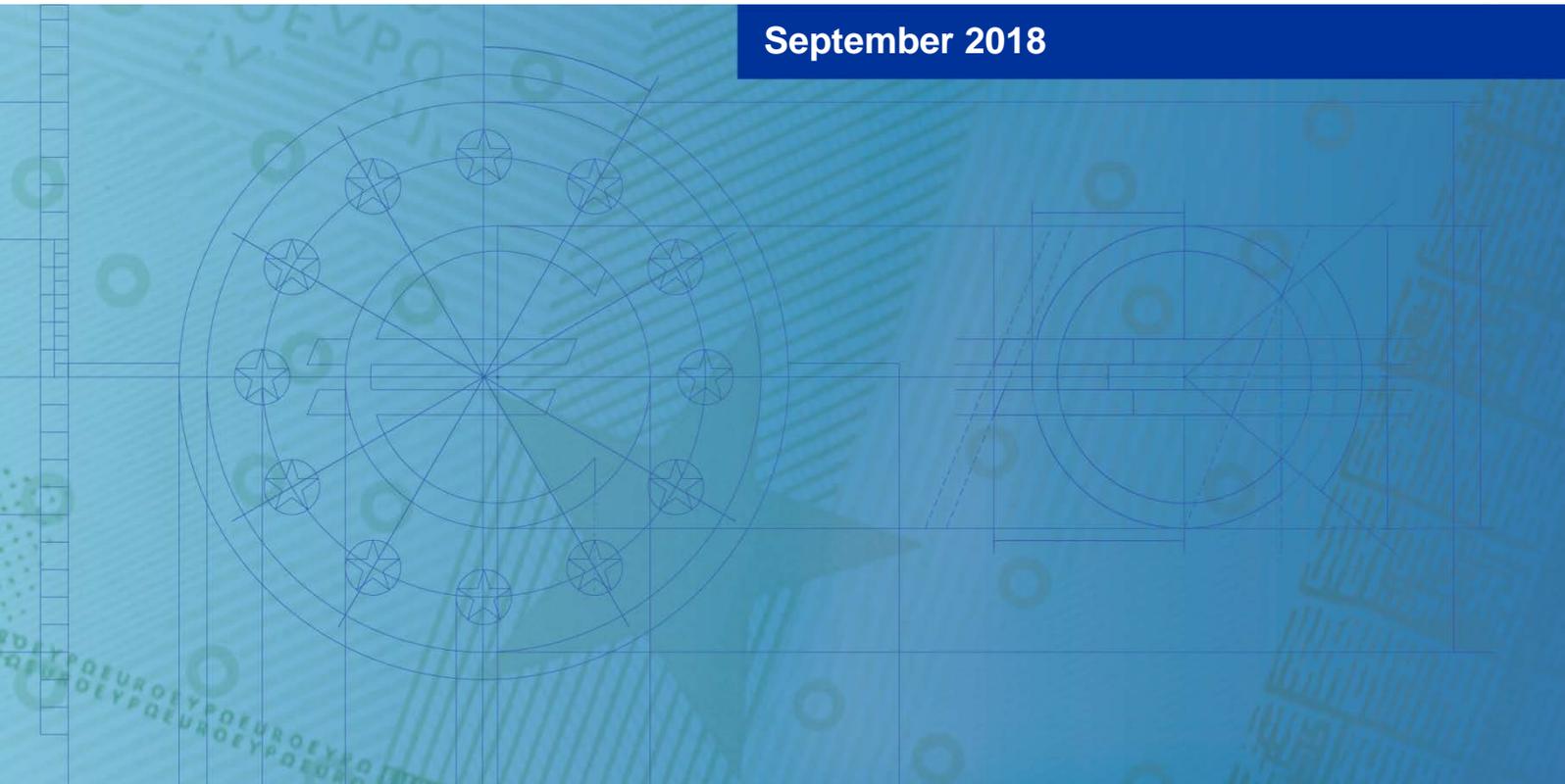




EUROPEAN CENTRAL BANK
EUROSYSTEM

Fifth report on card fraud

September 2018



Contents

Executive summary	2
Introduction	5
1 Total level of card fraud	7
2 Card fraud according to different card functions	9
3 Card-not-present fraud	10
Box 1 Some market perspectives on online card fraud	10
4 Categories of fraud committed at ATMs and POS terminals	13
Box 2 Some market perspectives on card-present fraud	14
5 Domestic and cross-border card fraud	16
6 A country-by-country perspective on card fraud	19
7 Conclusions	27

Executive summary

This fifth oversight report on card fraud analyses developments in fraud related to card payment schemes (CPSs) in the Single Euro Payments Area (SEPA) and covers almost the entire card market.¹ It provides an overview of developments in card payment fraud between 2012 and 2016.

The total value of fraudulent transactions conducted using cards issued within SEPA and acquired worldwide amounted to €1.8 billion in 2016 – a decrease of 0.4% compared with 2015. In relative terms, i.e. as a share of the total value of transactions, fraud dropped by 0.001 percentage point to 0.041% in 2016, down from 0.042% in 2015. Compared, again in relative terms, with the levels of fraud observed in 2012, fraud increased by 0.003 percentage points in 2016. Although there was an upward trend in card fraud between 2012 and 2015, it seems the trend is changing, given that fraud went down in 2016.

With respect to the composition of card fraud in 2016, 73% of the value of card fraud resulted from card-not-present (CNP) payments, i.e. payments via the internet, post or telephone, 19% from transactions at point-of-sale (POS) terminals and 8% from transactions at automated teller machines (ATMs).²

With €1.32 billion in fraud losses in 2016, CNP fraud was not only the largest category of fraud in absolute value but, unlike ATM and POS fraud, it was also the only one to record an increase (of 2.1%) compared with the previous year. Data on regular, i.e. non-fraudulent, CNP transactions, which are only partially available, suggest that there was also considerable growth in CNP transactions on the whole. Based on this partial information, it can be concluded that CNP fraud grew at a lower rate than CNP transactions.

In an interview, market representatives from a European security forum³ confirmed that there is an ongoing shift of fraud from the card-present to the card-not-present environment. However, the market has started to develop a plethora of fraud prevention and detection security tools with the objective of bringing online fraud rates down (e.g. implementation of 3D Secure, risk-based analysis, Tokenization). In addition, the European regulators have contributed to fighting online fraud with regulatory tools – the 2013 Recommendations for the security of internet payments and the 2014 Guidelines on the security of internet payments⁴. Recently, they also strengthened the security requirements for electronic payments with the revision of the Payment Services Directive (PSD2) in 2015 and specified further such requirements

¹ This report focuses mainly on data analysis and key messages. The general information on card usage, data collection methodology and classification provided in the first report on card fraud is not repeated in this version (see <https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201207en.pdf>).

² The same trends were observed with respect to fraud volumes, although ATM fraud was less prevalent and CNP fraud was more common.

³ Card Fraud Prevention Forum (CFPF) of the European Payments Council (EPC).

⁴ These guidelines, published by the European Banking Authority, applied as of August 2015 and thus may have had an impact in slowing down the increase of online fraud in the second half of 2015 and 2016.

in the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication in 2017.

The largest drop in the level of fraud concerned card fraud committed at ATMs, with 12.4% less fraud in 2016 compared with 2015, while fraud committed at POS terminals went down by 3.0%. The lower level of ATM fraud was mainly due to a substantial decrease in counterfeit card fraud and fraud using lost and stolen cards following the migration of cards and terminals to EMV. Fraud using lost and stolen cards accounted for 47% of the value of fraud at ATMs and POS terminals, while counterfeit card fraud made up 43%. As observed in previous years, counterfeit card fraud was predominant for transactions acquired in countries outside SEPA. This trend continued in 2016, although that geographical category has seen a decrease in counterfeit card fraud compared with 2015.

For delayed debit cards and credit cards, CNP fraud was the most common type of fraud in 2016, accounting for 76% of the total value, followed by fraud occurring at POS terminals (20%) and ATMs (4%). For debit cards, CNP fraud was also the most common type, making up 71% of the total fraud value for these cards, followed by POS and ATM fraud, which accounted for 19% and 10% respectively.

From a geographical perspective, domestic transactions accounted for 90% of all transactions, but only 35% of fraudulent transactions. Cross-border transactions within SEPA made up for 8% of all transactions, but 43% of fraudulent transactions. Finally, although only 2% of all transactions were acquired outside SEPA, they accounted for 22% of all fraud. The euro area experienced slightly lower fraud levels from an issuing and acquiring perspective than SEPA as a whole.

Compared with SEPA as a whole, fraudsters in the euro area focused more on ATM and POS fraud (fraud committed at ATMs and POS terminals accounted for 30% of the total value of fraud in the euro area, compared with 27% in SEPA). The difference can be attributed mainly to the influence of the United Kingdom, which had a relatively high share of CNP fraud and, with its total level of fraud, accounted for 40% of total fraud losses on cards issued within SEPA.

This report also covers data on transactions conducted using cards issued outside SEPA, but acquired inside SEPA. These data show that there are higher fraud losses on non-SEPA issued cards used inside SEPA than there are on SEPA issued cards used outside SEPA. This also holds true in relative terms in relation to the value of transactions: 0.57% of the value of transactions acquired inside SEPA using non-SEPA issued cards was fraudulent, compared with 0.44% of the value of transactions acquired outside SEPA using cards issued inside SEPA. The finding suggests that European cardholders also benefit from high European security standards for transactions conducted outside SEPA.

For individual European Union (EU) Member States, large variations with respect to card usage were identified, as in the previous report: the number of cards per inhabitant ranged from 0.8 to 3.9⁵, the number of payments made per year per

⁵ The 3.9 cards issued per inhabitant relates to Luxembourg, where a portion of cards are issued to cardholders not living in Luxembourg.

inhabitant ranged from 26 to 329, while the corresponding transaction values ranged between €1,800 and more than €17,000 per year and inhabitant. Fraud shares, i.e. the fraud-related share of the transaction value or volume, ranged from 0.005% for cards issued in Poland to 0.073 % for cards issued in Denmark in terms of value, and from 0.002% in Poland to 0.043% for cards issued in France in terms of volume. There were also big differences with respect to the transaction channels used by fraudsters in the EU. Broken down by country of card issue, fraud committed at ATMs ranged from 0% to 18% of the total, the share of CNP fraud ranged from 41% to 84%, and the share of POS fraud ranged from 13% to 55%. Broken down by country of acquirer, these variations were even larger; ATM fraud ranged from 0% to 26%, CNP fraud from 33% to 93% and POS fraud from 7% to 61%.

Most of the countries with significant card markets (defined as countries with high volumes and values of card transactions per inhabitant) experienced high rates of fraud. CNP fraud was typically the most common type of fraud involving cards issued in these markets. By contrast, countries with limited card usage experienced relatively low levels of fraud.

In summary, in 2016 the total value of card fraud decreased. Fraud involving cards issued inside SEPA increased for CNP transactions and decreased across the other transaction channels. In 2016 CNP fraud accounted for 73% of total fraud losses on cards issued inside SEPA, compared with 71% in 2015. Furthermore, and unlike 2015, fraud at ATMs and POS terminals decreased in 2016 following the near completion of migration to the EMV standard within SEPA. The drop in card-present fraud could be a result not only of this migration within SEPA but also of an increasingly high adoption rate of EMV for terminals outside Europe⁶. A wider usage of geo-blocking⁷, as well as increased physical security measures at terminals (e.g. lids to protect PIN entry, skimming device detectors, etc.) and the deactivation of the option to fall back to magnetic stripe (or “magstripe”) usage for cards might also be among the factors that contributed to this reduction. While ATM and POS fraud diminished substantially (and at a high pace between 2012 and 2016) as more countries outside SEPA migrated to EMV, CNP fraud saw a slight increase in 2016. The application of the Eurosystem’s “Guide for the assessment of card payment schemes against the oversight standards” (February 2015) could also have contributed to making card payment schemes more secure. In particular, the application of the Recommendations for the security of internet payments⁸, which are incorporated into the above-mentioned guide, may have helped limit the increase of online fraud.

⁶ Source: EMVco global adoption statistics.

⁷ Geo-blocking refers to blocking transactions abroad using EU-issued cards unless options allowing such transactions have been activated in advance.

⁸ Recommendations for the security of internet payments, European Central Bank, January 2013.

Introduction

In January 2008 the ECB's Governing Council approved an oversight framework for card payment schemes (CPSs). As part of the harmonised implementation of this framework, statistical information is gathered on card schemes. Each scheme is asked to supply general business data and volumes and values of transactions and fraudulent transactions per country for all Single Euro Payments Area (SEPA) countries as well as in aggregate for all countries outside SEPA. For automatic teller machines (ATMs) and point-of-sale (POS) terminals, fraud figures are broken down into "lost and stolen", "card not received", "counterfeit" and "other", while for total card-not-present (CNP) transactions, there is an option to provide a breakdown of the figures according to "online" and "mail or phone" fraud. Data collection is based on common templates and definitions. Please note that fraud is defined independently of whether the loss ends up being borne by the customer, issuer, acquirer or merchant.

This report summarises the information received from the following 22 CPSs: Sistema 4B, American Express, Bancontact, Oney Bank, BNP Paribas Personal Finance, Cartes Bancaires, Cashlink, Cofidis, Cofinoga, CONSORZIO BANCOMAT, Crédit Agricole Consumer Finance, Dankort, Diners Club International, EURO 6000, Franfinance, girocard, JCB International, Karanta, MasterCard Europe, Quikcash, ServiRed, SIBS' MB, and Visa Europe.

A comparison of the transaction data gathered from CPSs with data held in the ECB's Statistical Data Warehouse (SDW) suggests that the data available for 2016 exceed the total value of transactions within the European Union (EU) by 5%. However, this figure must be treated with caution as it may reflect both gaps in SDW data and double-counting of data reported for oversight purposes. Unfortunately, for four countries the coverage is below 90% of the value of transactions owing to the fact that either oversight requirements, including statistical reporting, were waived for some CPSs or as a result of incomplete data reporting. For another six countries the coverage is above 110% of the total value of transactions in SDW owing to the double-reporting of data – by international and domestic schemes alike – or to the fact that some types of small payment service providers (PSPs) are exempt from reporting under the ECB Regulation on payment statistics.

For Luxembourg, a further comparison of data available from other sources with the data provided for oversight purposes showed discrepancies in transaction and fraud levels.⁹ Such discrepancies, as well as those mentioned earlier, have been tolerated for the purpose of the present report.

This report rests on a number of assumptions and thus data adjustments in order to avoid the double-counting of figures reported by domestic card schemes and international ones have been made. Two methodological data issues identified a few years ago remain valid for this report, namely that some CPSs allocate (i) transactions

⁹ The main discrepancies came from the way CPSs split their card data per country, as explained in Footnote 10. The fact that Luxembourg issues a large number of cards for areas of use other than its own greatly affects the statistics for the country.

with cross-border issued cards to issuing SEPA countries by the area of use as opposed to the location of the issuer and ii) cross-border acquired CNP transactions according to the location of the acquirer instead of the location of the merchant. These methodological divergences result in some inconsistencies between data collected from the CPSs and similar data from the PSPs reported for SDW purposes; however, as they are limited to some schemes and countries they are considered tolerable.

The national central banks and the ECB have checked and processed the data with due care. Nevertheless, errors related to data provision, transmission or processing cannot be excluded.

Results “from an issuing perspective” refer to payments made with cards issued within SEPA and acquired worldwide. Results “from an acquiring perspective” therefore refer to transactions conducted using cards issued worldwide and acquired inside SEPA. Results are generally derived from an issuing perspective¹⁰, except in Chapter 6, where the acquiring perspective is adopted for some results. In these cases, the change of perspective is highlighted.

The report is structured as follows: the first chapter presents findings on the total level of card fraud. The second chapter looks at card fraud for different card functions and is followed by a chapter on CNP fraud. Next is an analysis of different categories of card fraud at ATMs and POS terminals. Chapter 5 compares domestic transactions and fraud figures with cross-border figures both within and outside SEPA. Chapter 6, which is based on EU Member States only, looks at absolute and relative fraud levels, as well as other information about individual EU Member States. Chapter 7 concludes.

¹⁰ From an issuing perspective, some CPSs have split their card data according to the area of use of a card, i.e. the main country of use defined by the issuer upon issuance of a card, while other CPSs have reported data according to the country in which the card issuer is domiciled. This may lead to discrepancies for some countries (e.g. Luxembourg) if card issuers issue cards for areas of use other than their own country.

1 Total level of card fraud

The total value of card fraud using cards issued in SEPA amounted to €1.8 billion in 2016. The total value of card transactions using cards issued in SEPA amounted to €4.38 trillion in 2016.¹¹

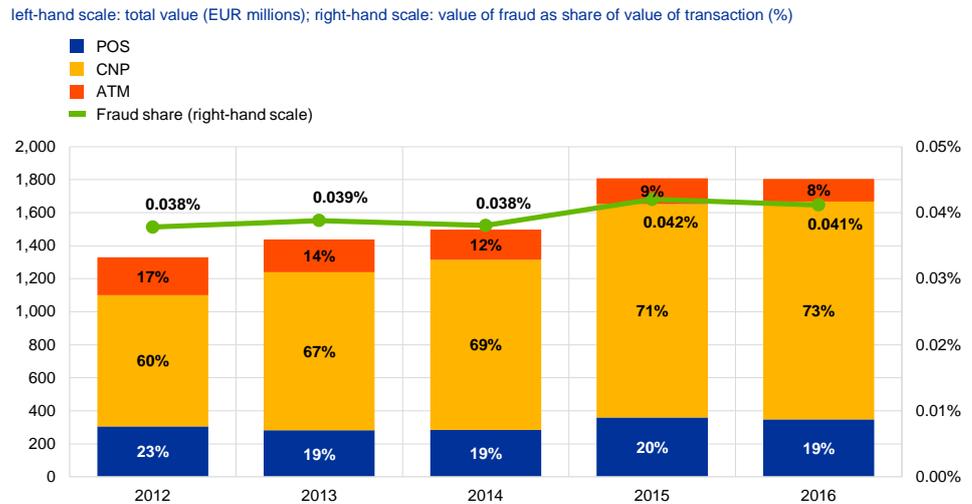
Card fraud experienced a decrease in terms of value of 0.4% compared with 2015, and an increase of 35% compared with 2012. However, since the value of all card transactions grew by 1.8% in 2016 compared with the previous year, fraud as a share of the total value of transactions decreased by 0.001 percentage point, i.e. from 0.042% in 2015 to 0.041% in 2016.¹²

Compared with 2015, CNP fraud has increased in proportion, whereas fraud at ATMs and POS terminals has become less prominent.

CNP accounted for 73%, POS for 19% and ATM for only 8% of the total value of card fraud.

Chart 1a

Evolution of the total value of card fraud using cards issued within SEPA



Source: All reporting CPSs.

The total number of cases of card fraud using cards issued in SEPA amounted to 17.30 million in 2016. The total number of card transactions using cards issued in SEPA amounted to 74.9 billion in 2016.¹³

¹¹ The fraud and transactions value figures cover data from two additional domestic schemes as of 2013 and 2015 respectively. As these schemes do not necessarily report correspondent volumes, this footnote does not apply to Chart 1b.

¹² The growth rates are not influenced by variations in data provision and the baseline fraud amounts used in the calculation of the share come from the same schemes and comparable data.

¹³ In general, volume figures are less accurate than value figures, and some small card schemes do not report them completely. Over time, their quality and completeness has increased; therefore, the percentage of increase over five years is to be treated with caution.

Card fraud increased in terms of volume by 27.2% compared with 2015, and by 92% compared with 2012. In comparison, the total number of transactions increased by only 9.6% in 2016 compared with the previous year. Therefore, fraud as a share of the total number of transactions increased to 0.023% in 2016 (i.e. by 0.003 percentage point compared with the previous year).

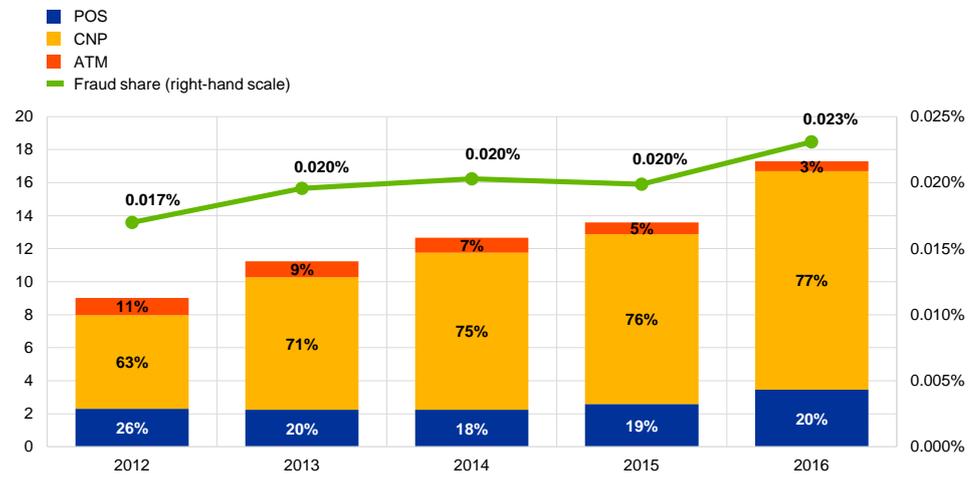
Compared with 2015, the relevance of ATMs as a channel for fraud has decreased when looking at fraud volumes, while the relevance of CNP and POS terminals continues to increase.

The share of ATM fraud in terms of volume was lower than its share in terms of value, owing to the high average values for fraudulent ATM transactions.

Chart 1b

Evolution of the total volume of card fraud using cards issued within SEPA

left-hand scale: total volume (million transactions); right-hand scale: volume of fraud as share of volume of transaction (%)



Source: All reporting CPSs

2 Card fraud according to different card functions

In 2016 the total share of fraud in overall transactions declined slightly for debit cards and increased slightly for delayed debit cards and credit cards compared with the previous year.

The share of delayed debit card and credit card fraud in overall transactions remained larger than that of debit card fraud.

For delayed debit cards and credit cards:

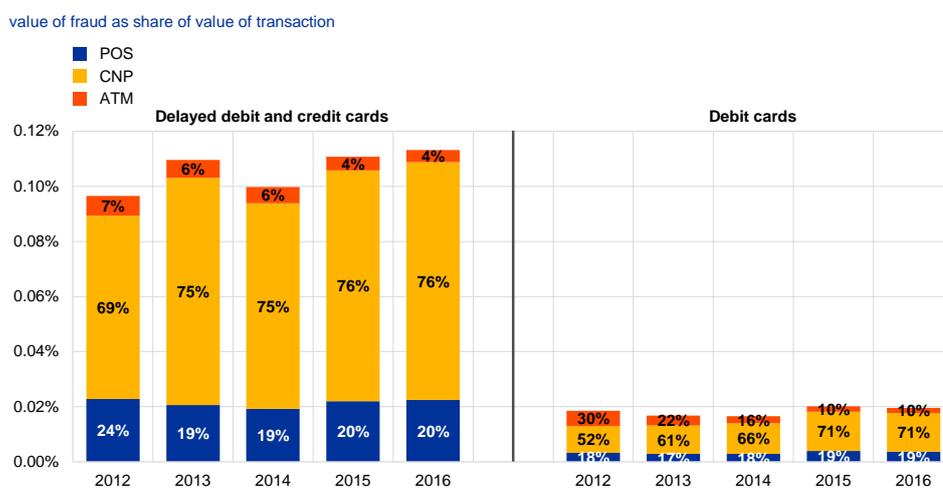
- in absolute terms, fraud increased in 2016 compared with the previous year for the CNP channel and POS terminals, but decreased for ATMs (not displayed in the chart);
- in relative terms (as a percentage of total delayed debit card and credit card transactions), CNP fraud increased in 2016 compared with the previous year, while POS remained constant and ATM fraud decreased.

For debit cards:

- in absolute terms (not displayed in the chart), all components of fraud (CNP, POS and ATM) decreased;
- in relative terms, the share of total fraud in all transactions decreased slightly, owing to the rise of transactions and the fall in fraudulent transactions for this card function.

Chart 2

Share and composition of fraud for different card functions



Source: All reporting CPSs excluding cards issued in France and Spain.

3 Card-not-present fraud

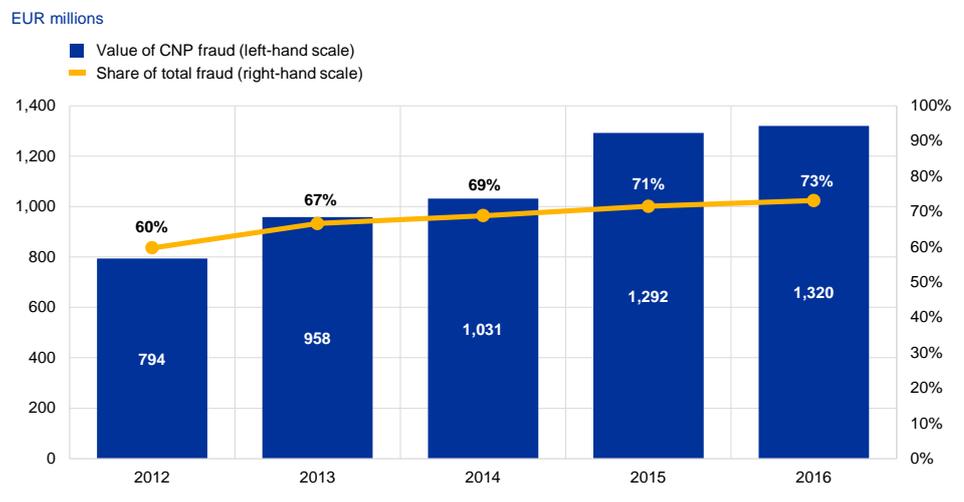
In 2016 the total value of CNP fraud increased by 2.1% compared with the previous year, reaching €1.32 billion.

CNP fraud accounted for 73% of the total value of card fraud in 2016. This share has been growing steadily since 2008 (not displayed in the chart).

An increase in CNP fraud of 66% over a period of five years was the main driver for the 35% increase in overall fraud over this period.

Chart 3

Evolution of the value of CNP fraud and its share of the total value of fraud



Source: All reporting CPSs.

Box 1

Some market perspectives on online card fraud

Card-not-present (CNP) fraud, which nowadays covers mainly “online fraud”, has become the most prominent type of card fraud, amounting to 73% of total card fraud losses in 2016.

Given this development, the ECB conducted a limited survey with market representatives (card schemes, banking associations and merchant/e-commerce associations) from the Card Fraud Prevention Forum of the European Payments Council on fraud modus operandi and prevention.

When asked to specify the top three types/modus operandi of online card fraud observed in its market in 2016, a merchant association provided the following classification:

- 1. Clean fraud** – where criminals obtain genuine cardholder details including 3D Secure and Address Verification credentials, etc. It is almost impossible for merchants to recognise that the individual using the card fraudulently is not the *bona fide* cardholder.

2. Identity theft – where the fraudster makes use of the cardholder’s personal data in order to make an unauthorised transaction. This fraud can also be categorised as “lost or stolen” fraud since customer card details are stolen and used to purchase goods and services online for the purpose of resale, for example. This type of fraud partly overlaps with clean fraud.

3. Friendly fraud or first-party fraud – where the payer, after having performed a genuine transaction to purchase goods or services online, contacts the card issuer to claim that they have been defrauded and request a chargeback. This type of fraud has reportedly been growing in recent years.

According to the security laboratory of one banking association, the increase in digital banking services had inevitably led to a shift of attacks and fraud towards the “card-not-present” type. In instances of CNP fraud, cards were both the target and the vector of the attacks, given that fraudsters aimed first to subtract data and then to spend money online (preferably at online merchants that had not adopted the highest security measures). For them, phishing had turned out to be the most relevant, widespread and effective means of gathering sensitive payment card data. In addition, another banking association remarked that online card fraud in its market was mainly related to credit cards, whereas the debit card part was negligible. This was mainly due to card issuers in these markets blocking the use of debit cards in an online e-commerce environment.

In the same context, one card scheme remarked upon the noticeable continued growth in “unsecured e-commerce transactions” (i.e. transactions without strong customer authentication) and consequently in related fraud. The scheme also mentioned that the increased digitisation of merchant payments was changing CNP risk dynamics.

When it came to fraud prevention, the surveyed respondents made reference to detection systems implemented by card issuers and merchants. In particular, tools such as Tokenization and 3D Secure authentication, particularly when used as part of a risk-based authentication process, had been helpful in reducing online fraud. Predictive measures based on neural systems also represented an effective security tool, in some cases more than other reactive solutions.

In one market, an incremental shift from card-based payments towards credit transfer payments initiated by a third-party provider had lowered fraud rates on payments.

In addition to 3D Secure and strong customer authentication more generally, the following **security tools** were mentioned from a merchant perspective as the most effective for detecting and preventing e-commerce fraud:

- Card Verification Code (CVV, CVN, CVC2, CID, etc.)
- Address verification service (AVS)
- Negative/black lists – including those provided by the international card schemes as well as internal lists within the organisation/merchant
- Fraud scoring models
- Geo-location
- Customer purchase history

- Device fingerprinting
- Email verification

With respect to the expected main threats to card payment security in the future, the surveyed entities mentioned a potential shift towards attacks against mobile payments, owing to an increase in the use of mobile services. The use of social engineering to obtain sensitive payment data relating to credit or debit cards was seen as an ongoing problem.

One respondent made a more detailed distinction between internal and external weakness:

Internal weaknesses included a lack of resources within organisations, especially personnel with the relevant expertise in fraud detection and prevention (seen as a key issue), gaps in fraud tool functionality and issues related to the speed of response to emerging threats and tracking friendly fraud.

Externally, threats could come from data compromises, such as data hacks on merchant client systems, system compromises etc., which continue to concern merchants. A potential risk that the detailed regulatory regime might limit the industry's ability to adjust to new threats was also mentioned by one card scheme in this context.

Finally, as to whether a reduction in online card fraud could be expected in the near future, some respondents either already saw a decrease in online fraud figures or expected it to happen as a result of increased security measures. However, a note of caution was sounded by the market regarding the ever-evolving nature of fraud and the resulting expected shift to other fraud methods.

4 Categories of fraud committed at ATMs and POS terminals

The combined value of ATM and POS fraud decreased by 5.9% in 2016, and the values of both ATM and POS fraud also decreased individually.

The decrease in ATM fraud values – down by 12.4% in 2016 – was more pronounced than for POS and was driven by considerably lower losses on counterfeit and lost and stolen card fraud in absolute values in 2016 compared with 2015.

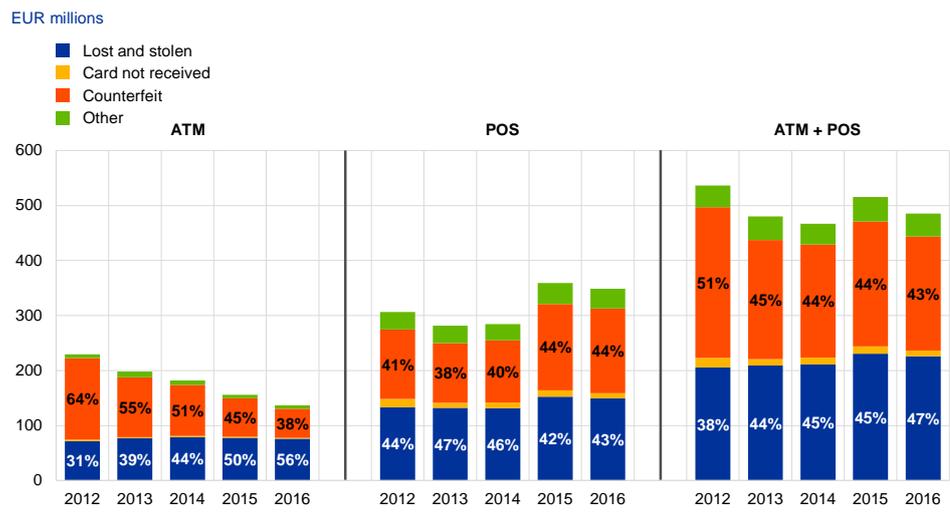
At POS terminals, a 21.5% decrease in card-not-received fraud losses and a 1.9% decrease in counterfeit and lost and stolen card fraud in 2016 contributed to the overall decrease of POS fraud by 3.0%.

From 2015, fraud using lost and stolen cards became the most onerous type of ATM fraud, followed by fraud using counterfeit cards. At POS terminals, counterfeit card fraud and fraud using lost and stolen cards were the most relevant categories in 2016.

Over the five years in question the value of counterfeit card fraud at ATMs and POS terminals combined decreased by 24.4%, while card-not-received fraud decreased by 39.1% (albeit from a comparatively low level). Over the same period, lost and stolen card fraud increased by 9.9% and became, starting from 2014, the most prominent category of card-present fraud in absolute value.

Chart 4

Evolution of the value of fraud by category at ATMs and POS terminals



Source: All reporting CPSs.

As in previous years, counterfeit card fraud in 2016 mostly involved transactions acquired outside SEPA.

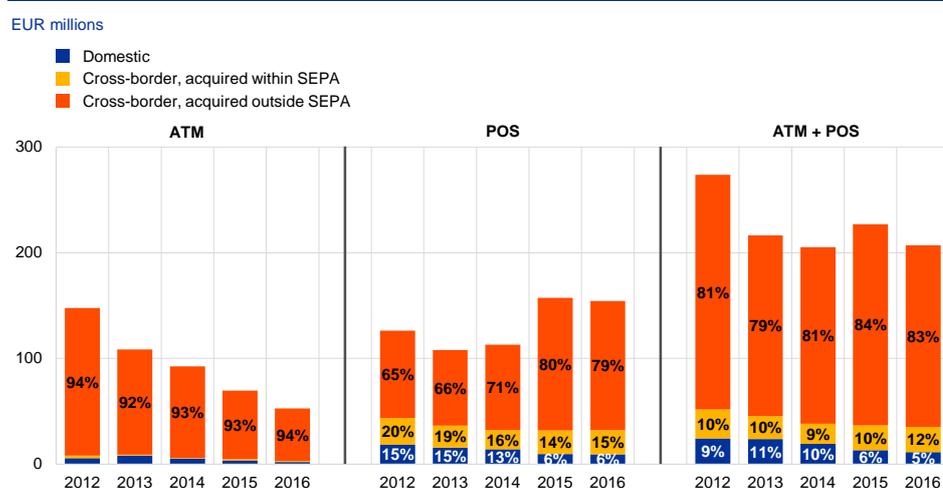
94% of ATM counterfeit card fraud and 79% of POS counterfeit card fraud concerned transactions acquired outside SEPA.

The total value of counterfeit card fraud decreased by 8.8% in 2016.

In 2016 two geographical categories saw decreases in counterfeit card fraud compared with the previous year, namely domestic counterfeit card fraud (by 13.85%) and to a smaller extent cross-border counterfeit card fraud acquired outside SEPA (by 9.76%). The latter was most likely due to the fact that migration to the EMV security standard was still ongoing in countries outside SEPA.

Chart 5

Evolution of the value of counterfeit card fraud at ATMs and POS terminals



Source: All reporting CPSs.

Box 2

Some market perspectives on card-present fraud

Card-present fraud decreased substantially between 2012 and 2016, falling by 9.5%. EMV migration in Europe reached 84.9% in 2016 with respect to the deployment of EMV-chip cards, according to statistics published by EMVCo¹⁴. Even outside SEPA, there has been great progress in this respect, with adoption rates exceeding 50% in the majority of geographical areas in 2016.

When asked to specify the top three types/modus operandi of card-present fraud observed in their market in 2016, representatives of the Card Fraud Prevention Forum (see Box 1) mentioned:

1. **Counterfeit card fraud** – performed by cloning the magnetic stripe of a card, particularly to spend money outside SEPA in countries where EMV standards have not yet been implemented.
2. **Lost and stolen card fraud** – primarily lost cards being used to perform unauthorised card transactions. Theft of physical cards had also been noticed but to a lesser extent than lost card fraud.

¹⁴ <https://www.emvco.com/about/deployment-statistics/>

3. **Identity theft/takeover** – as described in Box 1, fraudsters impersonate the genuine cardholder and make use of their personal information to carry out unauthorised card-present transactions (e.g. at a POS terminal). This category of fraud may overlap with other categories such as counterfeit card fraud or lost and stolen card fraud.

One representative of a merchant association also mentioned that there had been a slight increase in fraud in relation to contactless card transactions using stolen cards; however this remained quite low in absolute terms given the need for the cardholder to key in a PIN after a number of contactless transactions or when exceeding a certain cumulative threshold.

On the question of whether counterfeit card fraud was still an issue for Europe, the surveyed entities unanimously agreed that it had become an issue of low priority for European transactions. However, given that EMV had not been implemented worldwide and the liability shift was not always in place across European borders, this type of fraud was still a problem.

5 Domestic and cross-border card fraud

From 2012 to 2016, the geographical composition of the value of all transactions was marked by an increase in cross-border transactions within SEPA.

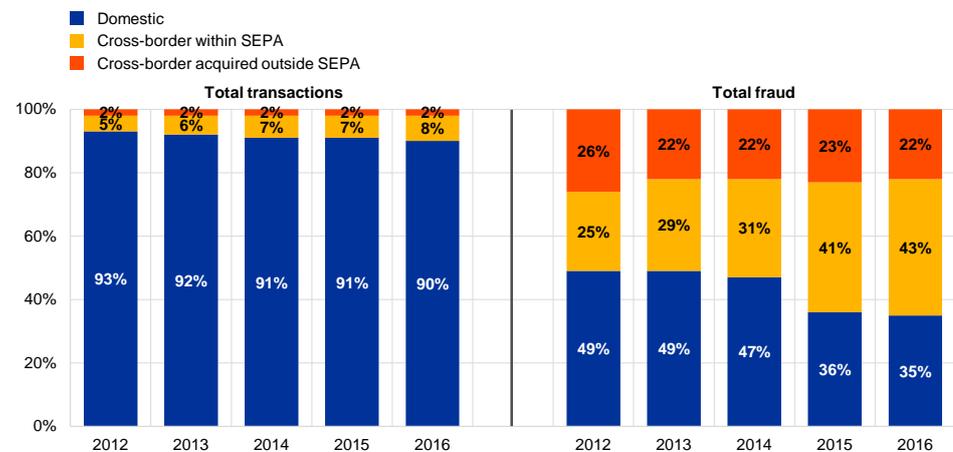
In 2016, domestic transactions accounted for 90% of all transactions, a decrease in the share of transactions but a slight increase (of 1.2%) compared with the previous year. Cross-border transactions within SEPA, on the other hand, went up by 10.16% in 2016 compared with the previous year.

However, cross-border transactions within SEPA accounted for the largest share of fraudulent transactions in 2016 (43%), followed by domestic fraud (35%) and cross-border fraud outside SEPA (22%).

The share of cross-border card fraud within SEPA increased slightly in 2016 compared with the previous year and has been constantly rising since 2012.

Chart 6

Evolution of the value of domestic and cross-border transactions and fraud



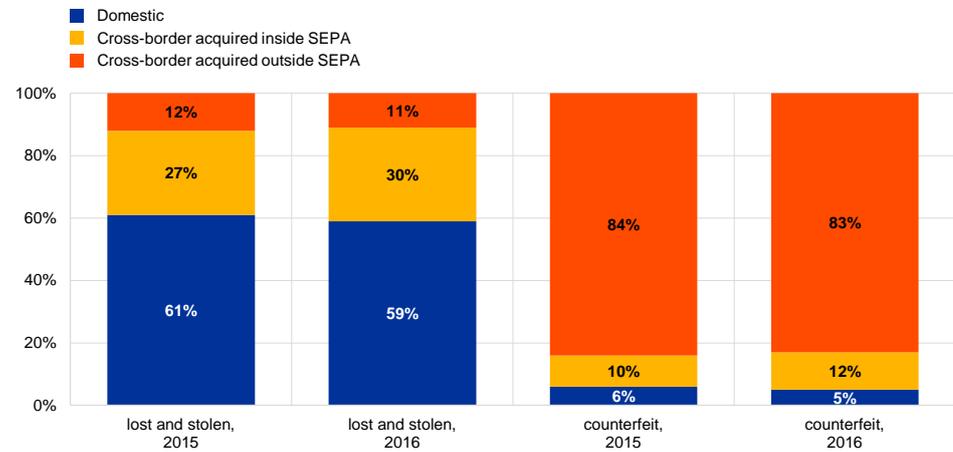
Source: All reporting CPSs.

The geographical composition of card fraud largely depends on the type of fraud:

- lost and stolen card fraud typically takes place at the domestic level, whereas counterfeit card fraud is typically committed outside SEPA;
- for counterfeit card fraud, the proportion of fraud committed outside SEPA decreased in 2016 compared with the year before;
- for lost and stolen card fraud, there was a slight drop in the proportion of domestic fraud at the expense of a rise in cross-border fraud acquired inside SEPA.

Chart 7

Geographical composition of lost and stolen and counterfeit card fraud at ATMs and POS terminals according to fraud value



Source: All CPSs, 2015 and 2016.

In 2016, domestic transactions rose while domestic fraud fell. In the same vein, cross-border transactions acquired outside SEPA increased slightly, whereas the respective fraud decreased.

Cross-border transactions and fraud acquired within SEPA both rose in 2016, with the former increasing at a higher rate than the latter.

Conversely, the number of cross-border transactions within SEPA rose more slowly than the number of those that were fraudulent (not displayed).

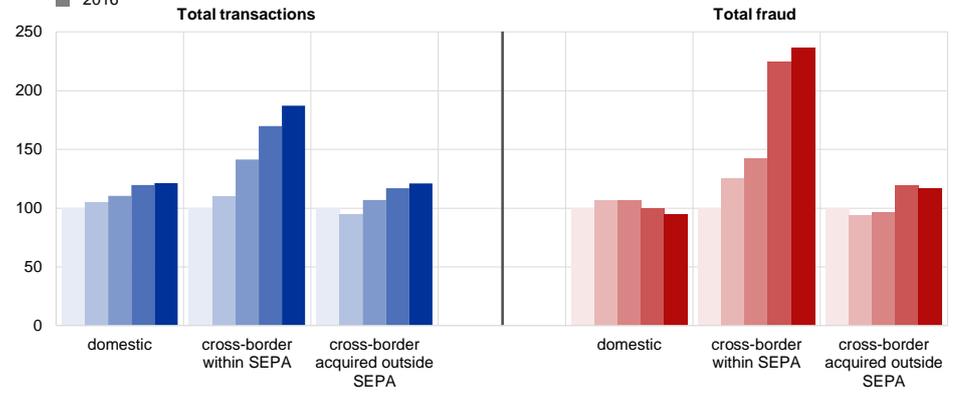
Cross-border fraud within SEPA and outside SEPA both exceeded their 2012 levels, whereas domestic fraud remained under its 2012 level.

Chart 8

Evolution of the total value of domestic and cross-border transactions and fraud

2012 = 100

- 2012
- 2013
- 2014
- 2015
- 2016



Source: All reporting CPSs.

6 A country-by-country perspective on card fraud

Fraud shares varied considerably in different EU Member States in 2016.

From an issuing perspective¹⁵, the rates of fraud in Denmark, the United Kingdom and France were the highest. Fraud rates in Hungary, Romania, Greece, Lithuania, and Poland were the lowest. In the case of Denmark, official statistics on card fraud¹⁶ show that the high levels of fraud in 2016 are mostly due to the high level of cross-border e-commerce fraud, which should be viewed in the light of the large number of e-commerce transactions made in this country in combination with a high share of cross-border transactions more generally. Nevertheless, domestic fraud levels remain low in Denmark.

The euro area in particular experienced lower fraud rates than SEPA as a whole (both from an issuing and an acquiring perspective).

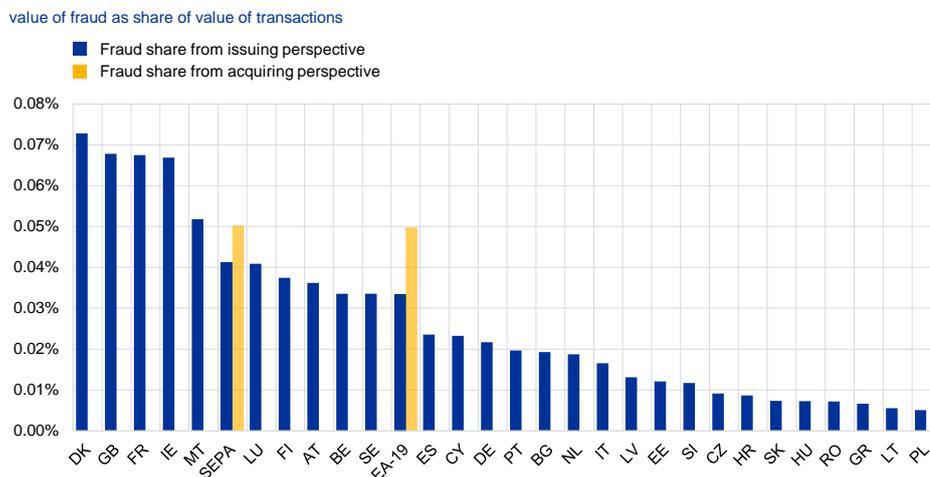
Fraud rates for SEPA (and the euro area) were lower from an issuing perspective than from an acquiring perspective. This indicates that cards issued inside SEPA experienced lower fraud rates for transactions acquired outside SEPA than cards issued outside SEPA for transactions acquired inside SEPA, thus providing a sense of security to European cardholders when shopping abroad.

¹⁵ From an issuing perspective, some CPSs have split their card data according to the area of use of a card, i.e. the main country of use defined by the issuer upon issuance of a card, while other CPSs have reported data according to the country in which the card issuer is domiciled. This may lead to discrepancies for some countries (e.g. Luxembourg) if card issuers issue cards for areas of use other than their own country.

¹⁶ <http://nationalbanken.statbank.dk/nbf/208814>.

Chart 9

Fraud share for transactions with cards issued in a specific country and acquired anywhere (blue) vs fraud share with cards issued anywhere and acquired within the country (yellow)



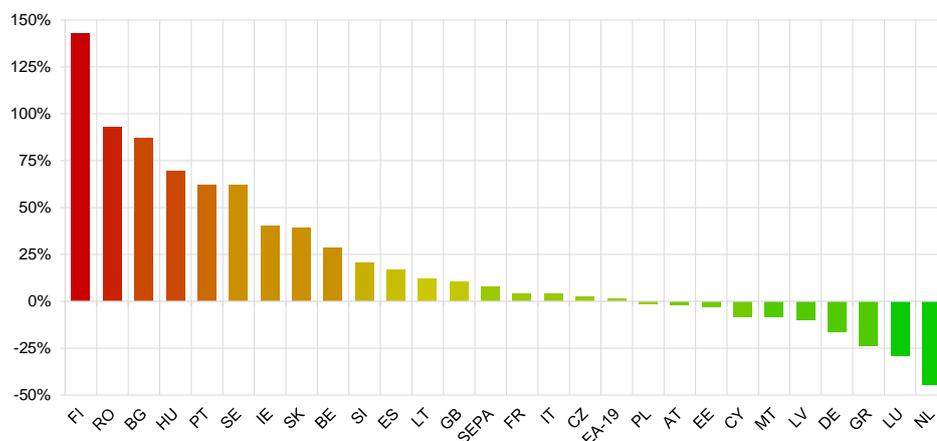
Source: All CPSs, 2016.

Compared with 2012, fraud as a share of the total value of transactions from an issuing perspective has increased for the majority of EU Member States. Thirteen countries have seen larger increases than the average increase of this share recorded in SEPA, which stood at around 7.86%.

Even though the growth rate of fraud as a share of transactions was highest in Finland, this was due to the comparatively low level of its respective fraud share in 2012.

Chart 10

Growth rate of the value of fraud as a percentage of the total value of transactions for cards issued in a specific country¹⁷ or area over five years (2012-2016)



Source: All CPSs.

¹⁷ Croatia is not included in this particular chart since it joined the European Union in 2013. Denmark is also excluded as the 2016 and 2012 data are not comparable for that country.

In general, smaller countries had much higher shares of cross-border transactions than larger countries. Over the five-year period, the picture has not changed much, i.e. a much higher percentage of card transactions take place at domestic level. However, for a few countries the share of cross-border transactions increased substantially over the five-year period in question (e.g. in Malta that share increased from 20% in 2012 to 30% in 2016).

Table 1

Percentage of the value of all transactions taking place domestically or cross-border from an issuing perspective

Country	Domestic	Cross-border	Country	Domestic	Cross-border
GR	97	3	BG	89	11
PT	97	3	GB	88	12
HU	95	5	SI	88	12
HR	95	5	SE	87	13
RO	95	5	EE	87	13
PL	94	6	DK	87	13
IT	94	6	IE	85	15
FR	94	6	BE	84	16
ES	93	7	NL	84	16
CZ	93	7	AT	81	19
DE	92	8	LV	80	20
LT	91	9	CY	74	26
FI	91	9	MT	70	30
SK	90	10	LU	59	41

Source: All CPSs, 2016.

CNP was the main channel for committing fraud using cards issued in all but one country (Portugal).

Main fraud channel by country of issue:

- CNP fraud: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Germany, Finland, France, Greece, Hungary, Ireland, Italy, Lithuania, Luxembourg, Latvia, Malta, Netherlands, Poland, Romania, Spain, Slovakia, Slovenia, Sweden, United Kingdom;
- POS fraud: Portugal¹⁸

There was a large variation in the fraudulent use of each channel for cards issued in different EU countries:

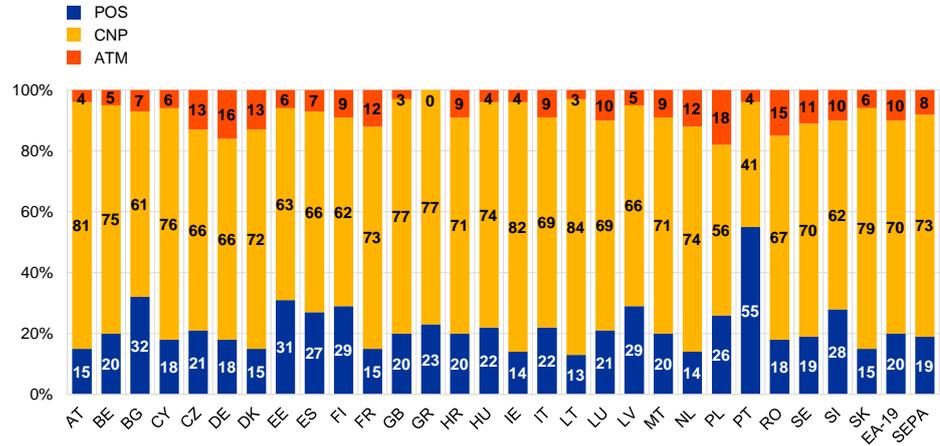
- ATM fraud accounted for between 0% and 18%, with a median share of 8%
- CNP fraud accounted for between 41% and 84%, with a median share of 71%

¹⁸ The high percentage of POS fraud in Portugal is due to a very onerous cross-border case of POS counterfeit fraud outside SEPA reported by one payment scheme.

- POS fraud accounted for between 13% and 55%, with a median share of 20%

Chart 11

Geographical distribution of the value of card fraud by transaction channel from an issuing perspective



Source: All CPSs, 2016.

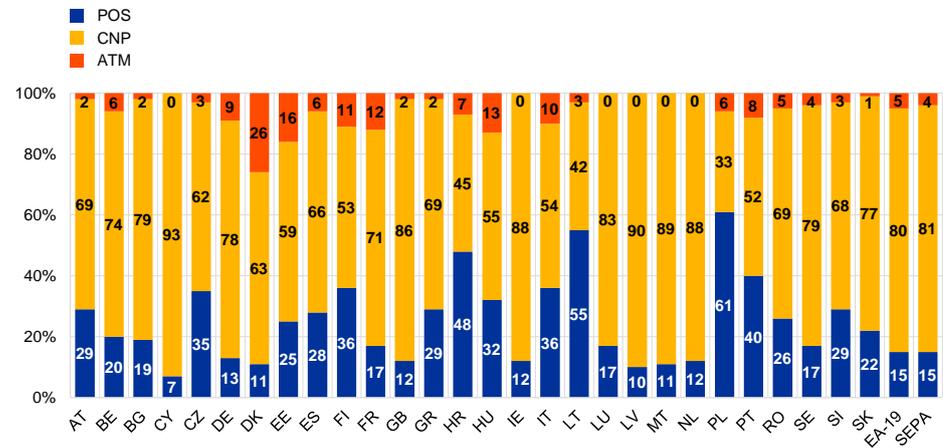
There was a large variation in the transaction channel used to commit fraud in different EU countries:

- ATM fraud accounted for between 0% and 26%, with a median share of 4%
- CNP fraud accounted for between 33% and 93%, with a median share of 69%
- POS fraud accounted for between 7% and 61%, with a median share of 24%

Variations in the fraudulent use of each channel were more pronounced from an acquiring perspective than from an issuing perspective.

Chart 12

Geographical distribution of the value of fraud using cards issued worldwide by transaction channel from an acquiring perspective



Source: All CPSs, 2016.

There were large variations in card use and fraud levels across EU countries.

Most of the significant card markets, which are characterised by high transaction values per inhabitant (for example, France and the United Kingdom) experienced high fraud rates. Fraud in these markets was predominantly CNP fraud (see Chart 11) and mostly occurred on cross-border transactions.

In countries where card use was rather low, e.g. Greece, Lithuania and Poland, fraud shares were typically also low.

Countries are listed according to fraud as a share of the total value of transactions.

The cell colour helps with the interpretation of the associated values:

- green is associated with high card usage or low levels of fraud;
- red is associated with low card usage or high levels of fraud;
- darker colours indicate more extreme values;
- each column in Table 2 is formatted independently.

Table 2

Card use, transaction and fraud levels from an issuing perspective

Country	Cards / inhabitant	Transactions / card		Transactions / inhabitant		Fraud / transaction		Fraud / 1,000 cards		Fraud / 1,000 inhabitants	
		Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume
DK	1.69	7,258	195	12,285	329	0.073%	0.021%	5,709	34	9,663	57
GB	2.49	6,691	117	16,678	291	0.068%	0.035%	4,365	39	10,880	98
FR	1.18	6,818	139	8,043	164	0.067%	0.043%	5,368	69	6,332	81
IE	1.52	6,099	93	9,298	141	0.067%	0.035%	6,328	47	9,648	71
MT	1.95	3,569	42	6,955	83	0.052%	0.040%	1,585	14	3,090	28
LU	3.93	4,539	54	17,832	212	0.041%	0.019%	1,523	9	5,983	36
FI	1.75	5,225	138	9,163	242	0.037%	0.010%	2,238	18	3,926	31
AT	1.53	6,079	65	9,280	100	0.036%	0.014%	1,513	8	2,311	13
BE	1.99	5,666	88	11,294	175	0.034%	0.015%	1,623	12	3,236	25
SE	2.12	5,685	142	12,045	300	0.034%	0.009%	1,938	14	4,106	31
ES	1.61	3,223	53	5,193	86	0.024%	0.022%	806	13	1,298	20
CY	1.32	3,583	26	4,740	34	0.023%	0.017%	1,319	11	1,746	14
DE	1.73	4,220	40	7,293	70	0.022%	0.014%	1,003	6	1,733	11
PT	1.99	4,777	75	9,514	150	0.020%	0.014%	987	15	1,966	29
BG	1.05	1,735	25	1,816	26	0.019%	0.010%	377	3	394	3
NL	2.20	4,560	113	10,030	250	0.019%	0.004%	812	5	1,786	11
IT	1.28	4,781	47	6,131	60	0.017%	0.013%	943	7	1,209	9
LV	1.21	3,996	118	4,823	143	0.013%	0.004%	560	6	676	7
EE	1.40	4,697	171	6,552	239	0.012%	0.003%	615	5	857	8
SI	1.62	3,192	63	5,162	102	0.012%	0.007%	356	4	576	7
CZ	1.14	3,590	74	4,086	84	0.009%	0.006%	331	4	377	5
HR	2.08	1,862	39	3,866	81	0.009%	0.003%	171	2	354	3
SK	1.03	3,826	73	3,937	75	0.007%	0.006%	287	4	296	4
HU	0.91	3,716	68	3,394	62	0.007%	0.003%	285	3	260	2
RO	0.81	2,655	34	2,142	28	0.007%	0.005%	207	2	167	2
GR	1.36	3,947	35	5,367	47	0.007%	0.010%	254	4	345	5
LT	1.20	3,721	87	4,459	104	0.006%	0.003%	203	2	243	3
PL	0.96	3,303	106	3,169	102	0.005%	0.002%	173	2	166	2
EA-19	1.53	4,733	72	7,236	109	0.033%	0.022%	1,712	18	2,616	28
SEPA	1.53	4,993	84	7,646	129	0.041%	0.023%	2,245	22	3,437	33

Sources: Data on cards, inhabitants, transactions per card and transactions per inhabitant were drawn from the ECB's SDW; data on fraud and fraud per transaction were collected for oversight purposes by all CPSs for 2016. Therefore, the fraud/transaction indicator is constructed from data coming from the same source.

Note: Values are in euro.

Table 3 reports fraud levels and changes in fraud levels in 2016 at country level in total and for selected types of fraud.

Developments in, and levels of, fraud differed significantly across different countries.

Although issuers and card schemes managed to reduce fraud in some countries with relatively high fraud rates, such as Denmark, the United Kingdom, France and Luxembourg, they experienced further growth in other markets, such as Ireland.

Similarly, among countries with low fraud shares, some, such as Poland and Slovakia, experienced a further reduction in fraud, while others, such as Hungary, experienced major growth.

The cell colour helps with the interpretation of the associated values:

- green is associated with low fraud shares or reductions in fraud shares;
- red is associated with high fraud shares or increases in fraud shares;
- darker colours indicate more extreme values.

Fraud shares and growth rates for individual fraud categories are jointly formatted in Table 3 to allow the comparison of different types of fraud.

Table 3

Relative fraud levels and trends per channel and category from an issuing perspective

Issuer location	Value of fraud as share of value of transactions	Change from 2015	ATM			POS			CNP			
			Value of lost+ stolen as share of all transactions	Change from 2015	Value of counterfeit as share of all transactions	Change from 2015	Value of lost+ stolen as share of all transactions	Change from 2015	Value of counterfeit as share of all transactions	Change from 2015	Value of CNP fraud as share of all transactions	Change from 2015
DK	0.00073	-4%	0.000081	196%	0.000015	-54%	0.000033	-56%	0.000078	-33%	0.000521	3%
GB	0.00068	-2%	0.000006	3%	0.000012	-27%	0.000064	13%	0.000038	-9%	0.000521	-2%
FR	0.00067 ¹⁾	-7%	0.000059	-17%	0.000018	-40%	0.000078	-16%	0.000036	-12%	0.000479	-1%
IE	0.00067	23%	0.000005	-23%	0.000019	-22%	0.000017	-6%	0.000075	45%	0.000548	25%
MT	0.00052	4%	0.000010	-3%	0.000035	7%	0.000006	109%	0.000072	-48%	0.000370	32%
LU	0.00041	-23%	0.000011	23%	0.000029	-8%	0.000005	-33%	0.000081	-43%	0.000282	-17%
FI	0.00037	34%	0.000012	8%	0.000022	8%	0.000038	214%	0.000066	38%	0.000233	29%
AT	0.00036	12%	0.000001	23%	0.000012	-25%	0.000016	6%	0.000037	33%	0.000294	12%
BE	0.00034	43%	0.000004	-51%	0.000010	2%	0.000008	35%	0.000060	37%	0.000253	52%
SE	0.00034	4%	0.000012	-19%	0.000024	20%	0.000016	-10%	0.000040	-6%	0.000233	9%
ES	0.00024	-4%	0.000010	1%	0.000006	-50%	0.000023	15%	0.000035	-8%	0.000157	1%
CY	0.00023	48%	0.000000	NA	0.000012	42%	0.000006	65%	0.000035	-5%	0.000177	68%
DE	0.00022	-9%	0.000021	1%	0.000011	-16%	0.000011	-4%	0.000027	-7%	0.000144	-10%
PT	0.00020	44%	0.000002	-4%	0.000006	9%	0.000003	-13%	0.000102	556% ²⁾	0.000081	-24%
BG	0.00019	79%	0.000000	-72%	0.000013	142%	0.000001	215%	0.000060	146%	0.000118	54%
NL	0.00019	15%	0.000006	-38%	0.000013	-14%	0.000005	-16%	0.000015	-19%	0.000138	32%
IT	0.00017	-11%	0.000009	-23%	0.000005	-29%	0.000014	-19%	0.000020	-21%	0.000114	-4%
LV	0.00013	1%	0.000000	NA	0.000007	-53%	0.000002	17%	0.000036	-19%	0.000086	25%
EE	0.00012	-19%	0.000000	-93%	0.000007	-54%	0.000000	-57%	0.000034	-42%	0.000076	12%
SI	0.00012	-18%	0.000001	173%	0.000011	39%	0.000002	-43%	0.000029	-31%	0.000072	-17%
CZ	0.00009	9%	0.000001	-22%	0.000010	-35%	0.000002	-19%	0.000015	-27%	0.000061	45%
HR	0.00009	-11%	0.000004	-27%	0.000004	-15%	0.000006	-39%	0.000009	-50%	0.000062	9%
SK	0.00007	-13%	0.000000	-76%	0.000004	-22%	0.000001	-68%	0.000009	-69%	0.000058	24%
HU	0.00007	52%	0.000001	-2%	0.000002	-39%	0.000001	61%	0.000015	28%	0.000054	73%
RO	0.00007	3%	0.000000	-77%	0.000011	76%	0.000000	-13%	0.000012	-57%	0.000048	36%
GR	0.00007	6%	0.000000	-68%	0.000000	-34%	0.000003	-62%	0.000012	-21%	0.000051	34%
LT	0.00006	8%	0.000000	NA	0.000002	-11%	0.000000	-92%	0.000007	-11%	0.000046	14%
PL	0.00005	-5%	0.000002	-2%	0.000007	-40%	0.000003	49%	0.000010	-27%	0.000028	23%
EA-19	0.00033	-1%	0.000022	-12%	0.000011	-28%	0.000028	-9%	0.000034	5%	0.000233	3%
SEPA	0.00041	-2%	0.000017	-4%	0.000012	-26%	0.000034	-4%	0.000035	-4%	0.000301	0%

Source: All reporting CPSs, 2015 and 2016.

1) The fraud rate deducted from data collected using Eurosystem methodology differs from the fraud rate according to the Banque de France's data collection (0.00064 according to data from www.banque-france.fr) owing to potential reporting inconsistencies or methodological divergence with respect to the collection of data on cross-border transactions and fraudulent transactions.

2) This percentage of increase for Portugal is due to a very onerous cross-border case of POS counterfeit fraud outside SEPA reported by one payment scheme in 2016.

7 Conclusions

This report shows that the total value of card fraud decreased in 2016 compared with the previous year. The overall decrease of 0.4% was due to a decrease in fraud using the ATM and POS transaction channels, which outweighed a slight increase in CNP fraud.

CNP fraud went up by 2.1%, accounting for 73% of all fraud losses on cards issued inside SEPA. Data on total CNP transactions, which unfortunately are only partially available, suggest that fraud has grown at a slower rate than transactions. Enhanced security standards for payment service providers and card schemes issued by the EBA and the Eurosystem at the end of 2014 and beginning of 2015 seem to have led to early signs of improvement in fraud rates in the EU. The banking associations and card schemes have already noted a positive shift with respect to online fraud and believe that this type of fraud should go down in the near future.

As to the card-present environment, the lower rate of ATM and POS fraud was mainly a result of a decrease in card-not-received and counterfeit fraud levels and, from a geographical point of view, decreases in domestic fraudulent transactions. Cross-border card-present fraud – in particular counterfeit card fraud – acquired outside SEPA also decreased, while countries outside SEPA made substantial progress in migrating to EMV. However, as magnetic stripe usage in such countries cannot be completely avoided, card schemes and issuers are encouraged to adopt further measures to prevent counterfeit fraud and to improve the protection of their customers.

As in previous years, this report shows that levels of fraud were lower in the euro area than in SEPA as a whole. Data on fraud and transactions using cards issued inside and outside SEPA show that fraud losses incurred outside SEPA on cards issued inside SEPA were lower than losses incurred inside SEPA on cards issued outside SEPA. The finding suggests that SEPA residents benefit from the high security features of their cards, even though the proportion of ATMs and POS terminals outside SEPA making use of enhanced security features is still small.

Although fraud seems to have decreased slightly in 2016, the Eurosystem will keep on monitoring developments within SEPA. As mentioned by market participants, fraud has a tendency to shift from one channel to another, from one instrument to another, and evolve towards new modus operandi. Regulators and overseers should therefore remain vigilant and monitor security developments in order to take prompt action if needed.

© **European Central Bank, 2018**

Postal address 60640 Frankfurt am Main, Germany

Telephone +49 69 1344 0

Website www.ecb.europa.eu

All rights reserved. Reproduction for educational and non-commercial purposes is permitted provided that the source is acknowledged.

For specific terminology please refer to the [ECB glossary](#).

PDF	ISBN 978-92-899-3192-2,	ISSN 2315-0033,	doi:10.2866/333885,	QB-BI-18-001-EN-N
HTML	ISBN 978-92-899-3647-7,	ISSN 2315-0033,	doi:10.2866/450506,	QB-BI-18-001-EN-Q