that, although SCA has had a positive impact on the fight against fraud, it is not effective, on its own, to eliminate it, due to its limited capacity to combat fraudulent social engineering practices.

This fact has given rise to various regulatory initiatives aimed, inter alia, at improving protection against fraud. In this regard, DORA[2] will demand more rigorous technology risk management by PSPs, which should mitigate the risk linked to the exploitation of technical vulnerabilities. The so-called Instant Payments Regulation[3] includes the obligation for the PSP of the payer to offer the payer a service ensuring the verification of the payee to whom the credit transfer is sent, immediately after the relevant information is provided and before the payer is offered the possibility of authorising the transaction. Also, the current PSR/PSD3 proposal contains various operational measures aimed at reinforcing the application of SCA, such as real-time monitoring of transactions, the possibility of sharing information on fraud among PSPs, cooperation between electronic communications service providers and PSPs to ensure the confidentiality and security of communications and raising awareness among payment service users about fraud.

2 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

3 Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro.