The Future of U.S. Fraud in a Post-EMV Environment

Douglas King

Retail Payments Risk Forum Working Paper
Federal Reserve Bank of Atlanta
June 2019

ABSTRACT

Having begun in earnest in 2015, the U.S. payments card industry is now, in 2019, approaching full adoption of EMV chip cards. The United States' efforts have lagged those of many other developed countries in adopting EMV. This paper explores data from three of these countries (the United Kingdom, France, and Australia) to extrapolate fraud trends we could see develop in the United States. Considering these trends and the current state of U.S. fraud, the paper looks at what the future might hold for fraud in the United States in a post-EMV environment.

INTRODUCTION

Since the Atlanta Fed published the paper "Chip-and-PIN: Successes and Challenges in Reducing Fraud" in January 2012 (King 2012), the U.S. payment card industry has taken great steps toward fully adopting chip-based cards based on EMVCo's global specification. Although the adoption process is ongoing, the industry has made great progress since the point-of-sale (POS) liability shift went into effect in October 2015. The majority of general-purpose credit and debit cards issued in the United States today contain a chip, with nearly all (97 percent) of the country's payment value occurring on these cards. Approximately two-thirds of U.S. merchant locations are set up to accept EMV chip-based payment cards (Visa 2018).

The original paper explored fraud trends in several countries, including the United Kingdom, France, and Australia. These countries had fully adopted EMV chip cards or were several years into the adoption process at the time of writing. The paper looked at these countries' experiences and fraud trends and hypothesized what those trends could mean for the future of fraud in the United States. It reported key findings, including that EMV chip cards were highly successful at reducing face-to-face counterfeit card fraud but overall fraud did not see dramatic declines. This lack of significant change in overall fraud was partly because fraudsters exploited card payments that could not involve the chip technology—namely, for purchases made online, in other non-face-to-face environments (mail or telephone orders), or in areas that had not yet adopted chip technology, including the United States.

This current paper updates the findings of the original paper by looking at payments fraud in three of the countries studied in the previous paper: the United Kingdom, France, and Australia.

In evaluating the new data, the paper addresses several questions:

- Has counterfeit card fraud continued to decline in these countries?
- Is card-not-present[1] (CNP) fraud an ongoing concern?
- Has overall card fraud in the three countries started to decline? Are there new payments fraud developments outside of cards in mature EMV markets that might be reason for concern in the United States?

This paper also considers the current state of payments fraud in the United States in light of the card industry's adoption of EMV chip cards and with new data collected by the Federal Reserve System. Keeping in mind the fraud trends in more mature EMV markets as well as the current fraud landscape in the United States, the paper concludes with what could happen with payments fraud in the United States as EMV use matures.

[1] "Card not present," or CNP, is used throughout this paper to describe transactions where a card is not presented at the time of payment. Some of the reports in the countries studied in this paper identify this type of transaction as a remote transaction. Most often, these transactions are made online through a web or mobile browser, but they can also be made through a mobile app, or by mail order or the telephone—these latter are sometimes referred to as *MOTO* transactions.

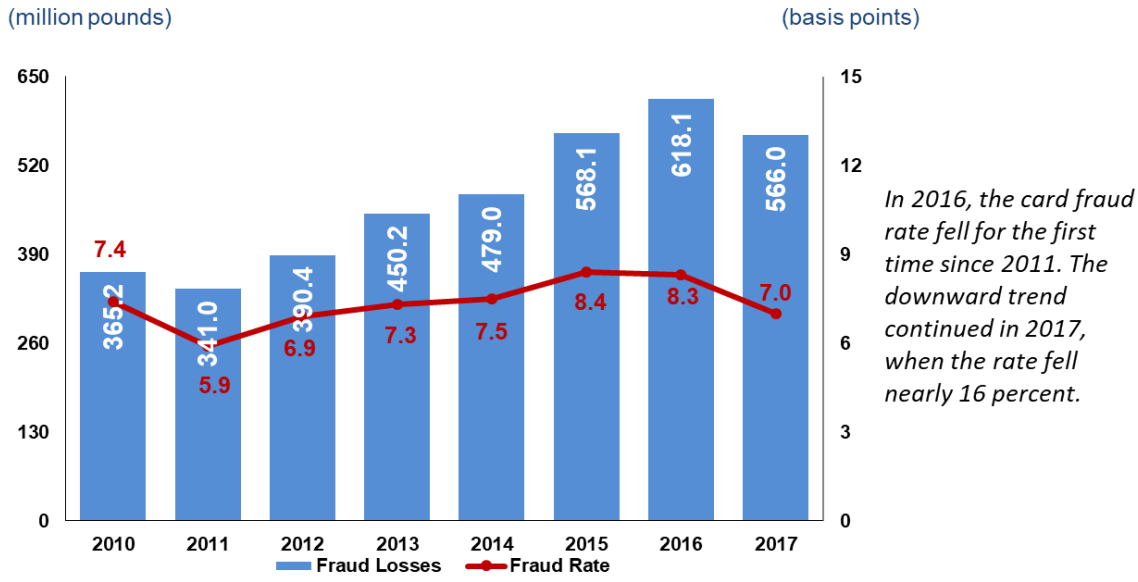
THE UNITED KINGDOM[2]

Total Card Fraud

Card fraud losses as a proportion of the total amount of card spend, also known as the fraud rate, was 7.0 basis points (or £7 for every £10,000 spent) for 2017. This represents an approximately 5 percent decrease from the 2010 fraud rate of 7.4 basis points. After dropping in 2011, the fraud rate steadily increased each year through 2015, reaching 8.4 basis points. The fraud rate then declined in 2016 and again in 2017 (see chart 1). After EMV's initial impact in 2011, when it reduced the card fraud rate, the fraud rate has remained relatively controlled, in the range of 6 to 8 basis points.

On an absolute basis, card fraud has risen since 2010, the last year of data included in the original paper. Even though card fraud declined by 8 percent in 2017, from £618.1 million in 2016 to £566.0 million, the 2017 card fraud amount represents an increase of 55 percent since 2010, when card fraud losses stood at £365.2 million. This rise has been driven specifically by two types of card fraud: CNP and lost or stolen card.

Chart 1: Fraud Losses and Rates on U.K.-Issued Cards



Source: UK Finance 2018

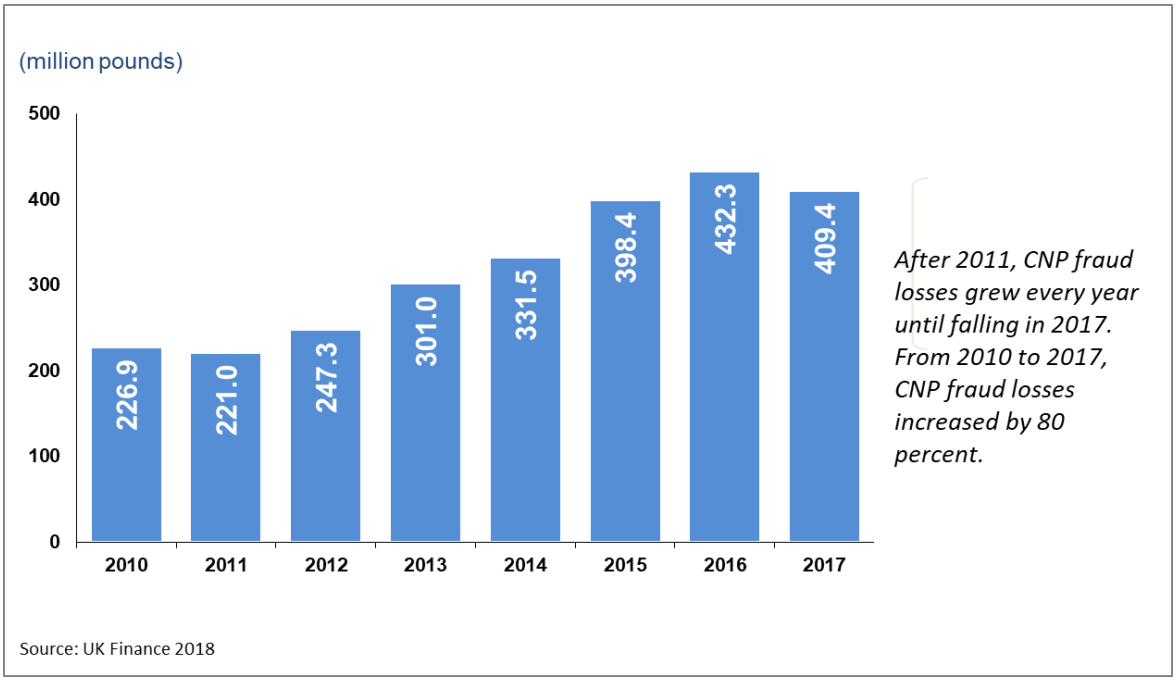
Card-Not-Present Fraud

In 2017, CNP fraud stood at £409.4 million, a significant increase over 2010 CNP fraud (see chart 2). Two factors explain this rise. First, EMV was designed to thwart counterfeit and lost-or-stolen card fraud when implemented with PIN cardholder verification, as was the case in the United Kingdom, so it was natural for fraudsters to shift their attention away from those fraud types and onto CNP fraud. Second, since CNP transaction volumes are rapidly growing, it seems reasonable that absolute fraud would also

[2] All information in this section is based on UK Finance 2018.

grow, even with a flat or more slowly declining fraud rate. However, it appears that there might be positive momentum with regard to CNP fraud. In 2017, CNP fraud declined from the prior year for the first time since 2011, which the Financial Fraud Action UK attributes to the finance industry's "investing in new, innovative security tools to identify suspicious transactions, including even more sophisticated ways of authenticating customers" and "providing fraud screening detection tools for retailers, such as the continued development of 3D Secure technology" (UK Finance 2018, 11).

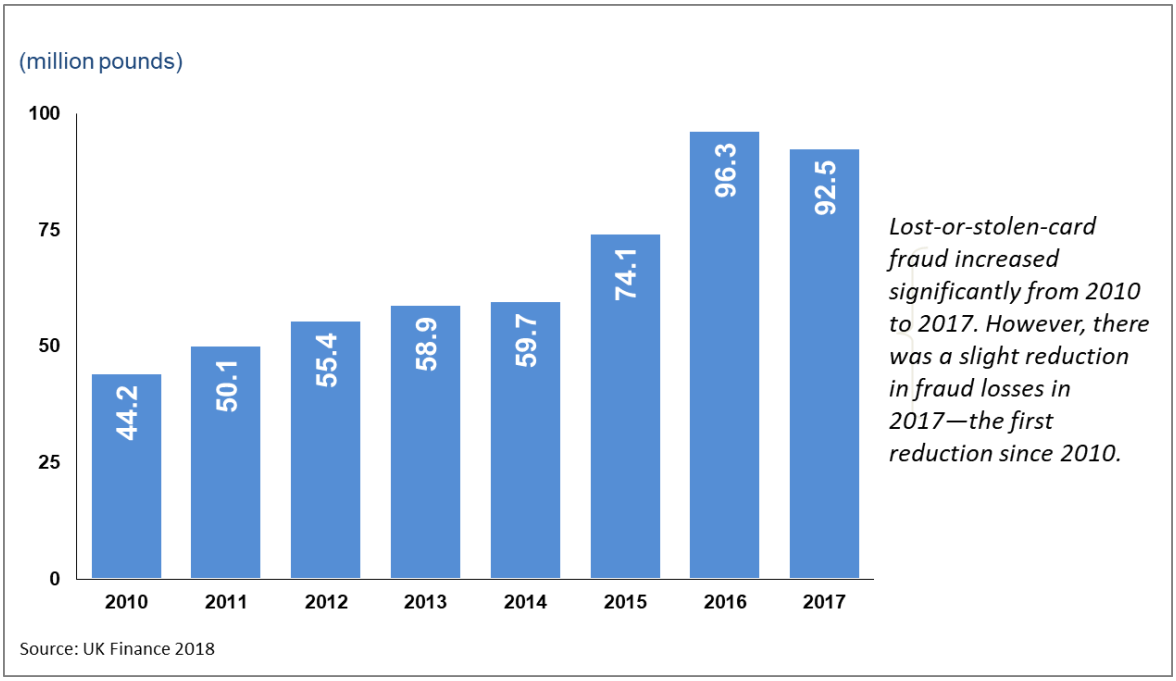
Chart 2: Card-Not-Present Fraud Losses on U.K.-Issued Cards



Face-to-Face Card Fraud

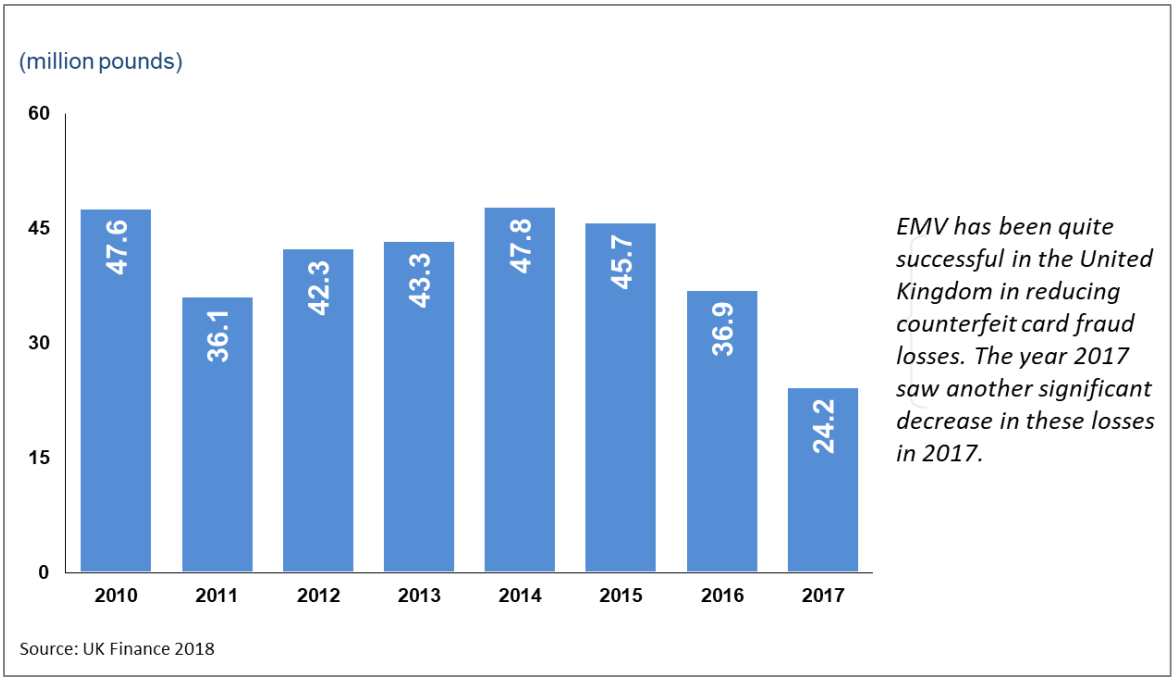
Although lost-or-stolen-card fraud started from a low base of £44.2 million in 2010, it increased every year through 2016 (see chart 3). Like CNP fraud, this type of fraud declined in 2017, though the decline was slight, dropping from £96.3 million to £92.5 million. On an absolute basis, however, lost-or-stolen-card fraud rose nearly 110 percent from 2010. This increase is surprising since the United Kingdom's implementation of EMV included the adoption of PIN verification, which is supposed to prevent lost-or-stolen-card fraud. Even with the increase, however, face-to-face card fraud in the United Kingdom remains low because counterfeit card fraud has been so drastically reduced.

Chart 3: Lost-or-Stolen-Card Fraud Losses on U.K.-Issued Cards



Counterfeit card fraud was greatly reduced as the United Kingdom reached full EMV adoption: fraud values had dropped to £47.6 million by 2010 (see chart 4). After that, counterfeit card fraud remained relatively stable, until it fell again—significantly—in 2016 and 2017, to £24.2 million in 2017. Most of the counterfeit card fraud on U.K.-issued cards occurs with in-person, cross-border transactions. Presumably, as acceptance of EMV cards around the globe and particularly in the United States has increased, opportunities for counterfeit card fraud are decreasing.

Chart 4: Counterfeit Card Fraud Losses on U.K.-Issued Cards



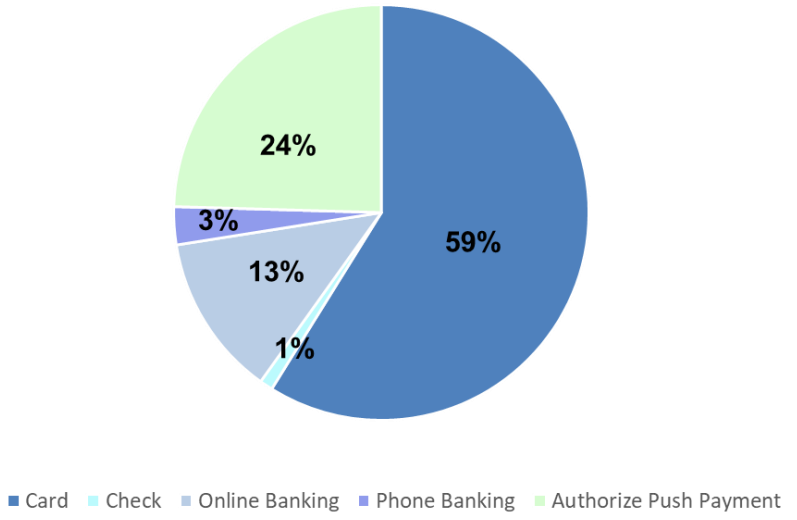
Other Card and Payments Fraud

Chart 5 shows the shares of all payment types in fraud losses. Mail nonreceipt card fraud, which describes cards stolen while in transit, has remained low since 2010. Card ID theft fraud has fluctuated each year since 2010 but fell to £29.9 million in 2017, a 25 percent decline from 2016 and its lowest level since 2011. Card ID theft fraud is defined as either application fraud, whereby someone uses a stolen identity to open a card account, or takeover of a card account.

Beyond payment cards, changes in fraud with other payment instruments and channels have been mixed. Check fraud losses, in decline since 2011, were only £9.8 million in 2017—the lowest value of check fraud ever reported in the United Kingdom. However, during this same period, both online and telephone banking fraud increased. Perhaps these channels are easier targets in light of EMV and other card-authentication measures such as 3D-Secure for CNP transactions. Online banking fraud occurs when a fraudster gains online access to a customer's bank account and makes an unauthorized payment or transfer of money. In 2017, online banking fraud losses stood at £121.4 million, up about 19 percent, or £19.6 million, from the year before and up 137 percent from its low in 2011 of £51.2. Losses from telephone banking fraud were £28.4 million in 2017.

For 2017, UK Finance collected data for a new type of fraud, authorized push payment, which is generally referred to in the United States as business email compromise (BEC) or email account compromise (EAC). Losses from this type of fraud were £236.0 million in 2017, which represented nearly 25 percent of all payment fraud reported in the country. (Chart 5 shows shares of all fraud types tracked in the United Kingdom.)

Chart 5: 2017 Fraud Losses by Payment Type in the United Kingdom



Fraud losses in the United Kingdom are dominated by card fraud, authorized push payment fraud, and online banking fraud. With CNP fraud accounting for 70 percent of the card fraud, it's clear that criminals prefer to exploit digital channels.

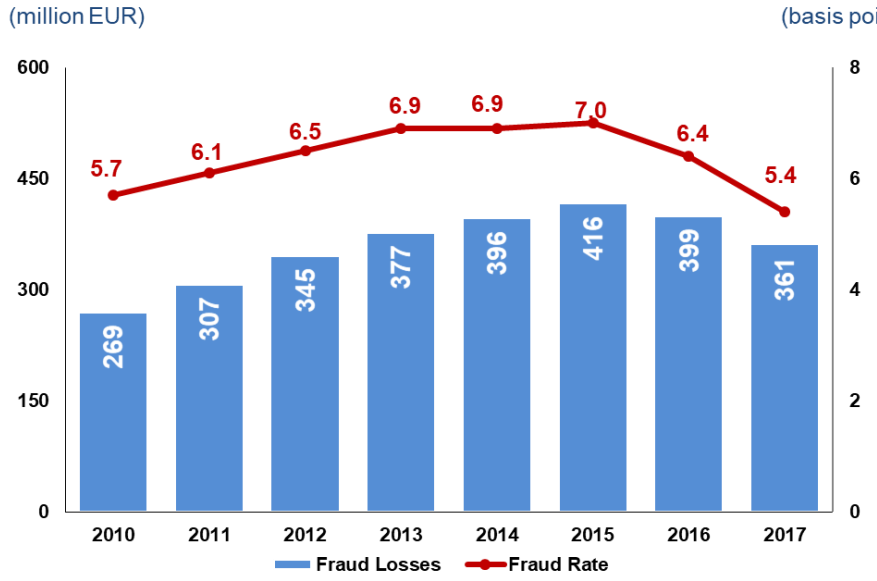
Source: UK Finance 2018

FRANCE[3]

Total Card Fraud

For 2017, the fraud rate for French-issued cards stood at 5.4 basis points, the lowest annual rate of fraud in the period from 2010 to 2017 (see chart 6). The rate steadily increased from 2010 to 2015 before it fell in 2016 and then dropped significantly in 2017. Not only did the fraud rate drop in both years, but absolute fraud figures also declined significantly: nearly 10 percent in 2017. As the next section notes, this decline was due largely to increases in the use of strong customer authentication solutions by both financial institutions and merchants for CNP transactions.

Chart 6: Fraud Losses and Rates on French-Issued Cards



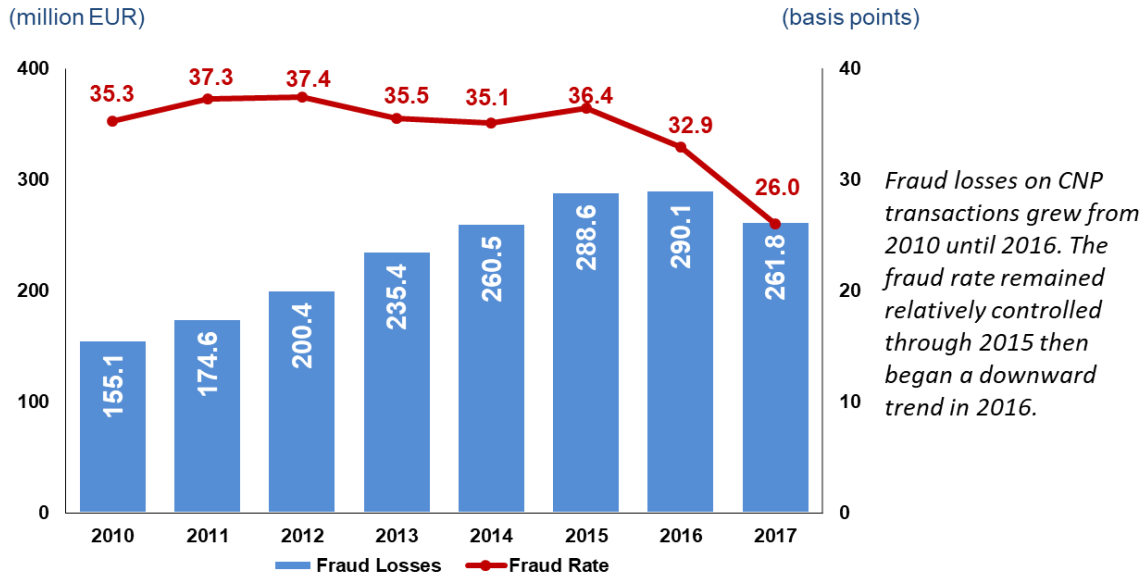
Source: Banque de France 2017

Card-Not-Present Fraud

The overall rise in card fraud losses in France after 2010 and then declines in 2016 and 2017 are highly correlated with CNP fraud losses (see chart 7). In 2016 and 2017, the CNP fraud rate fell sharply, for two reasons: one, 98 percent of French cardholders are receiving what the Observatory for the Security of Payment Means (the Observatory) calls "strong customer authentication solutions" from their financial institutions, and two, 73 percent of French merchants are now supporting 3D-Secure, an authorization protocol providing online authentication. In 2017, 3-D Secure authentication covered 41 percent of CNP payments. These domestic CNP payments have a fraud rate of 6 basis points, which is very similar to the overall card fraud rate in France.

[3] The information in this section is based on Banque de France 2017.

Chart 7: Card-Not-Present Fraud Losses and Rates on French-Issued Cards

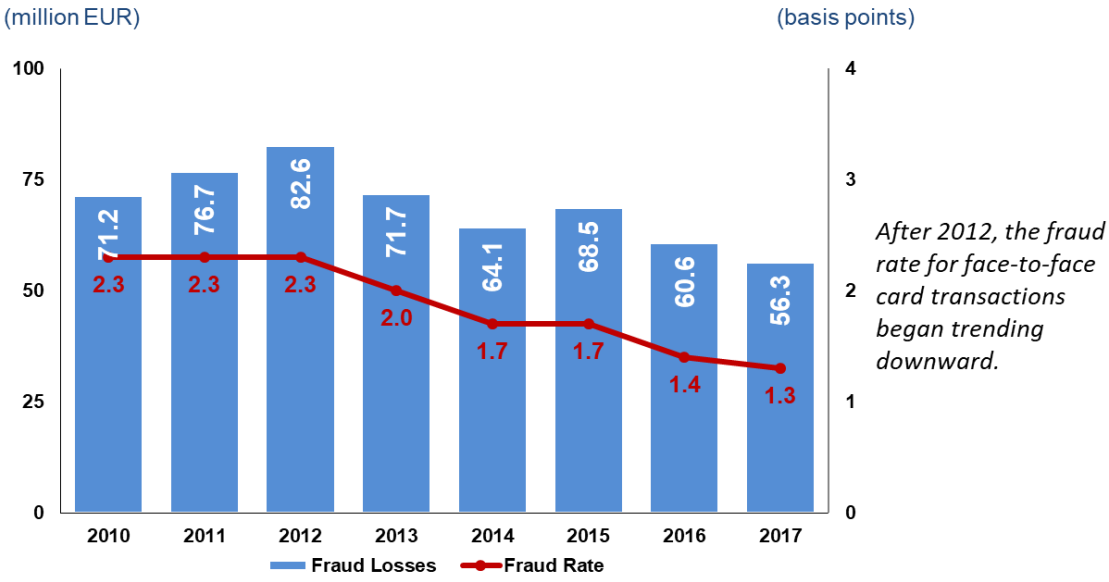


Source: Banque de France 2017, Retail Payments Risk Forum calculations

Face-to-Face Card Fraud

France was an early adopter of chip card technology, implementing chip cards even before the EMV specification release. (Chip cards were first tested in France in the 1980s, and all French banks were issuing them by 1994.) As a result, counterfeit card fraud has been a very small percentage of France's overall card fraud—it was just 1 percent of fraudulent domestic payments in 2017. Because counterfeit card fraud is so low, the Observatory does not report it specifically but rather includes it with other fraud, such as lost-or-stolen card fraud, committed in the face-to-face retail environment. And as to be expected in an EMV card environment, both absolute fraud and the fraud rate for face-to-face transactions are significantly lower than for CNP transactions.

Chart 8: Face-to-Face Fraud Losses and Rates on French-Issued Cards

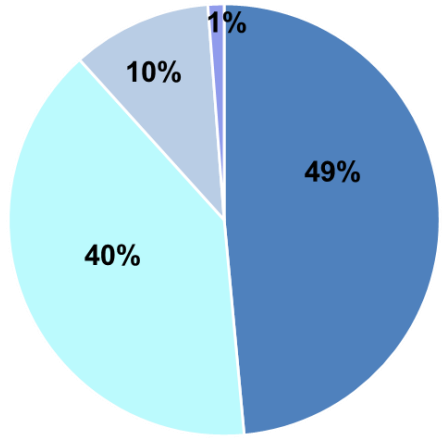


Source: Banque de France 2017, Retail Payments Risk Forum calculations

Other Card and Payments Fraud

Chart 9 shows the shares of all payment types in fraud losses. In 2016, the Observatory began including data on check, credit transfer, and direct debit fraud. (Credit transfers and direct debit are comparable to Automated Clearing House, or ACH, transactions in the United States.) In 2017, checks were second only to cards among targeted payment instruments, accounting for 40 percent of all France's payments fraud. Further, in 2017, checks were the only payment instrument that saw an increase in fraud; check fraud rose 9 percent year over year, to €296 million. Still, the fraud rate on checks for 2017 stood at 2.9 basis points, nearly half the rate for payment cards. Credit transfer fraud, which includes business email compromise, fell by 9 percent in 2017 to €78. Direct debit fraud, at €9, was the lowest.

Chart 9: 2017 Fraud Losses by Payment Type in France



Fraud losses in France are led by card fraud, closely followed by check fraud. Credit transfer fraud, which includes business email compromise schemes, makes up 10 percent of payments fraud in this country.

Card Check Credit Transfer Direct Debit

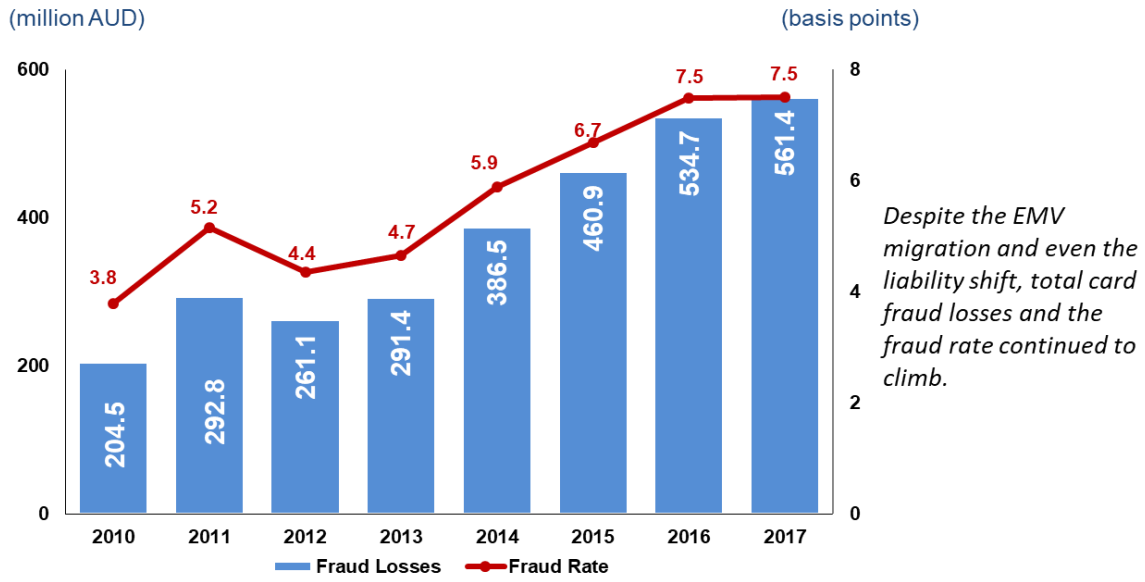
Source: Banque de France 2017

AUSTRALIA[4]

Total Card Fraud

The payment card industry in Australia began migrating to EMV chip cards in early 2008, but fraud liability shifts[5]— used by the global card networks to encourage merchants and issuers to adopt the technology—did not occur until April 2013 and April 2014, depending on each network's rules and regulations. So even though the migration to EMV began much earlier than it did in the United States, the liability shift dates were within a couple of years of the United States' October 2015 shift date. Since the beginning of the EMV migration, both absolute fraud losses and the fraud rate have increased significantly, climbs that continued even after the liability shift dates (see chart 10). Absolute fraud increased from $AUD204 million in 2010 to over $AUD561 million in 2017. For the same time period, the fraud rate for Australian payment cards nearly doubled, rising from 3.8 basis points to 7.5 basis points.

Chart 10: Fraud Losses and Rates on Australian-Issued Cards



Source: Australian Payments Network 2018

Australia's post-EMV migration fraud experience is in some regards similar to the experiences of the United Kingdom and France, but there are noticeable differences. Like those countries, Australia saw a rise in absolute CNP fraud, but unlike them, face-to-face fraud did not decline.

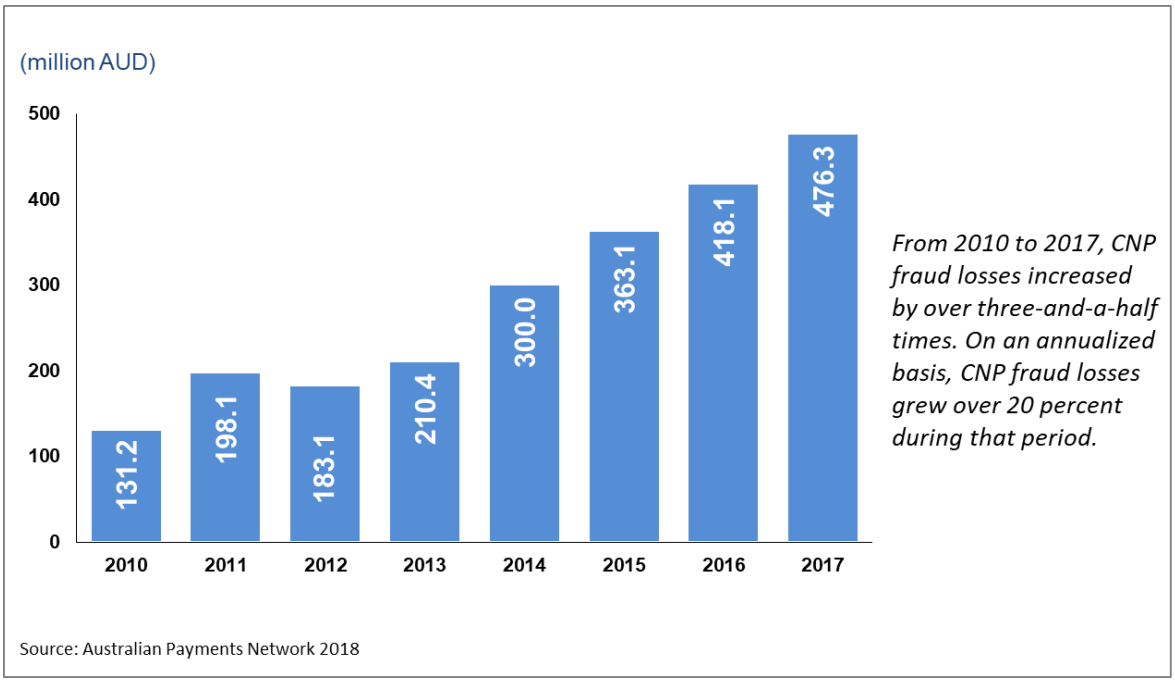
[4] Unless otherwise noted, data and other information in this section are based on Australian Payments Network 2018.

[5] Liability shifts place the burden of face-to-face counterfeit, and potentially lost-or-stolen, fraud on the entity (either merchant or card issuer) that has not adopted EMV chip technology. In the event both parties have adopted EMV technology and a fraudulent transaction occurs, card issuers remain primarily responsible for the fraud loss.

Card-Not-Present Fraud

CNP fraud rose steadily in 2012 and 2013, then increased sharply in 2014 following the liability shifts (see chart 11). Although the CNP fraud growth rate began declining in 2015, fraud losses still increased by more than 13 percent in 2017, reaching over $AUD476 million.

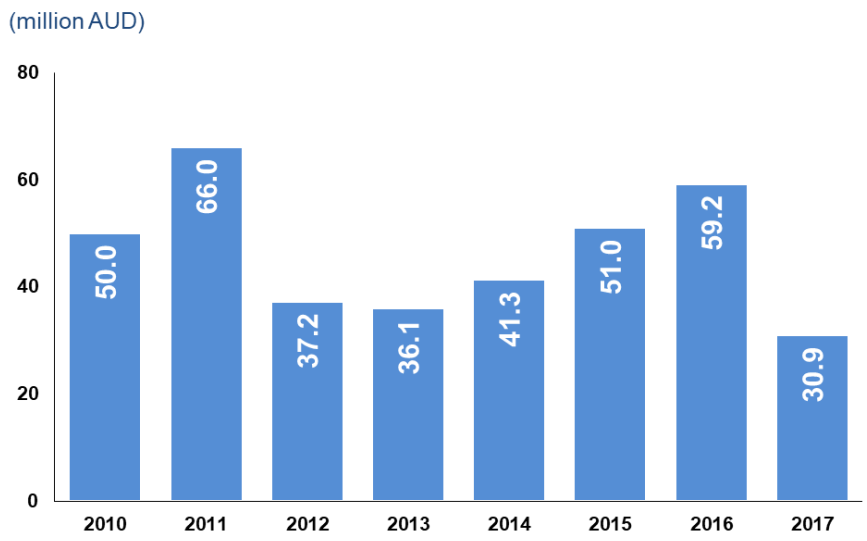
Chart 11: Card-Not-Present Fraud Losses on Australian-Issued Cards



Face-to-Face Card Fraud

Other countries saw a drop in their face-to-face card fraud after they migrated to EMV. Australia did, too, but the decline wasn't as steady or as significant. Counterfeit card fraud actually increased following the liability shift dates, though it did decline significantly in 2017, when it fell to its lowest level since the EMV migration (see chart 12). The initial increase occurred because the migration to chip-enabled ATMs lagged the migration of chip-enabled POS devices. The Australian Payments Network, a self-regulatory body created by payment industry participants, had mandated that all ATM terminals be EMV compliant by December 31, 2016, a date that lagged the POS liability shifts by two or three years. Fraudsters were able to continue to carry out counterfeit card fraud at the ATM through 2016, which is reflected in the counterfeit card fraud figures.

Chart 12: Counterfeit Card Fraud Losses on Australian-Issued Cards

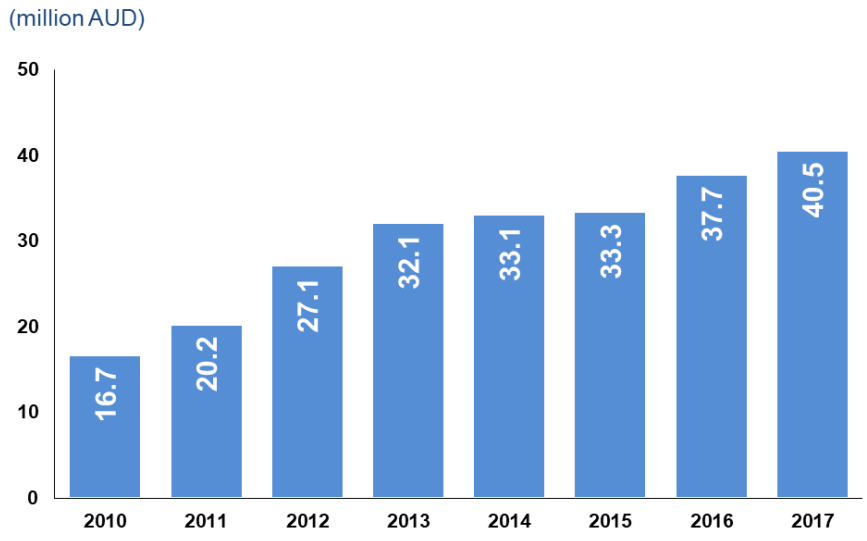


After the liability date shifts in 2013 and 2014, counterfeit card fraud rose through 2016, then dropped in 2017.

Source: Australian Payments Network 2018

Lost-or-stolen-card fraud in Australia has also been trending upward since 2010, even after the liability shifts (see chart 13). As in the United Kingdom, where lost-or-stolen-card fraud has also been rising, this type of card fraud represents a small portion of the total card fraud.

Chart 13: Lost-or-Stolen-Card Fraud Losses on Australian-Issued Cards



Lost-or-stolen card fraud rose from 2010 to 2017. Even after the implementation of EMV liability shifts in 2013 and 2014, this fraud type continued to rise.

Source: Australian Payments Network 2018

Other Card and Payments Fraud

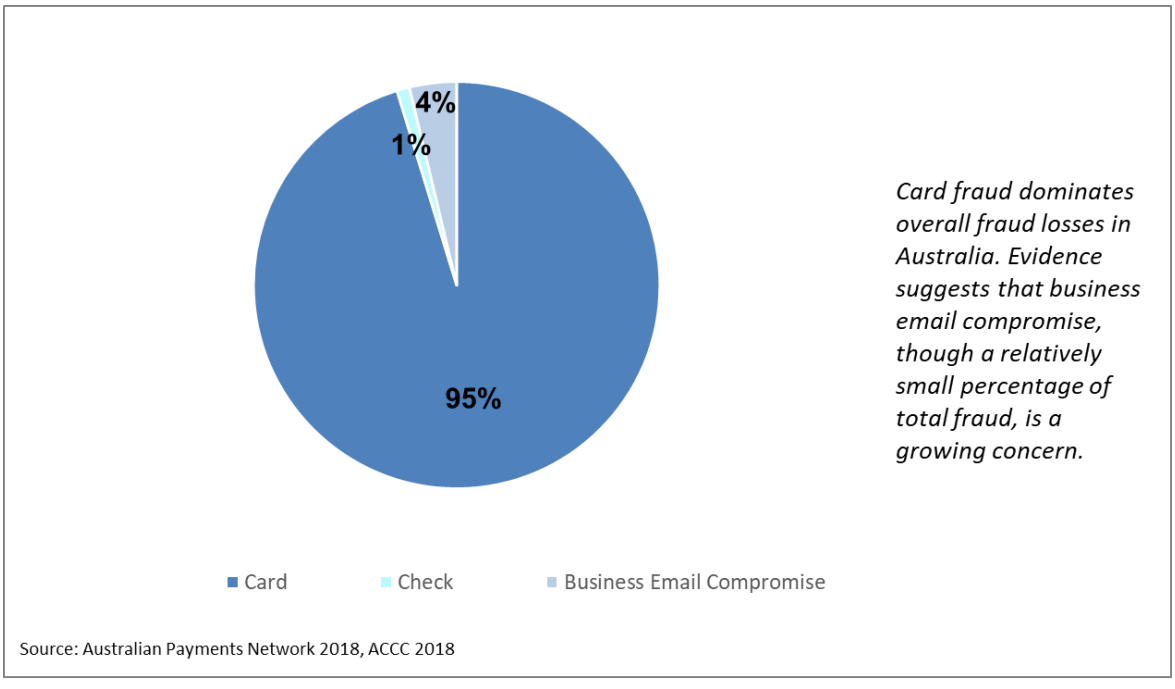
Other types of card fraud beyond CNP, counterfeit, and lost-or-stolen-card fraud made up less than 2.5 percent of Australia's 2017 total card fraud. (CNP fraud losses represented a staggering 85 percent of all card fraud losses.) Other types of card fraud include fraud on cards never received by the intended party and on cards obtained through fraudulent applications. Fraudulent application fraud has risen over the last several years while fraud from cards never received has declined. The former trend aligns with the growth of data breaches and thefts, which can lead to more fraudulent applications; the latter, to the drop in mailings of payment cards after the surge of mailings when existing cardholders were issued replacement cards during the EMV migration process.

The fraud rate on checks in Australia has historically been substantially lower than for cards, and it's declining further as check usage goes down. In 2017, check fraud totaled $AUD5.9 million, with a very low fraud rate of 0.5 basis points.

As in the United Kingdom, BEC is a growing concern in Australia. A report by the Australian Competition and Consumer Commission found that BEC losses exceeded $AUD22 million during 2017 (ACCC 2018). This figure is well below that of card fraud but more than three-and-a-half times greater than check fraud. Research found that during the first half of 2017, Australian companies were the world's second most popular target for BEC (Braue 2017). They received over 27 percent of the global BEC attacks, trailing only the United States.

Chart 14 shows how card fraud compares to non-card payments fraud.

Chart 14: Fraud Losses by Payment Type in Australia



Source: Australian Payments Network 2018, ACCC 2018

UNITED STATES[6]

In 2012, the Federal Reserve began collecting fraud data about non-cash payments fraud as part of the Federal Reserve Payments Study, a benchmark study of non-cash payments in the United States. However, the history of available fraud data does not date back as far as the data from the other countries studied in this paper. The limited data since the EMV POS liability shift occurred makes it difficult to provide any assessments regarding the long-term success of EMV in mitigating U.S. fraud. Still, it is possible, at a minimum, to assess changes leading up to the EMV migration and one year after.

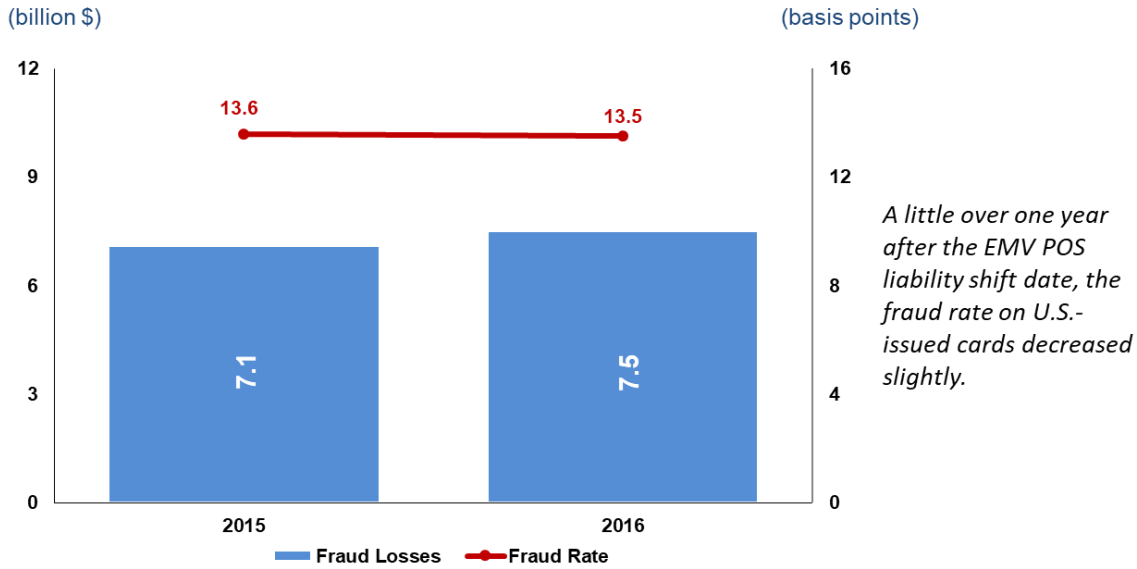
Total Card Fraud

More than three years after the October 2015 POS liability shift, the EMV environment in the United States is beginning to mature. According to Visa's latest published EMV figures, over 3.1 million merchant locations, representing about 67 percent of U.S. storefronts, now accept chip cards. Furthermore, Visa has issued nearly 500 million EMV credit and debit cards, representing 69 percent of all the issuer's credit and debit cards (Visa 2018).

Because the United States' move to EMV lagged other countries, it should be no surprise that card fraud rates are higher than in those markets that had migrated to EMV earlier (see chart 15). However, a very slight positive change to the card fraud rate occurred in 2016, while absolute card fraud rose to $7.5 billion from $7.1 billion in 2015. What the positive development in the fraud rate means is that during 2015–16, spending on cards—or dollar volume on cards—grew faster than the amount of fraud on cards.

[6] Data and information in this section are based on BOG 2018, unless otherwise indicated.

Chart 15: Fraud Losses and Rates on U.S.-Issued Cards



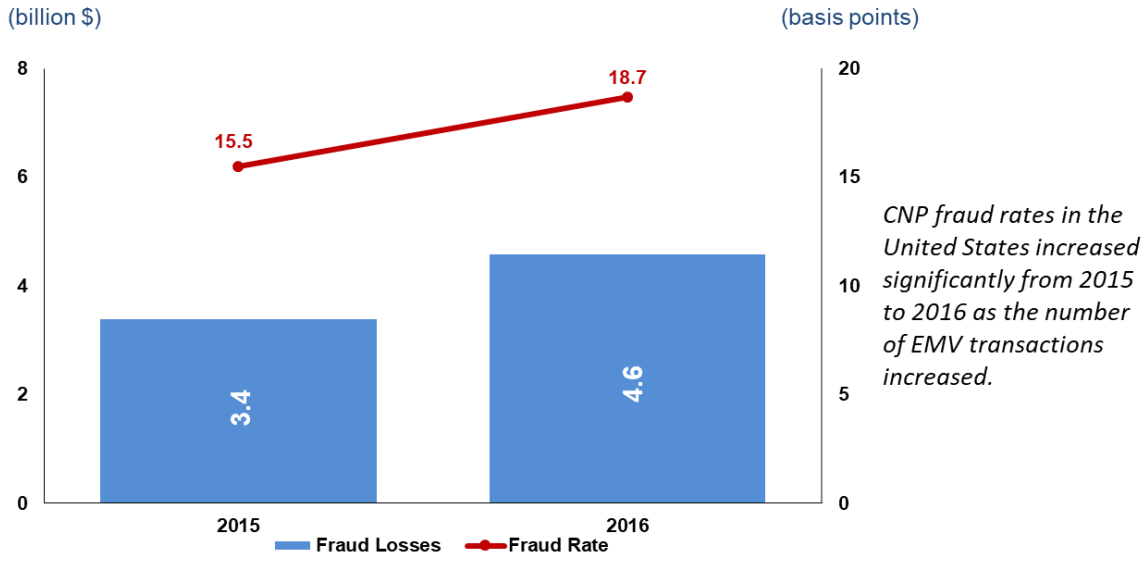
Source: Board of Governors of the Federal Reserve System 2018

As in other countries, it's primarily counterfeit fraud and CNP fraud driving U.S. card fraud. Elsewhere, we saw how card counterfeiting dropped after EMV chip cards were introduced. We also saw that CNP fraud was barely affected, which is not surprising considering that EMV cards can add security only for physical transactions. Will this pattern also hold in the United States?

Card-Not-Present Fraud

The United States, like the other countries, has CNP fraud as the top type of card fraud (see chart 16). CNP fraud was responsible for nearly $4.6 billion in losses in 2016. Absolute fraud for CNP transactions exceeded the face-to-face channel for the first time that year, and the fraud rate for CNP transactions was significantly higher, and grew substantially from 2015 to 2016.

Chart 16: Card-Not-Present Fraud Losses and Rates on U.S.-Issued Cards

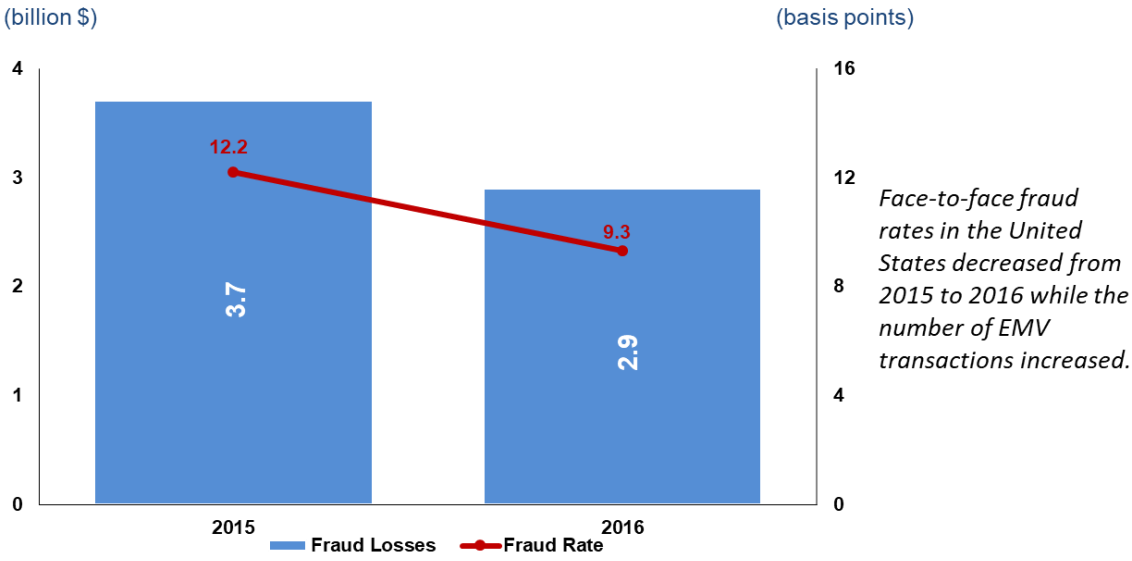


Source: Board of Governors of the Federal Reserve System 2018

Face-to-Face Card Fraud

Although we do not have enough fraud data since the October 2015 liability shift to accurately assess EMV's impact on card fraud (more specifically, on face-to-face card fraud), data from 2015 and 2016 suggest that the U.S. experience may be similar to that of the United Kingdom and France: falling face-to-face fraud but increasing CNP fraud. The rate of in-person card fraud in the United States fell from 12.2 basis points in 2015 to 9.3 basis points in 2016, while the fraud rate for remote transactions climbed from 15.5 basis points to 18.7 basis points. The rate of fraud on face-to-face transactions dropped to less than half of that for CNP transactions in just a little more than a year after the POS liability shift (see chart 17).

Chart 17: Face-to-Face Fraud Losses and Rates on U.S.-Issued Cards

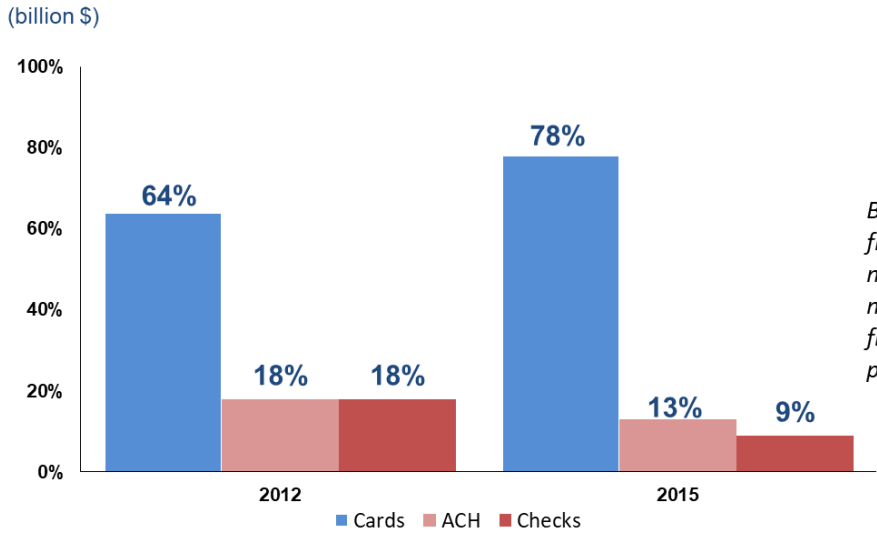


Source: Board of Governors of the Federal Reserve System 2018

Other Card and Payments Fraud

Card fraud is the leading contributor to payments fraud in the United States. Among fraudulent card, check, and ACH transactions, it accounted for nearly 65 percent of fraud in 2012 (see chart 18). By 2015, that figure had reached 78 percent.

Chart 18: Percent of Total Fraud Losses by Payment Type in the United States

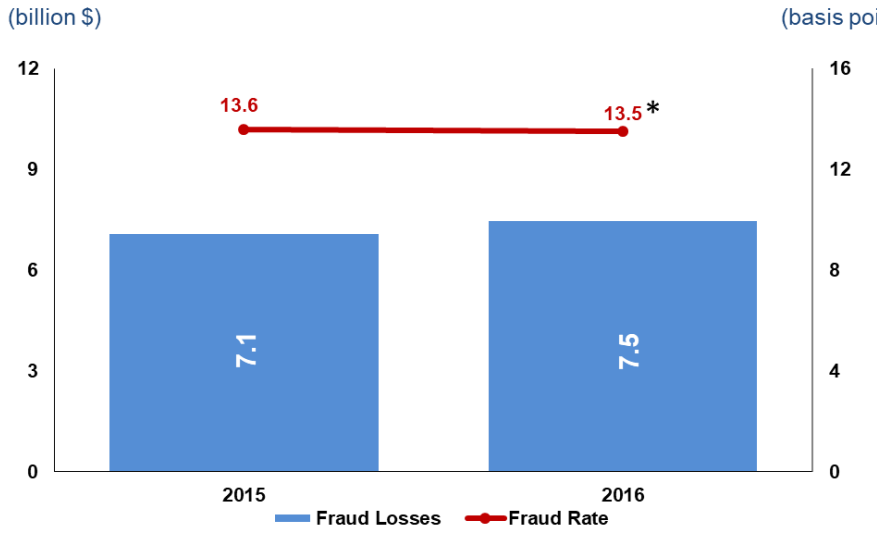


By 2015, fraud losses from cards represented nearly 80 percent of non-cash payments fraud, up from 64 percent in 2012.

Source: Board of Governors of the Federal Reserve System 2018

Not only is the amount of fraud on card transactions significantly larger than for other payment types, but also the fraud rate for card transactions is much greater (see chart 19).

Chart 19: Fraud Rates by Payment Type in the United States



A little over one year after the EMV POS liability shift date, the fraud rate on U.S.-issued cards decreased slightly.

* The card fraud rate in this chart differs from the card fraud rate in chart 19 (10.8). Two different surveys were used to derive these figures. For a detailed explanation of this discrepancy, see Appendix A in BOG 2018.
Source: Board of Governors of the Federal Reserve System 2018

Although the Federal Reserve study did not capture data on BEC or EAC fraud, other data suggests that this fraud type is having a significant impact on payments fraud. While it is possible that BEC scams are responsible for some check or ACH fraud, most of BEC/EAC fraud involves wire transfers, which was not included in the Federal Reserve's fraud report. According to the Federal Bureau of Investigation, victims reported sending more than 19,000 financial transactions valued at over $1.6 billion from June 2016 to May 2018 to fraudulent recipients (FBI 2018b).

CONCLUSION

EMV chip cards appear to have mitigated counterfeit card fraud. Early data in the United States show a trend in that direction that is consistent with the countries that migrated to EMV well before the United States: counterfeit card fraud is dropping.

In all of the countries examined, CNP fraud is the leading type of card fraud and is becoming an even larger portion of total card fraud. But could the increase in CNP fraud following EMV chip card migration be slowing? In the United Kingdom, the growth rate of absolute CNP fraud fell to single digits (8.5 percent) in 2016 and then CNP fraud declined in 2017 for the first time since 2011. In France, though the fraud rate on CNP transactions remains significantly higher than that for face-to-face transactions, it declined for two consecutive years, reaching 26.0 basis points in 2017 from 36.4 in 2015. While this fraud rate is still high, it is the lowest rate of CNP fraud recorded in France since the EMV chip card migration in the nineties. In Australia, although absolute CNP fraud continues to grow, the growth rate of CNP fraud declined after 2015, reaching its slowest growth rate in 2017 since the migration.

Although the United States at the end of 2016 was only a little more than a year removed from the EMV POS liability shift, CNP fraud losses had already exceeded losses for all other types of card fraud. Moreover, the CNP fraud rate was more than double that of in-person fraud. What was more alarming was that the rate of CNP fraud grew three times faster from 2015 to 2016 than the rate of overall CNP transaction volume.

However, the CNP fraud trends in the United Kingdom and France show that the industry became better equipped to mitigate CNP fraud a few years after EMV migration. Many improvements in CNP risk solutions and technological advances have been made since these countries first began moving to EMV chip cards. In fact, a paper published in June 2018 by the Accredited Standards Committee X9 identifies many strategies and solutions that are either widely available now or will be soon and could significantly reduce CNP fraud. Further, EMVCo recently released the first version of specifications for a new e-commerce standard, Secure Remote Commerce, or SRC, which is designed not only to streamline consumers' online shopping experience but also to enhance the security of e-commerce transactions through tokenization and dynamic data. We do not yet know whether or not payment industry participants will ultimately adopt any of these, but the industry is undoubtedly in a much better position today to mitigate CNP fraud than it was in the early days of EMV adoption in other countries. CNP transaction volumes will continue to rise as more consumers shop online, so it is not unreasonable to expect CNP absolute fraud figures to increase solely based on increasing transaction volumes.

While CNP fraud is a considerable challenge that EMV cards unfortunately cannot address, two new themes are emerging that could significantly affect payments fraud. In the United Kingdom, lost-or-stolen-card fraud has risen significantly since that country's EMV migrations, most notably over the past three years. Australia has also seen a steady—but slower—rise in this type of fraud during the same time. There are a growing number of transactions that do not require cardholder verification, as floor limits for transactions requiring a PIN continue to rise and signatures are being phased out. With these types of transactions poised to grow in the United States, it is possible that lost-or-stolen-card fraud will worsen here in the United States as it did in the United Kingdom and Australia.

A relatively new fraud threat in the United States is starting to draw attention. Business email, or email account, compromise (BEC/EAC) has generally taken place outside the realm of payment cards. However, it is becoming increasingly attractive to fraudsters as an alternate target as EMV effectively continues to mitigate counterfeit card fraud and more issuers and merchants implement new technologies and processes to mitigate CNP fraud.

Wire transfers are the usual payment method that fraudsters use to perpetrate BEC/EAC, though some have used ACH and even checks. As BEC/EAC has evolved, it has begun to include payment cards, to the point that, in October 2018, the FBI issued a press release regarding the growing use of gift cards in BEC/EAC schemes (FBI 2018a). This fraud is a global phenomenon and, according to FBI data, accounted for over $12.5 billion in global fraud losses from October 2013 to May 2018 (FBI 2018b). Of that amount, $5.3 billion occurred from January 2017 through May 2018, a relatively short period that underscores the rapid growth of this type of fraud. Anecdotal information suggests that BEC/EAC continued to grow throughout 2018. Given its social engineering aspect as well as ongoing efforts to mitigate card fraud both in person and remotely, BEC/EAC is poised to become a significant, if not the leading, contributor to fraud in the United States. (See the appendix for more information about BEC.)

APPENDIX: BUSINESS EMAIL COMPROMISE

According to the Federal Bureau of Investigation (FBI), business email compromise (BEC) and email account compromise (EAC) are sophisticated scams that target businesses and individuals, respectively, and most often involve wire payment transfers to finalize the fraud (FBI 2018b). The scammer frequently carries out BEC by compromising legitimate email accounts through social engineering or computer intrusion techniques, then conducting fraudulent, or unauthorized, payment transfers. In the United Kingdom, this type of fraud is referred to as *authorized push payment fraud*.

In perhaps the most common form of business email compromise, the fraudster impersonates a senior executive, usually the chief executive officer or chief financial officer. The fraudster initially gets access into a company's network through various social engineering attacks and the use of malware, then spends time studying such things as the company's vendors, accounts receivables and payables systems, executives' travel schedules, and communication styles. Timing the opportunity to commit the fraud based on invoice due dates or executive travel, the imposter then sends an email directly from the executive's email account, or a spoofed account, to an employee in the finance department. That person is instructed to immediately submit a wire transfer to a vendor—but the accompanying wire instructions direct the funds to the fraudster's account.

Other varieties of business email compromise include vendor impersonation scams, when the fraudster impersonates a vendor and requests that funds be transferred, but as with the previous scam, the funds go to the fraudster's account rather than the vendor's account.

Email account compromise targets individuals, unlike business email compromise which targets businesses. These schemes have been heavily focused on real estate and trust account transactions in the past several years. For example, a fraudster may impersonate an attorney, title company representative, or real estate agent or broker and instruct a real estate buyer to transfer funds related to the transaction to the fraudster's account. Or, in the trust account scheme, fraudster poses as a lawyer or law firm involved in a time-sensitive matter for another party supposedly acting on behalf of the victim. The fraudster requests that the victim initiate a transfer of funds from a trust account. The fraudster convinces the target that secrecy is critical, so the victim should not provide a reason for the transfer. And as in the other schemes, the fraudster controls the receiving account.

More recently, some BEC schemes haven't involved an immediate funds transfer. Rather, the scammer seeks obtain sensitive financial records. Like the early steps of the standard BEC, a fraudster compromises or spoofs an executive's email account and sends a request to the finance or human resources department requesting copies of an employee's W-2 or other financial records. The fraudster can then use this information for various purposes ranging from filing fraudulent tax returns to create synthetic identities or to get confidential information on the company's financial performance for acquisition or stock purchase.

REFERENCES

Australian Competition and Consumer Commission (ACCC). 2018. *Targeting Scams: Report of the ACCC on Scams Activity 2017*." Accessed February 28, 2019, https://www.accc.gov.au/system/files/F1240_Targeting%20scams%20report.PDF.

Australian Payments Network. 2018. *Australian Payment Card Fraud 2018*. Accessed January 30, 2019. https://www.auspaynet.com.au/sites/default/files/2018-08/AustralianPaymentCardFraud-2018-Report.pdf.

Banque de France. 2018. "Annual Report of the Observatory for the Security of Payment Means: 2017" (English version). Accessed January 30, 2019. https://www.banque-france.fr/sites/default/files/medias/documents/annual-report-2017-osmp2017-gb-20181108.pdf.

Board of Governors of the Federal Reserve System (BOG). 2018. *Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study*. Accessed January 30, 2019. https://www.federalreserve.gov/publications/files/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf.

Braue, David. 2017. "Australian Companies Are World's Second Most-Popular Targets for Email Fraud." *CSO* (September 13, 2017). Accessed February 28, 2019. https://www.cso.com.au/article/627211/australian-companies-world-second-most-popular-targets-email-fraud/.

Federal Bureau of Investigation (FBI). 2018a. "Business E-Mail Compromise: Gift Cards." Public Service Announcement (October 24, 2018). Accessed January 30, 2019. https://www.ic3.gov/media/2018/181024.aspx.

———. 2018b. "Business E-Mail Compromise: The 12 Billion Dollar Scam." Public Service Announcement (July 12, 2018). Accessed January 30, 2019. https://www.ic3.gov/media/2018/180712.aspx.

King, Douglas. 2012. "Chip-and-PIN: Success and Challenges in Reducing Fraud." Retail Payments Risk Forum Working Paper (Federal Reserve Bank of Atlanta). Accessed January 29, 2019. https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/120111wp.pdf.

UK Finance. 2018. *Fraud the Facts 2018*. Accessed January 29, 2019. https://www.ukfinance.org.uk/wp-content/uploads/2018/07/Fraud-the-facts-Digital-version-August-2018.pdf.

Visa Inc. 2018. "Visa Chip Card Update." Accessed January 29, 2019. https://usa.visa.com/dam/VCOM/regional/na/us/visa-everywhere/documents/visa-emv-chip-infographic.pdf.