Card-Not-Present Fraud around the World

Version 1.0

Date: March 2017

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV is a trademark owned by EMVCo LLC.

The U.S. Payments Forum has used best efforts to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. The U.S. Payments Forum disclaims all warranties as to the accuracy, completeness or adequacy of information in this document. Comments or recommendations for edits or additions to this document should be submitted to: receipt-best-practices@uspaymentsforum.org.

Table of Contents

Table of Figures

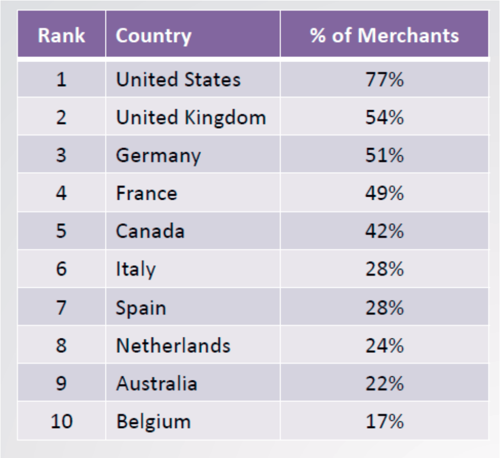
1 Introduction

Globally, card-not-present (CNP) fraud includes telephone, Internet, and mail-order transactions where the cardholder does not physically present the card to the merchant. Most CNP fraud involves the use of card details that have been obtained through skimming, hacking, email phishing campaigns, telephone solicitations or other methods. The card details are then used to facilitate fraudulent transactions.

Although EMV deals effectively with counterfeit fraud, it does not address CNP fraud. With the migration to EMV for card-present transactions, fraudsters shift their focus to other channels, such as CNP transactions.

This white paper provides U.S. industry stakeholders with an overview of CNP fraud in regions or countries that are similar to the United States in overall payment infrastructure and e-commerce maturity and have also migrated to EMV.

Figure 1 lists the 10 countries with the largest percentage of online merchants, according to the results of the 2015 Merchant Risk Council (MRC) Global Fraud Survey. This paper examines CNP fraud in these countries, either individually or as part of a region (e.g., Single Euro Payments Area or SEPA.)



Rank	Country	% of Merchants
1	United States	77%
2	United Kingdom	54%
3	Germany	51%
4	France	49%
5	Canada	42%
6	Italy	28%
7	Spain	28%
8	Netherlands	24%
9	Australia	22%
10	Belgium	17%

Source: MRC 2015 Global Fraud Survey Results

Figure 1. Countries with the Highest Percentage of E-commerce Sales

Publicly available information is scarce and data are reported differently in each country (depending on whether the focus is on issuers or merchants), so this paper is unable to cover all solutions to the problem of CNP fraud in all countries. Rather, the paper offers insight into solutions implemented in those locations for which data are available. In addition, the paper presents an overview of fraud prevention tools and methods in each location along with relevant legislation and its impact.

2 Global Overview

The world might seem smaller than ever in this digital age. However, a minimum of truly global information is available about fraud, probably as a result of the diversity of payment landscapes and the resulting singularity of fraud patterns in individual markets. Fortunately, the annual surveys conducted by associations with global memberships provide some insight into global fraud.

The MRC conducts an annual study to analyze the state of CNP fraud globally and discover what fraud prevention solutions are being used by participants in the payments ecosystem. According to the results of the 2015 Global Fraud Survey, e-commerce sales fraud is becoming “cleaner.” (“Clean” fraud refers to fraudulent orders that look legitimate due to the fraudster’s ability to provide complete and accurate personal data.) While fraud tracking is not gap-free, chargeback and confirmed fraud rates tend to be the most important key performance indicators. Fraud scoring models and device fingerprinting are reported to be the most effective tools; however, 3D-Secure (3DS) and device fingerprinting are being deployed the most quickly.

2.1 Evolving Fraud Rates[1]

Figure 2 shows fraud rates for global e-commerce sales in 2013 and 2014. MRC merchants report a fraud rate of 0.53% on global sales in 2014, down from 2013.

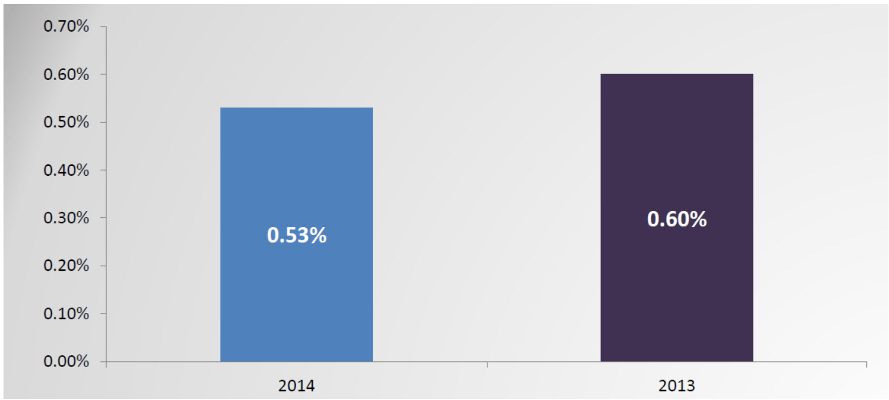


Figure 2. Average Percentage of E-commerce Sales Lost Annually to Payment Fraud Globally

Figure 3 illustrates rates of e-commerce sales lost to fraud in the top 10 countries.

[1] The source for all figures in this section is the MRC 2015 Global Fraud Survey Results. Note that the respondents to the survey were primarily members of the MRC.

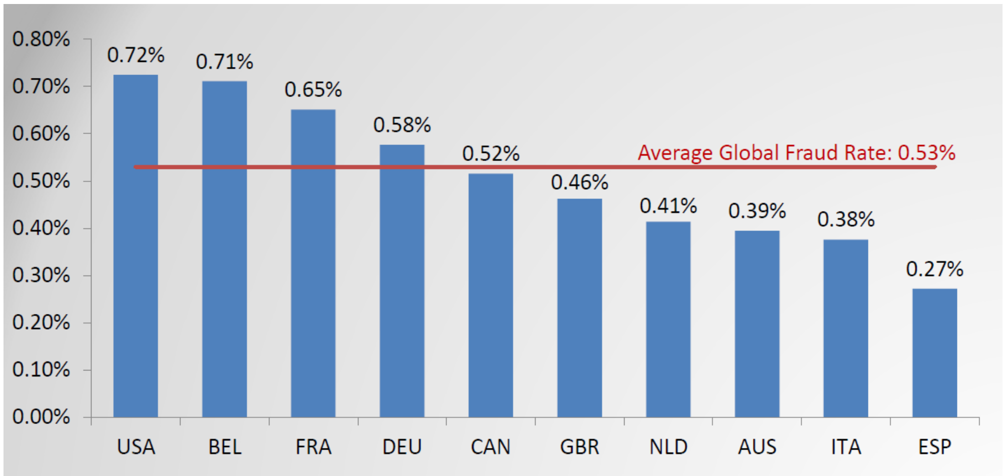
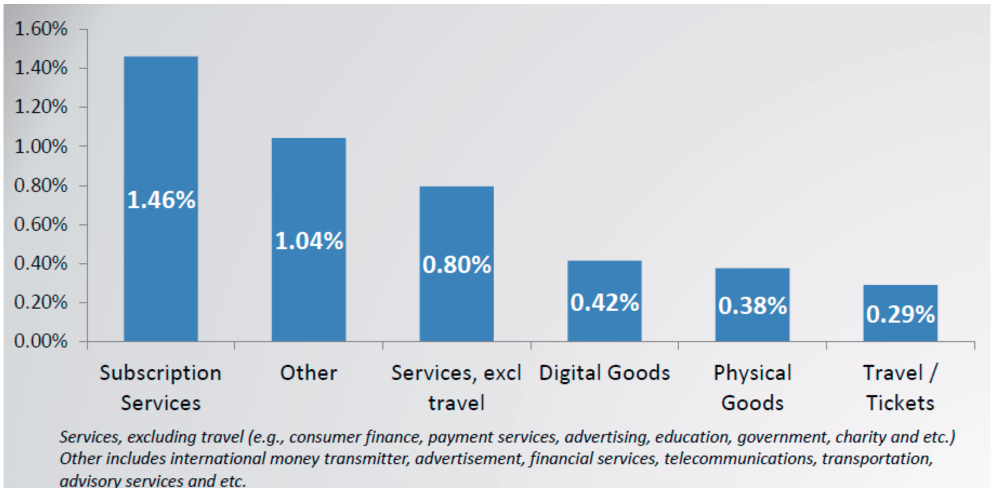


Figure 3. Fraud Rates by Country for E-commerce Sales

Figure 4 shows rates of fraud by type of merchant.



Services, excluding travel (e.g., consumer finance, payment services, advertising, education, government, charity and etc.)
Other includes international money transmitter, advertisement, financial services, telecommunications, transportation, advisory services and etc.

Figure 4. Global Fraud Rates by Merchant Type

2.2 Authentication Methods and Fraud Detection Tools

According to the MRC study, the two most commonly used methods for authenticating online transactions are card verification numbers (CVN) and negative lists (also known as blacklists). The report indicates that the most common authentication tools to be added in the next 12 months are 3DS and device fingerprinting. However, merchant opinion on the effectiveness of different fraud detection and prevention tools varies. Manual fraud review percentages also vary, by market; in most countries, merchants review less than 15 percent of their transactions.

Figure 5 illustrates how a number of different validation services (i.e., services that validate cardholder information for a transaction) are currently being used and how merchants plan to use these services over the next 12 months. This figure shows that the two transaction validation tools scheduled to be deployed most often are e-mail address validation and payer authentication (3DS).

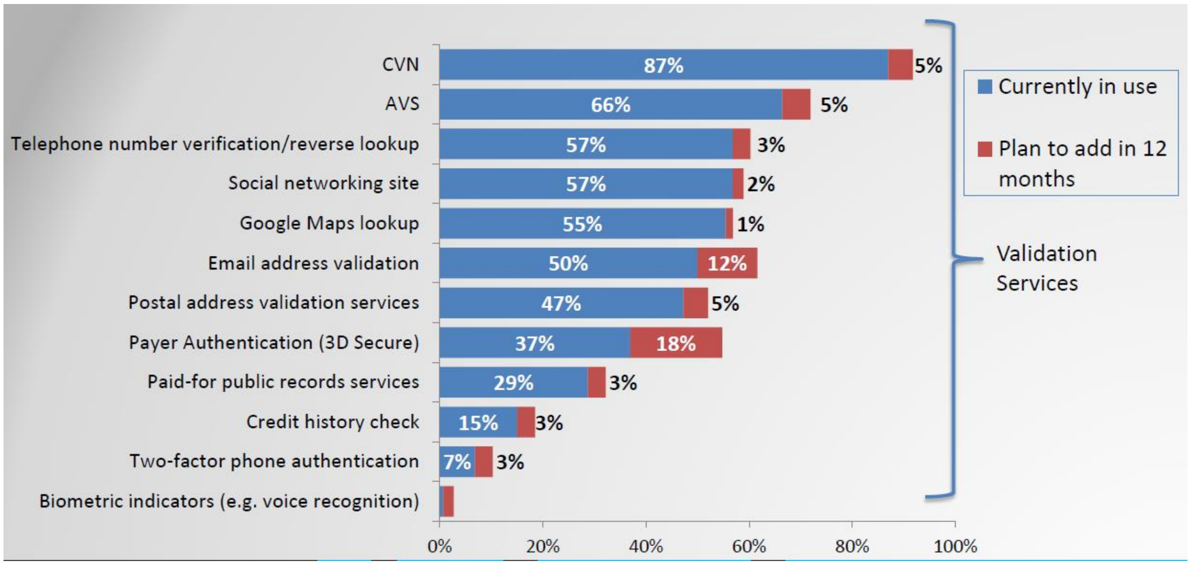


Figure 5. Transaction Validation Services Currently Used and Anticipated to be Used

Figure 6 illustrates current and anticipated use of proprietary and multi-merchant tools (i.e., tools that leverage data from multiple merchants to provide more insight for authenticating a transaction) that analyze data and track purchase devices. The tools anticipated to grow the most are customer Web site behavior analysis and device fingerprinting.

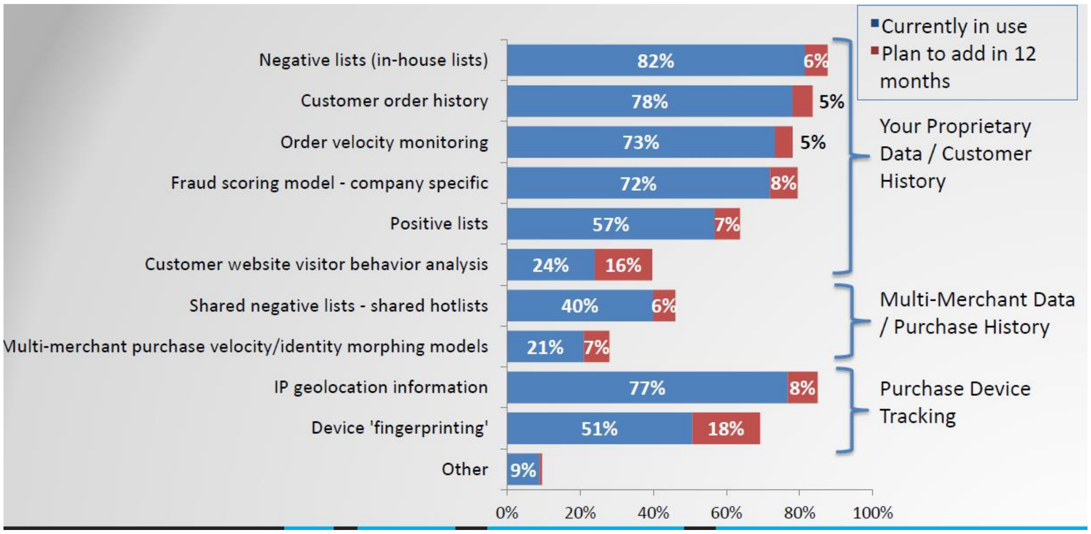


Figure 6. Data Analysis and Device Tracking Tools Currently Used and Anticipated to be Used

Figure 7 indicates how merchants evaluate the effectiveness of five particular tools. Note that three of the tools (device fingerprinting, 3DS, and fraud scoring models) are considered to be almost equally effective.

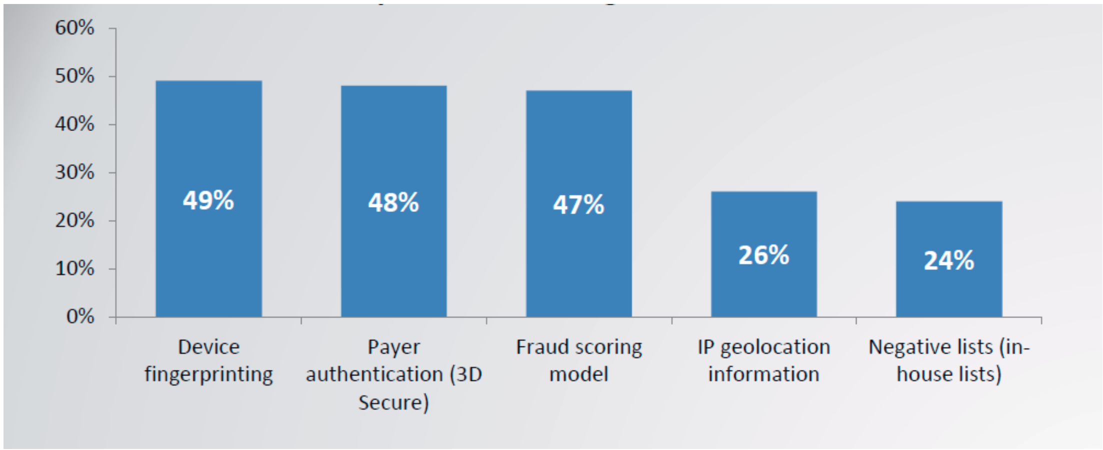


Figure 7. Merchant Evaluation of Current Tools (% Positive)

As Figure 8 shows, currently 8–15 percent of transactions are still being screened manually in the top 10 countries, despite the available technology.

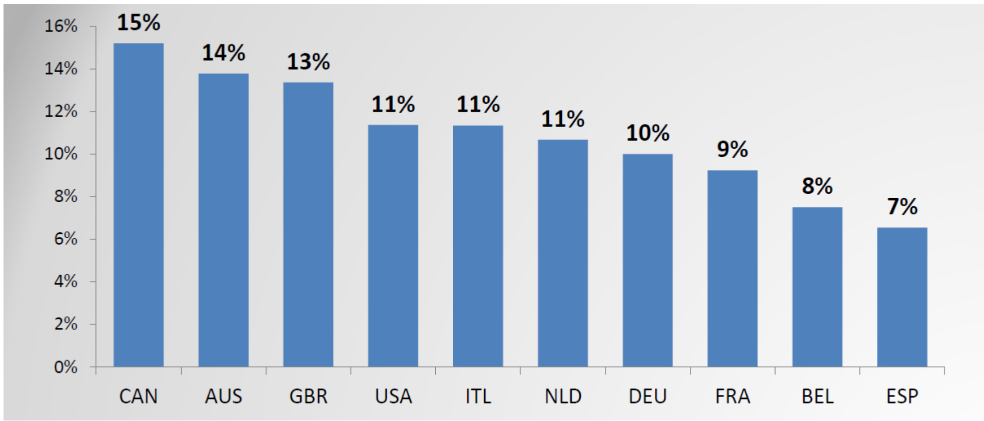


Figure 8. Percentage of Transactions Screened Manually in the Top 10 Countries

2.3 Legislation

There is no global legislation governing CNP fraud, and this situation will likely persist. However, some regions and countries have, or are considering, various types of legislation; these initiatives are described in the following sections.

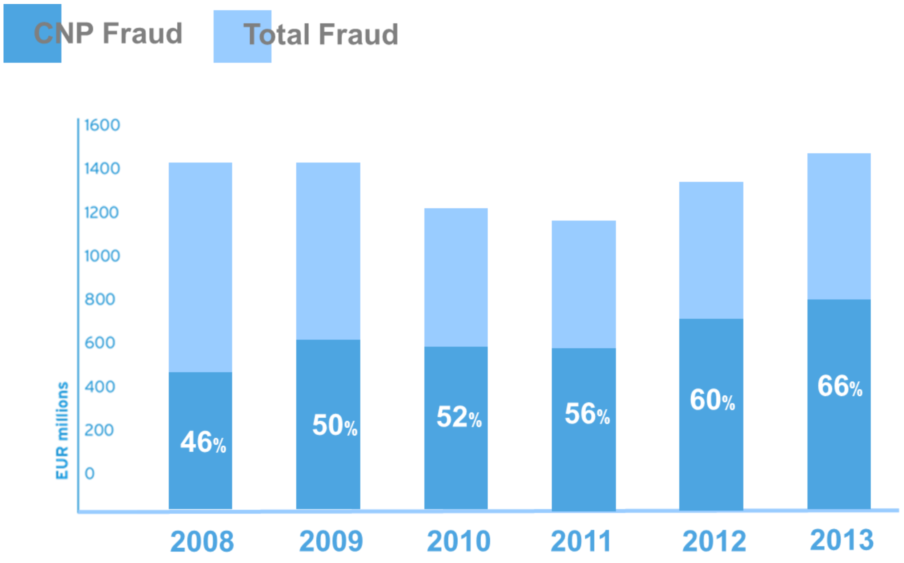
3 Europe/SEPA

In Europe and the Single Euro Payments Area (SEPA), most countries with mature 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, accounting for 41–85 percent.

Given the trends of the past several years, CNP fraud is likely to continue to increase in the absence of appropriate mitigation measures. The European Banking Authority has published guidelines that are required to be followed to ensure the security of Internet payments, and the European Central Bank has published oversight standards for card payment schemes that focus particularly on security and efficiency.[2]

3.1 Evolving Fraud Rates

Figure 9 shows the evolution of CNP fraud within the SEPA from 2008 through 2013. It is important to note that fraud is defined independently of whether the loss is ultimately borne by the customer, issuer, acquirer, or merchant. (Note that the percentages shown in graph indicate the percentage of CNP fraud for that year.)



Source: ECB, 4th report on Card Fraud, July 2015

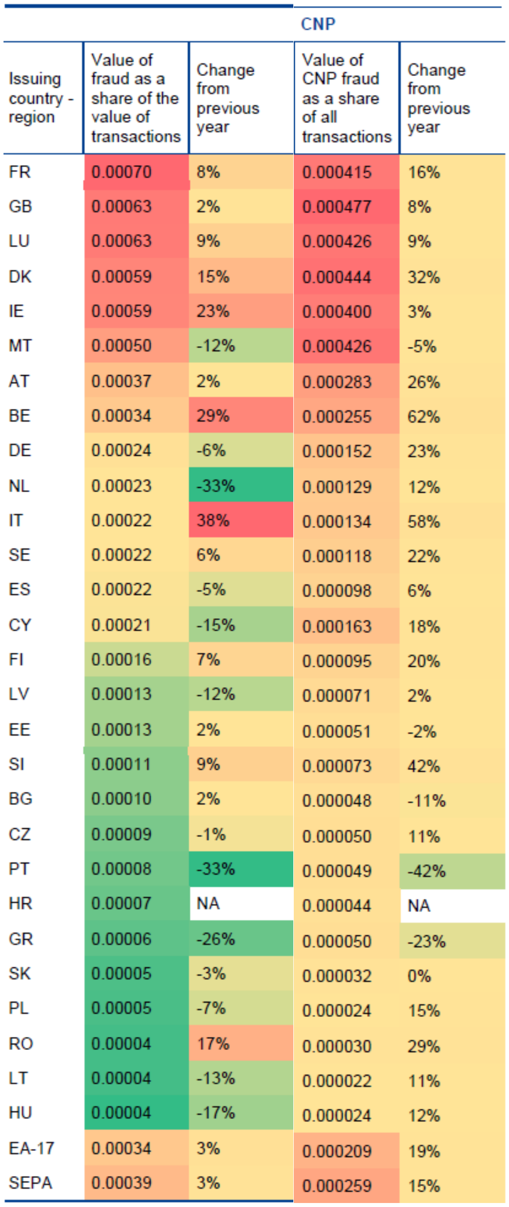
Figure 9. CNP Fraud as a Percentage of the Total Value of Card Fraud

In 2013, the value of fraud perpetrated using cards issued inside the SEPA increased for CNP transactions but decreased across other transaction channels. CNP fraud accounted for 66 percent of total fraud losses, compared with 60 percent in 2012; CNP's share has been growing steadily since 2010. The overall increase of 4% in total fraud was largely driven by a 40% increase in CNP fraud over a five-year period.

[2] European Central Bank, Eurosystem, *Guide for the assessment of card payment schemes against the oversight standards*, February 2015.

CNP fraud was the largest category of fraud in absolute value, with €958 million in losses in 2013. In contrast to ATM and point-of-sale fraud, CNP fraud was the only category reporting an increase over the previous year, up 20.6 percent from 2012. While available data on non-fraudulent CNP transactions suggest that there was also considerable growth in total CNP transactions, the (admittedly incomplete) information seems to indicate that CNP fraud increased faster than total CNP transactions.

Card-present fraud within the SEPA and worldwide is expected to decline even further as a result of EMV migration. CNP fraud remains the most prevalent type of fraud and generates the largest losses, particularly for countries with high EMV migration rates. Most of the mature card markets characterized by high transaction values per inhabitant (e.g., France, the United Kingdom) experienced high CNP fraud rates. Figure 10 illustrates the value of CNP fraud as a percentage of overall fraud categorized by country, from an issuing perspective.[3]



			CNP	
Issuing country - region	Value of fraud as a share of the value of transactions	Change from previous year	Value of CNP fraud as a share of all transactions	Change from previous year
FR	0.00070	8%	0.000415	16%
GB	0.00063	2%	0.000477	8%
LU	0.00063	9%	0.000426	9%
DK	0.00059	15%	0.000444	32%
IE	0.00059	23%	0.000400	3%
MT	0.00050	-12%	0.000426	-5%
AT	0.00037	2%	0.000283	26%
BE	0.00034	29%	0.000255	62%
DE	0.00024	-6%	0.000152	23%
NL	0.00023	-33%	0.000129	12%
IT	0.00022	38%	0.000134	58%
SE	0.00022	6%	0.000118	22%
ES	0.00022	-5%	0.000098	6%
CY	0.00021	-15%	0.000163	18%
FI	0.00016	7%	0.000095	20%
LV	0.00013	-12%	0.000071	2%
EE	0.00013	2%	0.000051	-2%
SI	0.00011	9%	0.000073	42%
BG	0.00010	2%	0.000048	-11%
CZ	0.00009	-1%	0.000050	11%
PT	0.00008	-33%	0.000049	-42%
HR	0.00007	NA	0.000044	NA
GR	0.00006	-26%	0.000050	-23%
SK	0.00005	-3%	0.000032	0%
PL	0.00005	-7%	0.000024	15%
RO	0.00004	17%	0.000030	29%
LT	0.00004	-13%	0.000022	11%
HU	0.00004	-17%	0.000024	12%
EA-17	0.00034	3%	0.000209	19%
SEPA	0.00039	3%	0.000259	15%

Figure 10. Relative Fraud Levels and Trends from an Issuing Perspective

[3] A list of country codes can be found at http://www.immigration-usa.com/country_digraphs.html

3.2 Authentication Methods and Fraud Detection Tools

In December 2015 and January 2016, CyberSource, a subsidiary of Visa, polled a total of 193 merchants representing a variety of industries and sizes. Although respondents identified fraud as their top payments-related concern,[4] only 33 percent use 3DS to authenticate online buyers. According to the MRC, use of 3DS is highest in Europe because of various issuer or acquirer mandates. Some 46 percent of German merchants use 3DS, followed by 45 percent in France and 40 percent in the United Kingdom; only 18 percent of U.S. and 14 percent of Canadian merchants use the technology.

The SEPA leverages most of the tools found on the list of merchant tools in Figure 5, with the exception of address verification, which seems to be available only in the UK.

Finally, various issuers in some countries adopt other authentication technologies, such as one-time password (OTP) devices, to use in conjunction with 3DS.

3.3 Legislation

In December 2014, the European Banking Authority (EBA) published guidelines to increase the security of Internet payments.[5] These guidelines impose a minimum set of security requirements to be implemented by payment service providers (PSPs) in the EU by August 1, 2015. The guidelines are based on the 2013 recommendations issued by the European Forum for the Security of Retail Payments (SecuRe Pay) and require, among other things, that the issuing PSPs support strong customer authentication (e.g., a method requiring two independent authentication factors, one of which must be dynamic) for the initiation of payments and access to sensitive payment data. Additionally, the guidelines require that PSPs who offer acquiring services must support the issuer PSP for this purpose and that the e-merchant do the same for card transactions over the Internet.

Card payment schemes are required to observe EBA guidelines. Requirements for Internet payments form part of the ECB's guide for the assessment of card networks.

The recently published Payment Services Directive (PSD2)[6] has mandated that EBA provide additional guidelines on strong consumer authentication. EBA published their draft "Regulatory Technical Standards on strong customer authentication and secure communication" and has received numerous feedback. EBA is working on resolving issues and is expected to publish the final version in Q1 2017. These guidelines will come into force 18 months after publication.

[4] *Fraud and Chargeback Reduction Are Top of Mind for E-Commerce Payment Execs, May 27, 2016,* http://www.digitaltransactions.net/news/story/Fraud-and-Chargeback-Reduction-Are-Top-of-Mind-for-E-Commerce-Payments-Execs

[5] *Final Guidelines on the Security of Internet Payments*, December 19, 2014 (EBA/GL/2014/12_Rev1), https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+(Guidelines+on+the+security+of+internet+payments)_Rev1

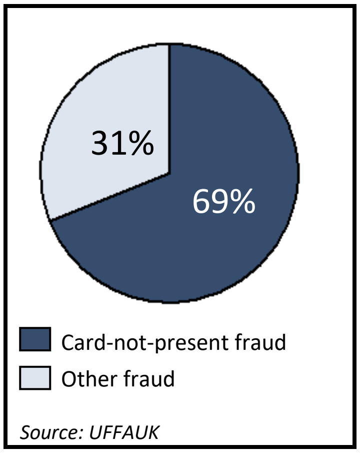
[6] The Payment Services Directive (PSD) was first adopted by the European Union in 2007. This directive provided a legal framework for an EU single market for payments made in Europe, with the aim of making cross-border payments as easy, efficient, and secure as 'national' payments within a Member state. The revised PSD (PSD2) is a data and technology-driven directive which aims to drive increased competition, innovation and transparency across the European payments markets, while increasing the security of Internet payments and account access.

4 United Kingdom 🇬🇧

The United Kingdom (UK) is second only to the U.S. in terms of e-commerce sales, with 54 percent of merchants having an online presence. 3DS is currently used by 40 percent of UK online merchants.

4.1 Evolving Fraud Rates

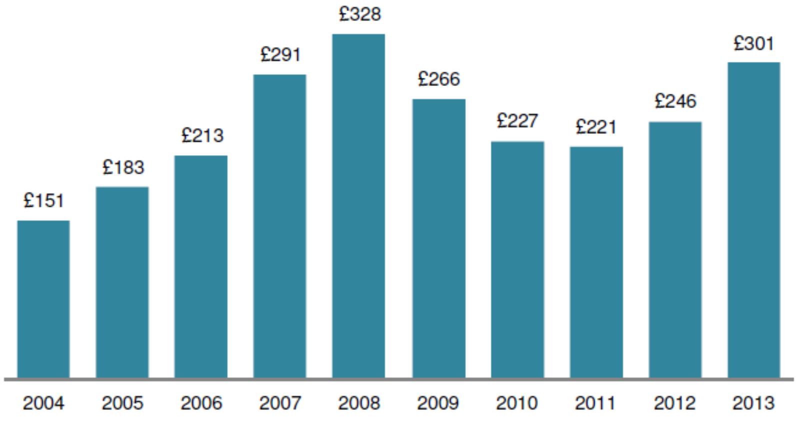
In 2014, card fraud in the UK totaled £479 million (an increase of 6 percent over 2013) of which CNP fraud accounted for 69 percent (Figure 11). However, it is important to consider the massive growth in CNP spending over the past 10 years, especially for transactions over the Internet as opposed to mail order or telephone order (MOTO) transactions.



Source: UFFAUK

Figure 11. CNP vs. Other Card Fraud in the UK in 2014

As Figure 12 shows, CNP fraud decreased between 2008 and 2011, due to the implementation of 3DS. However, in 2012, CNP fraud increased, due to the growth of e-commerce and the declining use of 3DS (the original version affected sales negatively due to cardholder friction). This trend may be changing with the use of risk-based versions of 3DS that are usually transparent to the cardholder.



Source: Financial Fraud Action UK

Figure 12. CNP Fraud in the UK, 2004–2013 (£millions)

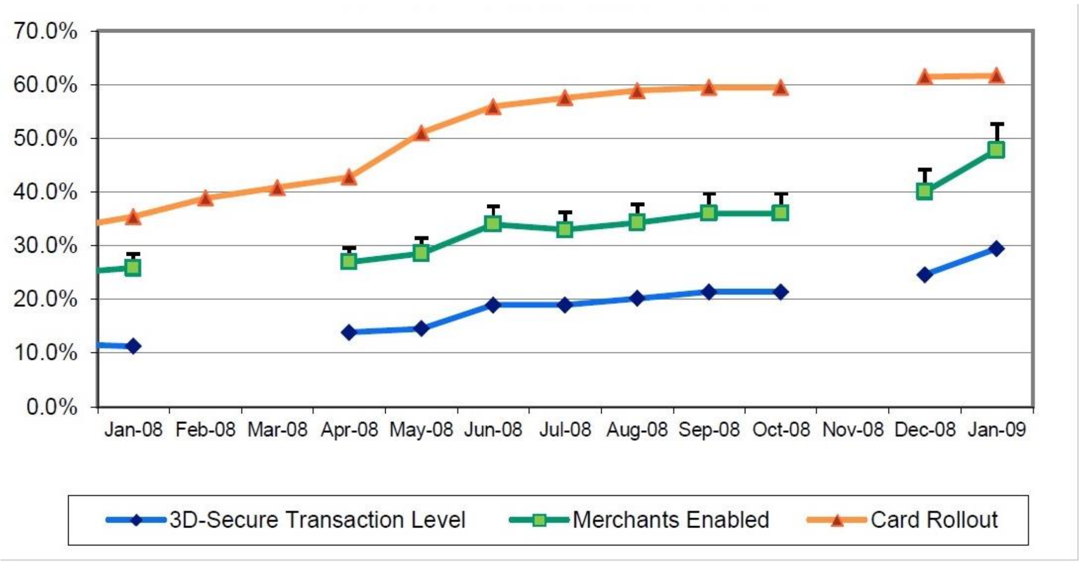
4.2 Authentication Methods and Fraud Detection Tools

Use of sophisticated fraud screening detection tools by retailers and banks is increasing, as is the use of 3DS (e.g., American Express SafeKey®, Discover ProtectBuy, MasterCard SecureCode®, or Verified by Visa®) by both online retailers and cardholders. These online fraud prevention initiatives provide an extra layer of protection for online shopping.

According to the Barclaycard Payment Security Newsletter,[7] the fraud-to-turnover ratio varied markedly between 3DS and non-3DS transactions. Barclaycard's advice to merchants was as follows:

> "To improve your fraud-to-sales ratio in the e-commerce space, think about authentication through 3DS. As of September 2010, Verified by Visa (VbV) penetration in the UK was 53.3% and 90% of the UK VbV volume was fully authenticated. This reduced the fraud-to-sales ratio on fully authenticated transactions to 0.08%, compared to 0.25% for non VbV traffic."

Figure 13 illustrates the rate at which 3DS was adopted in the UK during 2008–2009. As these data show, adoption of such initiatives in mass markets is a gradual process.



Source: ECB Paper, "Recommendations for Security of Internet Payments," response from the UK Cards Association, June 2012.

Figure 13. UK 3D-Secure Rollout, 2008–2009

Hardware-based solutions are possible in the CNP environment for chip-and-PIN transactions. These solutions often require a USB device through which a secure connection is created and dynamic data are generated, making the transaction similar to a card-present transaction. To date, however, these solutions have not gained much traction with merchants or cardholders, due to cost and consumer adoption concerns.

The *BeCardSmart Online* campaign, launched at the end of 2008, provides UK consumers with practical tips for safe Internet shopping.

[7] *Barclaycard Payment Security Newsletter Jan11* Issue 1, January 2011, http://www.slideshare.net/neirajones/barclaycard-payment-security-newsletter-jan11

4.3 Legislation

Initiatives such as the introduction of 3DS and the compliance programs associated with the Payment Card Industry Data Security Standard (PCI DSS) indicate that the UK payment card industry takes the issue of fraud seriously and is addressing it without the need for regulatory intervention. The UK is subject to PSD2, described in Section 3.3.

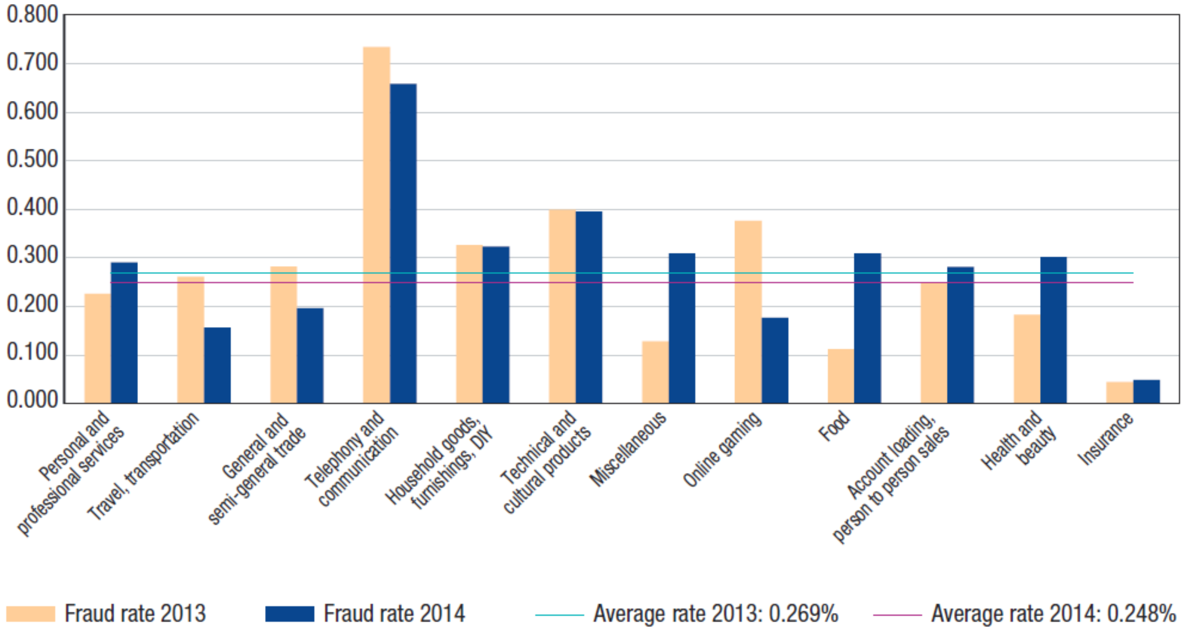
5 France 🇫🇷

France is the fourth largest country in terms of e-commerce sales; 49 percent of French merchants maintain an online presence.

5.1 Evolving Fraud Rates

The fraud rate for Internet card payment transactions in France has recently declined, reflecting efforts by issuers and e-merchants to make such transactions more secure. The fraud rate for all CNP transactions decreased to 0.248 percent from 0.269 percent in 2013. However, with sustained growth in e-commerce, the amount of CNP fraud in that sector continues to rise. CNP payments still account for the lion's share of fraud by value (66.5 percent in 2014) while representing only 11.6 percent of the total value of payments.

As Figure 14 illustrates, fraud rates differ by market sector. Certain market sectors, such as telephony and communication, experience higher fraud rates for online transactions, emphasizing the need for increased vigilance in these markets.



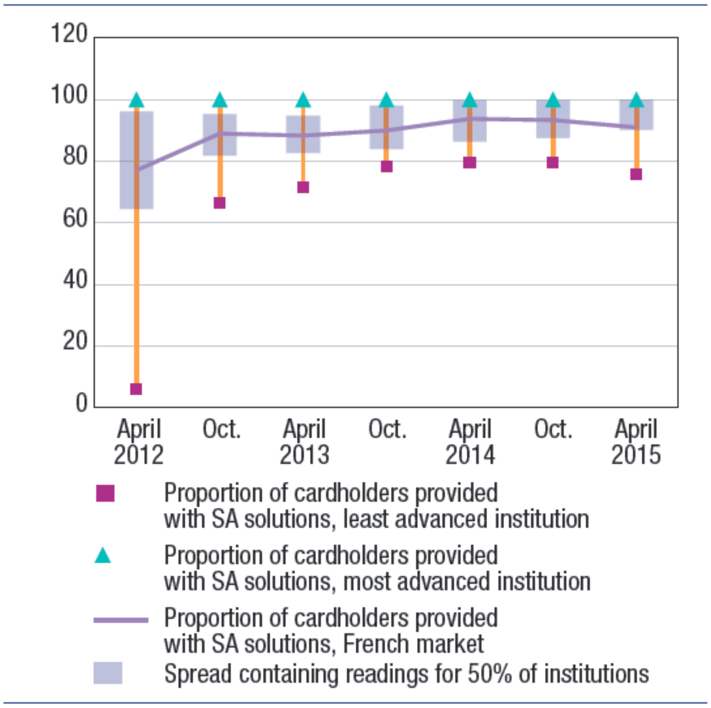
Source: Annual Report of the Observatory for Payment Card Security 2014

Figure 14. Domestic Fraud Rate in CNP Transactions by Market Sector (%)

Fraud rates for CNP payments made using French cards both within and outside of the SEPA remain high (0.910 percent and 0.960 percent, respectively), reflecting the fact that improved protection for CNP transactions on French Web sites has prompted criminals to shift their focus to international targets. The guidelines issued by the EBA on the introduction of strong customer authentication solutions (Section 3.3) should combat CNP payment fraud more effectively within the SEPA.

5.2 Authentication Methods and Fraud Detection Tools

As of April 30, 2015, over 90 percent of cardholders have cards that offer strong authentication solutions, an increase from 70 percent of cardholders three years ago (Figure 15). The rate is close to 100 percent among cardholders who actually carried out an online payment transaction in the last six months. The most prevalent authentication solution is to send an OTP by text message.



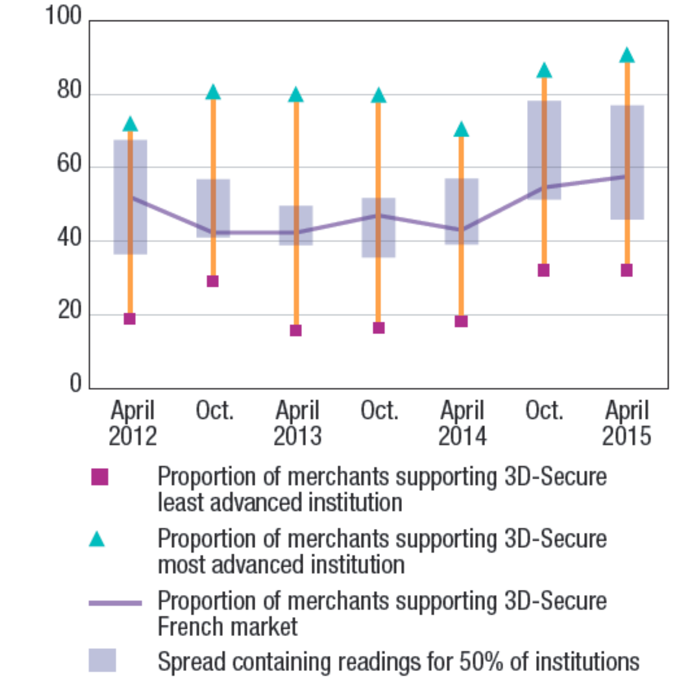
Source: Observatory for Payment Card Security

Figure 15. Distribution of Cardholders Provided with Strong Authentication Solutions (%)

Adoption of strong authentication by e-merchants now stands at close to 60 percent (Figure 16), substantially higher than the 43 percent reported in 2013, chiefly owing to the adoption of 3DS by smaller e-merchants and the ability to activate authentication based on risk analysis.

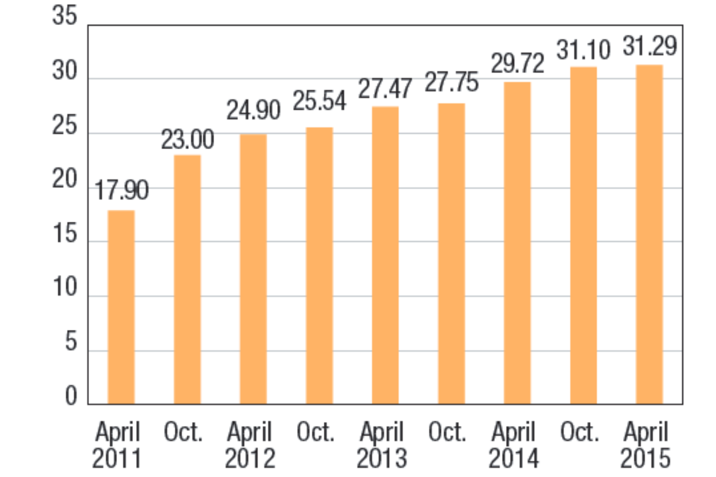
The value of authenticated transactions as a share of all transactions increased from 29.7 percent to 31.3 percent over the course of one year (Figure 17). This increase contributed to the decrease in the fraud rate for CNP payments in 2014.

It is interesting to note that the failure rate for authenticated transactions remains on a par with the failure rate for non-authenticated transactions (Figure 18), indicating there are no obstacles to the adoption of this solution by e-merchants. Moreover, the spread in failure rates across the institutions surveyed has narrowed sharply, reflecting a better understanding of strong authentication solutions among cardholders.



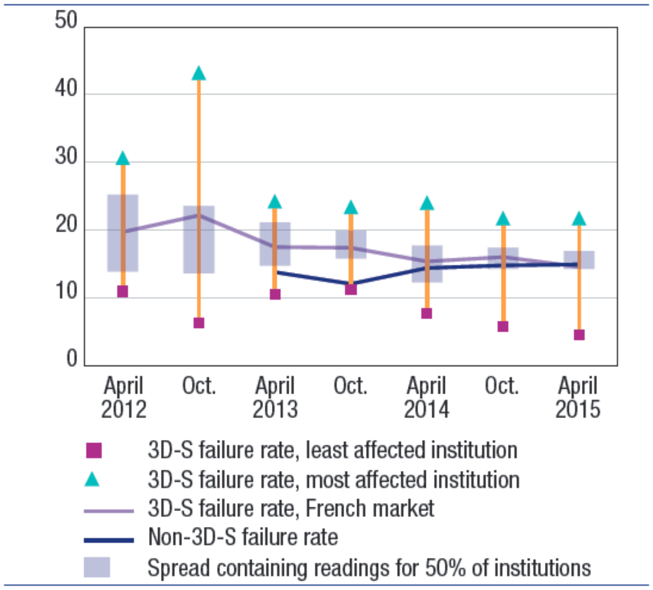
Source: Observatory for Payment Card Security

Figure 16. Adoption of 3DS by E-merchants (%)



Source: Observatory for Payment Card Security

Figure 17. Percentage of Online Payments Protected by 3DS (Value Terms)



Source: Observatory for Payment Card Security

Figure 18. Distribution of 3DS Failure Rates (%)

Another authentication method that is often mentioned is the use of biometric techniques. Use of biometrics in France is strictly regulated by the Data Privacy Act. An authorization application must be filed with the French Data Protection Authority (CNIL) before such methods can be employed with payment solutions. The trials of biometric solutions in France as reported by the Observatory for Payment Card Security 2014 Annual Report are primarily intended to test user-friendliness. Before large-scale deployment can take place, it will be important to analyze the risks created by biometric authentication to ensure that these solutions provide a level of protection that is at least equivalent to what is offered by current techniques (e.g., PIN and smart card for card-present payments, OTP for CNP payments).

Furthermore, given the shortage of information available to assess the security level of biometric solutions in comparison to current technologies, the Observatory for Payment Card Security[8] has called on participants involved in trials to establish security standards for evaluating proposed solutions. These standards would cover assessment of all components and parameters, including the equipment used to sense and process biometric information, algorithms, and use cases. In view of the inherent limitations of biometrics and the immaturity of applicable security evaluation techniques, the Observatory continues to recommend maintaining an alternative authentication solution.

[8] The Observatoire de la sécurité des cartes de paiement (Observatory for Payment Card Security – hereinafter the Observatory), referred to in section I of Article L141-4 of France's Monetary and Financial Code, was created by the Everyday Security Act 2001-1062 of 15 November 2001. The Observatory is meant to promote information-sharing and consultation between all parties concerned by the smooth operation and security of card payment schemes (consumers, merchants, issuers and public authorities).

5.3 Legislation

France is both adopting the PSD2 (Section 3.3) and considering additional legislation.

The Banque de France (French National Bank) has pursued efforts to raise awareness about fraud prevention among e-merchants and their PSPs, building on steps taken in 2013 at the Observatory's request. The bank also introduced a procedure that allows payment chain participants to report production incidents connected to cardholder authentication. This information will be used to identify weaknesses in deployed solutions that potentially reduce the conversion rate of authenticated payments.

The Observatory regularly monitors fraud in Internet card payments as well as the anti-fraud methods deployed by participants in the payment chain. In 2014, the Observatory noted that the majority of the large e-merchants it contacted had action plans to curb fraud rates, particularly using strong cardholder authentication mechanisms. The existence of these plans should help in implementing European regulatory changes intended to enhance the security of Internet payments.

A National Conference on Payments, organized by the Minister for Finance and Public Accounts and the Minister for the Economy, Industry and Digital Technology, was held on June 2, 2015. The purpose of the event was to outline a national strategy to modernize payment instruments and meet user needs for speed, security, and accessibility, promote the use of innovative payment instruments, and foster a competitive national payments industry. The conference clearly identified widespread rollout of strong customer authentication solutions for CNP payments as part of the process of developing straightforward, secure means of payment to respond to strong growth in online commerce and the substantial proportion of card payment fraud attributable to CNP payments.

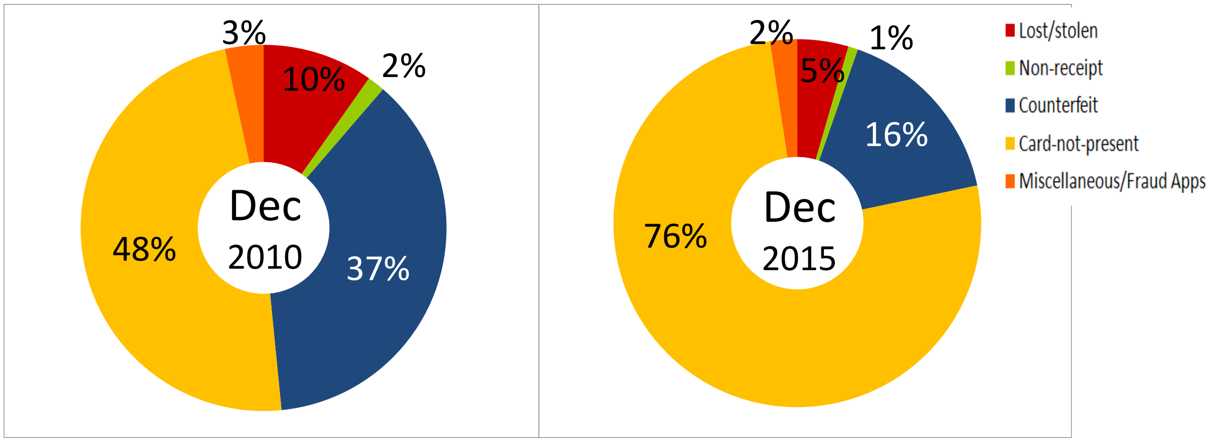
Proposals put forward before the conference recommend encouraging initiatives supporting adoption of strong authentication by increasing communication with and education of merchants and users. It was also proposed to support "second generation" strong authentication solutions, including biometric techniques and methods that do not require e-merchants to have special equipment. These new solutions are intended, among other things, to address e-merchant concerns, particularly regarding the sharp growth in payments made by mobile phone and the lack of suitable solutions for this type of transaction. The solutions that establish themselves will undoubtedly be those that marry ease of use and security with a viable business model.

6 Canada

Canada is the fifth largest country in terms of e-commerce sales. While it is natural to assume that Canada is the country most similar to the U.S., it is very different in terms of its selection of technologies (e.g., chip-and-PIN as opposed to chip-and-signature) and its banking infrastructure (one debit network).

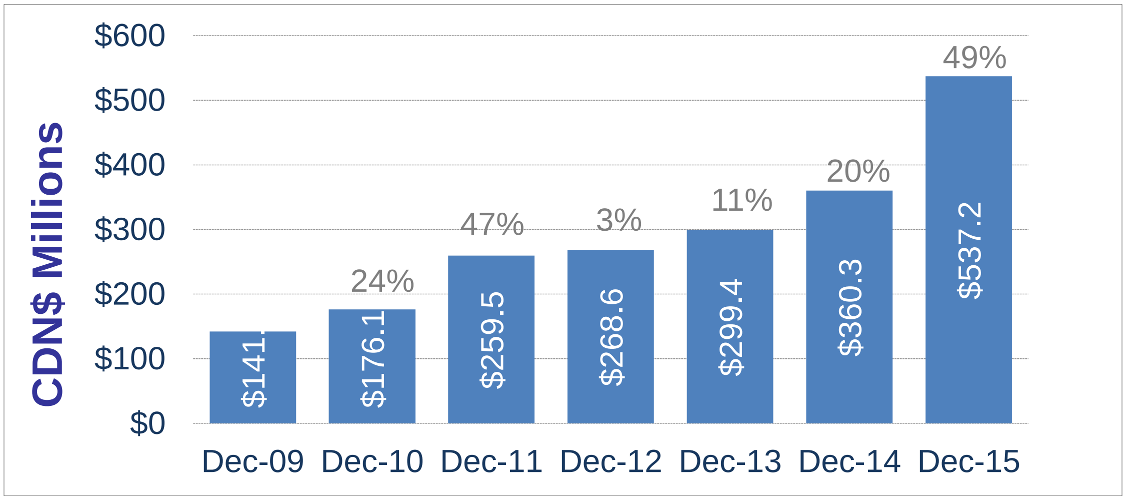
6.1 Evolving Fraud Rates

Figure 19 illustrates the change in overall fraud rates on Canadian cards between 2010–2015. Canada has experienced the expected increase in CNP fraud during this period, driven by substantial growth in e-commerce transactions and an increased focus by fraudsters on CNP transactions.



Source: Canadian Bankers Association Payment Card Partners Working Group (VISA Canada; MasterCard Canada; American Express Canada). Data for period ending December 2015.

Figure 19. Card Fraud on Canadian Cards, 2010–2015



Source: Canadian Bankers Association Payment Card Partners Working Group (VISA Canada; MasterCard Canada; American Express Canada). Data for period ending December 2015.

Figure 20. Card-Not-Present Fraud on Canadian Cards, 2009-2015

As illustrated in Figure 19 and Figure 20, Canada has seen growth in CNP fraud from 2009 to 2015, driven by substantial growth in CNP transactions and an increased focus by fraudsters on the CNP channel. From December 2010 to December 2015, CNP fraud increased by 205 percent and accounted for 76 percent of all fraud in 2015.

Figure 20 illustrates the increasing value of CNP fraud for the 12 months ending in December between 2009 and 2015. The value of CNP fraud increased very little between 2011 and 2014 (rising by only 3 percent between 2011 and 2012, for example). It then increased by almost 50 percent in 2015.

As is true in other regions, fraud is higher in cross-border transactions, highlighting the need for global tools and solutions.

6.2 Authentication Methods and Fraud Detection Tools

According to industry sources and although many retailers protect against fraud using tools such as CVN, address verification service (AVS), and 3DS, CNP transactions remain an area of weakness. One contributing factor is that not all merchants and issuers use tools. Some merchants who sell digital goods (such as software) do not use any CNP fraud prevention measures because, unlike merchants who sell physical goods, their potential loss is minor compared to the cost of implementing the tools.

In addition, the underutilization of CNP fraud prevention tools means that not all transactions are subject to the same type of verification, which weakens the system. Some merchants who deploy 3DS use a risk-based approach to authentication—only risky transactions are routed through 3DS—while low risk transactions are not subject to additional authentication.

The trend is to migrate from static-data solutions to dynamic, risk-based authentication, both to eliminate cardholder friction (e.g., no password to remember) and to improve the online shopping experience. Such solutions involve using tools to track and verify data elements such as IP address, geolocation, and device ID; another possible solution is a dynamic CVV2. The goal is to introduce a dynamic element to the CNP channel; it is anticipated that incorporating a dynamic element would improve fraud prevention for CNP transactions much as EMV has for card-present transactions.

6.3 Legislation

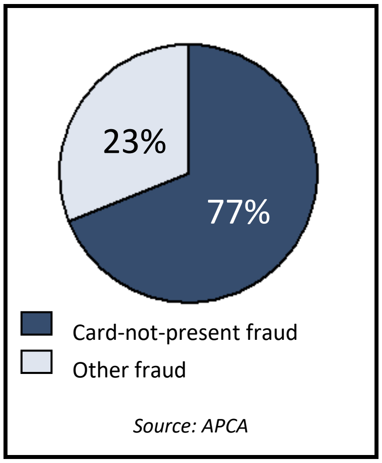
The U.S. Payments Forum does not have information on legislation in Canada at the time of publication.

7 Australia

Australia is the ninth largest country in terms of e-commerce sales, with 22 percent of merchants having an online presence.

7.1 Evolving Fraud Rates

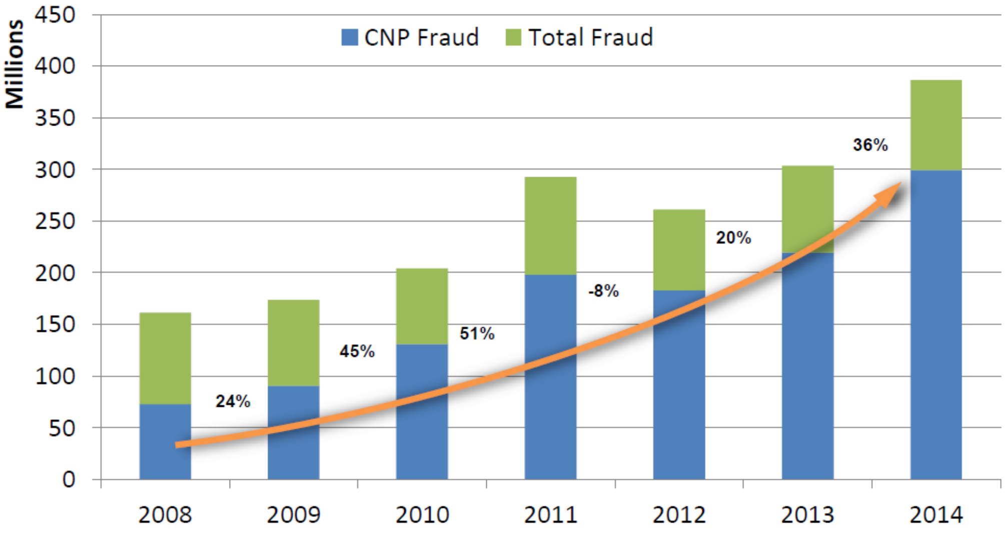
In 2014, card fraud in Australia totaled $300 million (AUS) (an increase of 16 percent from 2012), of which CNP fraud accounted for 77 percent (Figure 21).



Source: APCA

Figure 21. CNP vs. Other Card Fraud in Australia in 2014

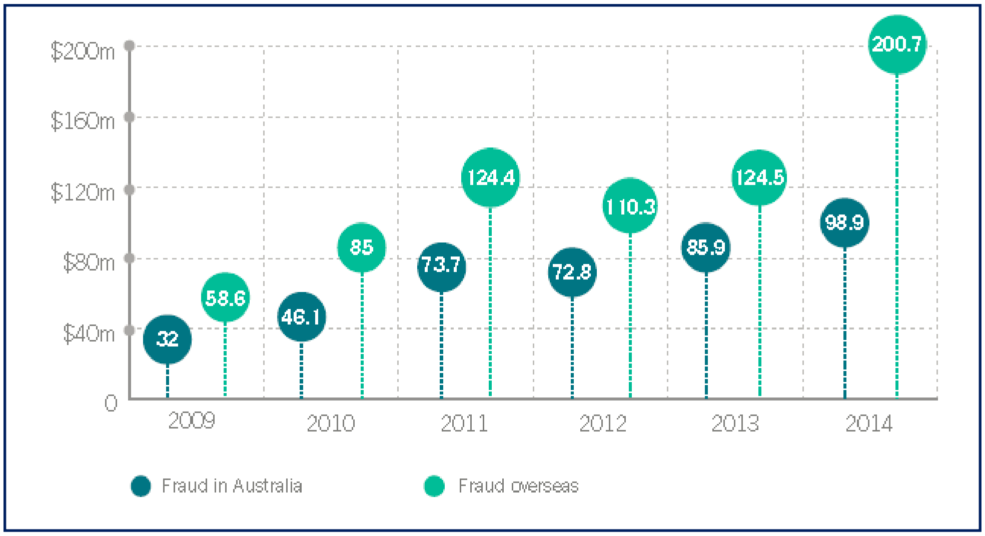
Figure 22 illustrates the trend in Australian card fraud from 2008–2014. As Australia's migration to EMV progressed, year-to-year growth of CNP fraud continued to rise, accounting for a larger share of the total card fraud. However, 2011 was somewhat of an anomaly as CNP fraud perpetrated overseas declined, leading to a one-year drop in total CNP fraud before rising again the following year.



Sources: APCA

Figure 22. Australian Card Fraud, 2008–2014

Payments industry data for 2014 show that fraud on Australian payment cards continues to increase, particularly for CNP transactions, reflecting the global trend in online payment card fraud. In 2014, CNP fraud on Australian cards rose 42 percent, to $299.5 million (AUS), with two-thirds of this amount ($200.7 million) a result of overseas transactions (Figure 23).



Source: APCA, "2015 Australian Payments Fraud Details and Data"

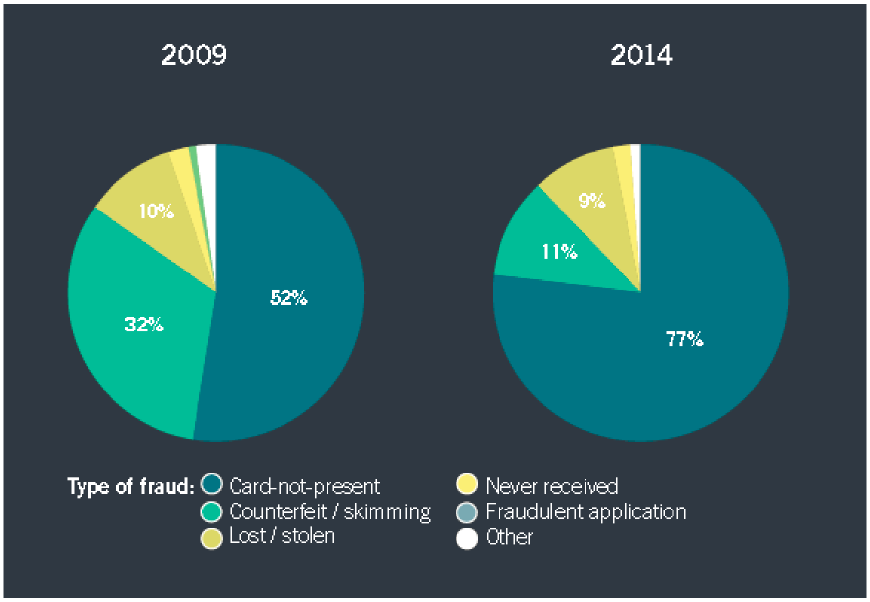
Figure 23. Value of CNP Fraud on Australian Cards, 2009–2014

This phenomenon is partially attributable to the growing popularity of payment card use for CNP transactions. According to a study of consumer payments by the Reserve Bank of Australia[9], card purchases made online, by telephone, or by mail order represent nearly 25 percent of the total value of debit card purchases and about 40 percent of credit card purchases.

Part of the challenge currently faced by the industry is the amount of card data that has recently been stolen through large data breaches, which can lead to an increase in CNP fraud in Australia and overseas. As a result, industry measures to reduce the opportunity for such breaches, particularly through tokenization and stricter reinforcement of PCI DSS standards at merchants and service providers, have accelerated.

Fraud continues to migrate from the card-present environment to the CNP environment, as illustrated by the changing proportions of different types of card fraud (Figure 24). In 2009, CNP fraud constituted 52 percent of total Australian card fraud, compared to 77 percent in 2014.

[9] *The Changing Way We Pay: Trends in Consumer Payments*, summary results from the 2013 tri-annual consumer payment survey conducted by the Reserve Bank of Australia



Source: APCA "2015 Australian Payments Fraud Details and Data"

Figure 24. Types of Card Fraud in Australia, 2009–2014

7.2 Authentication Methods and Fraud Detection Tools

The Australian payments industry has implemented several measures to help prevent CNP fraud:

- Requiring additional information, such as the three- or four-digit code written on the card itself, to verify that the card details are valid and that the person providing them is the genuine cardholder
- Using stronger online authentication tools, such as American Express SafeKey®, Discover ProtectBuy, MasterCard SecureCode®, Verified by Visa®
- Using fraud detection tools to identify risky or unusual purchases made with a card
- Requiring merchants to comply with the PCI DSS standards to strengthen data security and reduce the risk of card details being stolen

The industry is also undertaking a major structural upgrade to implement tokenization. Tokenization, which replaces sensitive information, such as a card number, with a non-sensitive replacement value, is expected to significantly reduce CNP fraud, since it will make it more difficult for criminals to steal and make use of card details.

7.3 Legislation

That the Australian government is increasing its focus on protecting against cyber-attacks (such as the capture of card data) is exemplified by the establishment of the Australian Cyber Security Centre and the Serious Financial Crime Taskforce. The government also provides advice on protecting personal and financial information online, such as Stay Smart Online and ScamWatch, and law enforcement has set up the Australian Cybercrime Online Reporting Network for people to report instances of cybercrime securely.

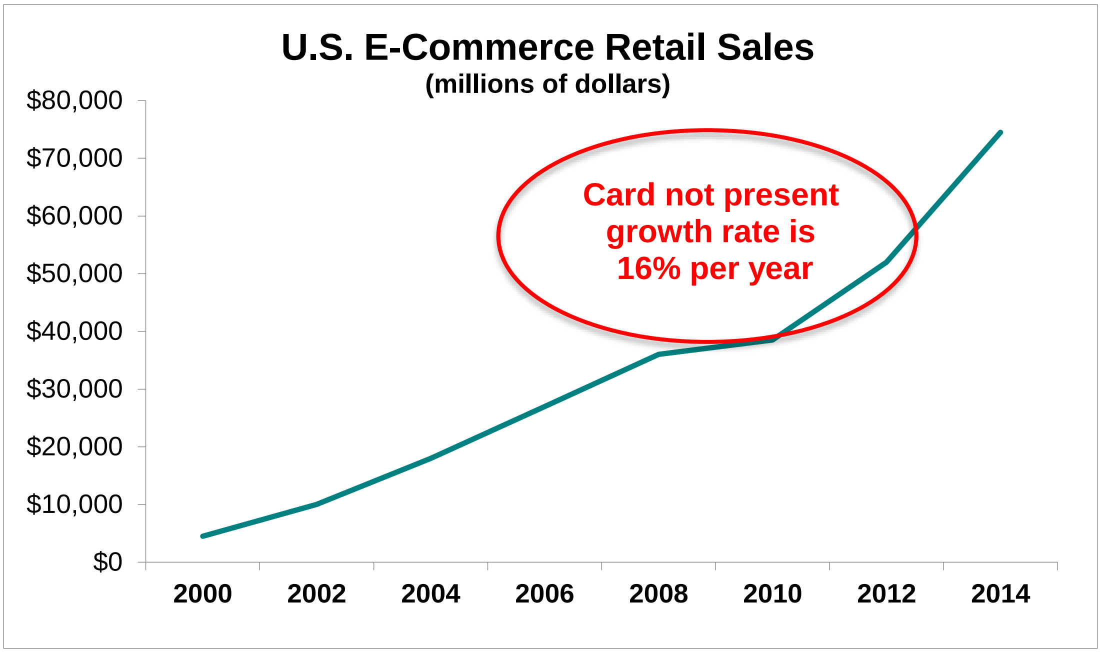
In response to the increasing threat of fraud, the Reserve Bank of Australia requested that the Australian Payments Council (APCA) lead an industry review on how best to address online security. The APCA coordinated an industry recommendation to mandate the implementation of 3DS v2, following a risk-based approach, over the next four years. In January 2016, the APCA applied to the Australian Competition and Consumer Commission (ACCC) for authorization to mandate 3DS. In May, the ACCC released a draft determination proposing not to grant authorization, citing the following concerns about the request:

- Mandates a specific solution
- Mandates a proprietary solution as opposed to generic fraud mitigation
- Poses a competitive disadvantage for new entrants without access to the tool
- Potentially constrains competition and innovation for new fraud tools
- Potentially imposes costs to merchants

The APCA therefore withdrew its application and plans to facilitate a working group to propose alternate options to be funded by issuers and acquirers (not operator merchants). The working group will analyze the changing fraud landscape, audit all approaches to address the issue, and make recommendations, with results planned in 2016. However, currently there is no mandate for strong authentication to reduce CNP fraud.

8 United States of America

The U.S. is the leading e-commerce country in the world, with the largest spend per person and with 77 percent of merchants selling online. The percentage of CNP fraud (out of total fraud) in the U.S. is currently lower than in other countries, but the recent migration to EMV, combined with a 16 percent per year increase in e-commerce (Figure 25) is expected to contribute to a surge in CNP fraud.



Source: U.S. Dept. of Commerce: Census Bureau.

Figure 25. Growth in U.S. E-commerce Retail Sales

A recent report published by Forter, a fraud prevention firm, and PYMNTS, a media company focused on the payments industry, reveals that cyber fraud has been soaring since October 2015, when the migration to EMV began in earnest.[10] An 11 percent increase in fraud attacks since the third quarter of 2015 confirms that fraudsters are indeed refocusing on online businesses. In Q4 of 2015, there were 27 attacks for every 1,000 e-commerce transactions conducted, with $5 of every $100 of sales at risk of a fraud attack. In Q1 of that same year, the numbers were, respectively, three attacks and $2. The attack rate more than tripled between Q1 2015 and Q4 2015 (percentage of transactions subject to fraud attacks in Q4 2015 compared to Q1 2015).

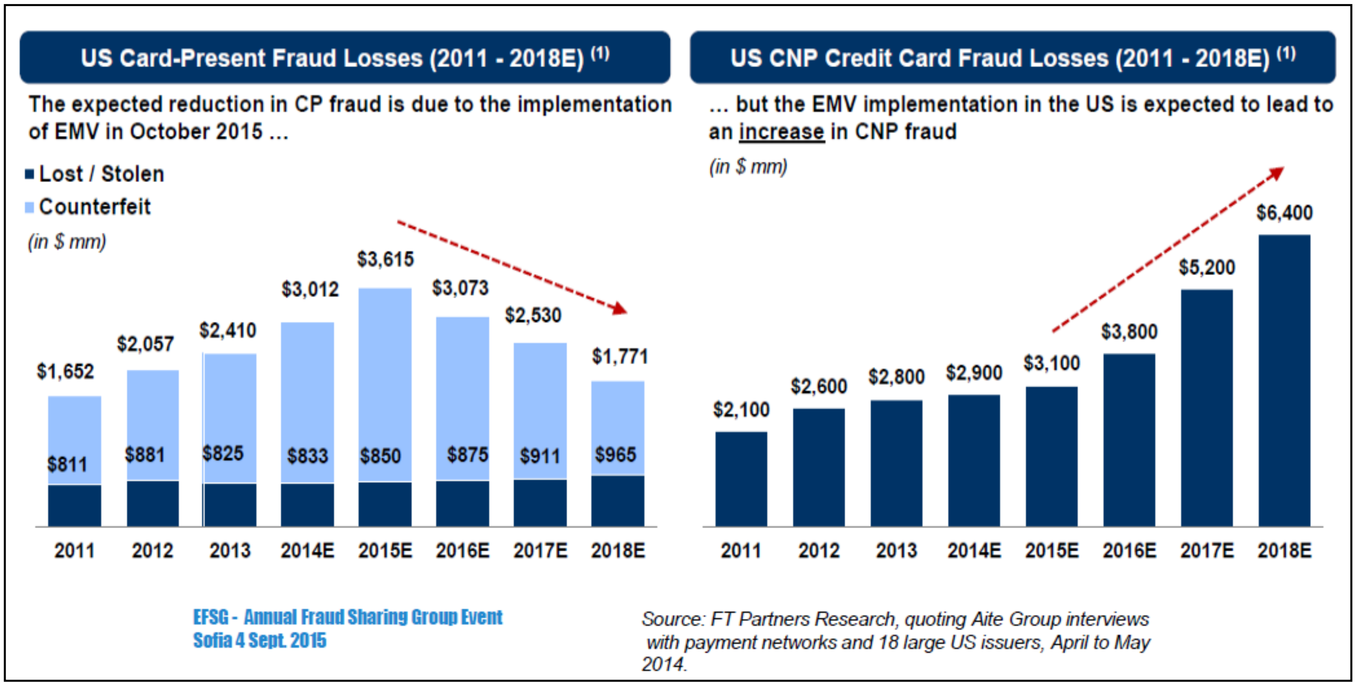
The 2016 report, "3-D Secure: The Force for CNP Fraud Prevention Awakens," prepared for RSA by Boston-based researcher Aite Group, forecasted that online fraud in the U.S. would grow from $2.8 billion in 2014 to $7.2 billion in 2020.

8.1 Evolving Fraud Rates

In 2012, CNP fraud represented 40 percent of total U.S. card fraud. This number increased to 45 percent in 2014.

[10] Forter®, *Global Fraud Attack Index™:Q1 2015-Q1 2016 Data*, http://info.forter.com/global-fraud-attack-index-q1-2016

Figure 26 illustrates Forter's and Aite Group's estimated impact on card-present and CNP fraud after the implementation of EMV.



US Card-Present Fraud Losses (2011 - 2018E) (1)

The expected reduction in CP fraud is due to the implementation of EMV in October 2015 …

US CNP Credit Card Fraud Losses (2011 - 2018E) (1)

… but the EMV implementation in the US is expected to lead to an increase in CNP fraud

EFSG - Annual Fraud Sharing Group Event
Sofia 4 Sept. 2015

Source: FT Partners Research, quoting Aite Group interviews with payment networks and 18 large US issuers, April to May 2014.

Figure 26. Comparison of Card-Present and CNP Fraud Losses in the U.S., 2011–2018

8.2 Authentication Methods and Fraud Detection Tools

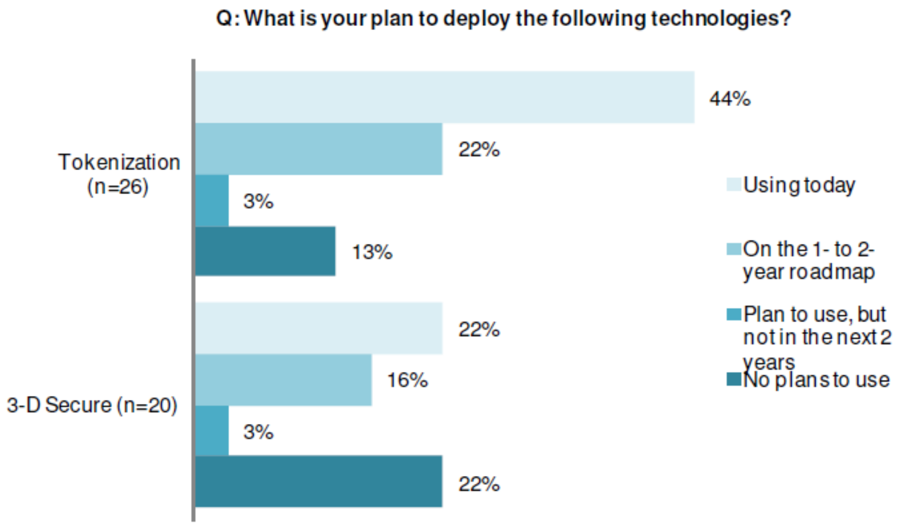
In addition to the global tools described in earlier sections for detecting fraud, U.S. e-merchants and issuers are considering (and in some cases implementing) tokenization, behavioral analytics, and 3DS.

When a recent Aite Group survey[11] inquired about the perceived effectiveness of tokenization and behavioral analytics, merchant reaction was quite positive: 50 percent believe that tokenization has a high or very high impact on fraud and data security issues, and 62 percent believe that behavioral analytics have high or very high impact. A total of 28 percent of the merchants surveyed believe that 3DS has a moderate or high impact on fraud and data security issues, while 47 percent of respondents were undecided.

When asked about the use of technologies such as tokenization and 3DS, 44 percent of the merchants surveyed claim they currently use tokenization in at least one of their channels, and another 22 percent plan to introduce tokenization within the next one to two years. A total of 22 percent of the merchants surveyed use 3DS, while another 16 percent plan to deploy it within the next one to two years (Figure 27). These results actually represent a significant change in attitudes toward 3DS, resulting from the introduction of risk-based authentication and other enhancements to the user experience.[12] (Moving

[11] *Card-Not-Present Fraud in a Post-EMV Environment: Combating the Fraud Spike*, June 2014, http://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf

away from static passwords within 3DS, which has recently been suggested, would also support this change in attitude.)



Source: Aite Group survey of 36 merchant fraud executives, March to May 2014.

Figure 27. Merchant Adoption of Security Solutions

A majority of the issuers surveyed by Aite Group either have already deployed risk-based authentication to support 3DS or plan to do so within the next year. The combination of rising CNP fraud and an improved user experience should continue to make 3DS more attractive.

8.3 Legislation

At this time, there is no specific U.S. legislation governing CNP fraud; rather, industry stakeholders set standards and allocate liability for CNP fraud through individual network rules and applicable merchant/acquirer contractual relationships. However, the Federal Financial Institutions Examination Council (FFIEC) has released security guidance[13] for mobile banking and payments that its examiners will now use in their assessments of financial institutions. Financial institutions that offer mobile financial services such as mobile payments will be tested against this guidance.

[13] https://www.ffiec.gov/press/PDF/FFIEC_booklet_Appendix_E_Mobile_Financial_Services.PDF

9 Conclusion

As is evidenced by the countries and regions examined in this white paper, CNP fraud is currently the most prevalent type of fraud reported in countries that have migrated to EMV, and it continues to increase. In an effort to curb CNP fraud, many of these countries have deployed various fraud prevention tools, such as 3D-Secure and device fingerprinting, which have proven to be effective. However, many countries report that CNP fraud continues to increase, because of the rapid growth of Internet sales and because fraud prevention tools have not been fully adopted and implemented by all stakeholders.[14]

To reduce exposure to CNP fraud, merchants, acquirers, and financial institutions must work together to secure all of the sensitive data elements handled during transaction lifecycles. No single security mechanism can protect against all possible fraud scenarios; rather, a systematic, layered approach must be implemented to secure all transaction data.

Merchants, acquirers, and financial institutions are encouraged to regard phasing in these and other security practices as a high priority business requirement. Ideally, each stakeholder should address CNP fraud within their EMV migration strategy.

[14] A white paper published by the EMV Migration Forum explored the various authentication tools and methods available to stakeholders. For more information, see EMV Migration Forum, "Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud, Version 2," *EMV Connection*, July 2016, http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/.

10 Publication Acknowledgements

This white paper was developed by the U.S. Payments Forum Card-Not-Present Fraud Working Committee to review the status of CNP fraud around in the world in countries that have migrated or are in the process of migrating to EMV.

Publication of this document by the U.S. Payments Forum does not imply the endorsement of any of the member organizations of the Forum.

The U.S. Payments Forum wishes to thank the Card-Not-Present Fraud Working Committee members for their contributions to the white paper. Special thanks go to **Francine Dubois**, NID Security, for leading this project.

The following members participated in the development of the white paper:

- **Teresa Bryan**, Mastercard
- **Francine Dubois**, NID Security
- **Anne Hagen**, Wells Fargo
- **Mary Hughes**, Federal Reserve Bank of Minneapolis
- **Keith Koval**, UBS
- **Janet LaFrence**, Federal Reserve Bank of Minneapolis
- **Lisa Weimar**, Target
- **Amy Zirkle**, ETA

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.

11 References

Aite Group: http://aitegroup.com

Australian Payments Council: http://australianpaymentscouncil.com.au

Banque de France: https://www.banque-france.fr/en/home.html

Barclaycard Payment Security Newsletter Jan11, Issue 1, January 2011, http://www.slideshare.net/neirajones/barclaycard-payment-security-newsletter-jan11

CyberSource: http://www.cybersource.com

EMV Connection web site: http://www.emv-connection.com

Guide for the Assessment of Card Payment Schemes Against the Oversight Standards, European Central Bank, Eurosystem, February 2015. https://www.eba.europa.eu

European Forum for the Security of Retail Payments: https://www.ecb.europa.eu/paym/pol/forum/html/index.en.html

Global Fraud Attack Index™:Q1 2015-Q1 2016 Data, Forter®, http://info.forter.com/global-fraud-attack-index-q1-2016

Final Guidelines on the Security of Internet Payments, December 19, 2014 (EBA/GL/2014/12_Rev1), https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+(Guidelines+on+the+security+of+internet+payments)_Rev1

French Data Protection Authority: https://www.cnil.fr/en/french-data-protection-authority-publicly-issues-formal-notice-facebook-comply-french-data

2015 Merchant Risk Council (MRC) Global Fraud Survey, Merchant Risk Council

Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud, Version 2, *EMV Migration Forum*, July 2016, http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/

PYMNTS: http://www.pymnts.com

Reserve Bank of Australia: http://www.rba.gov.au

Scam Watch: https://www.scamwatch.gov.au

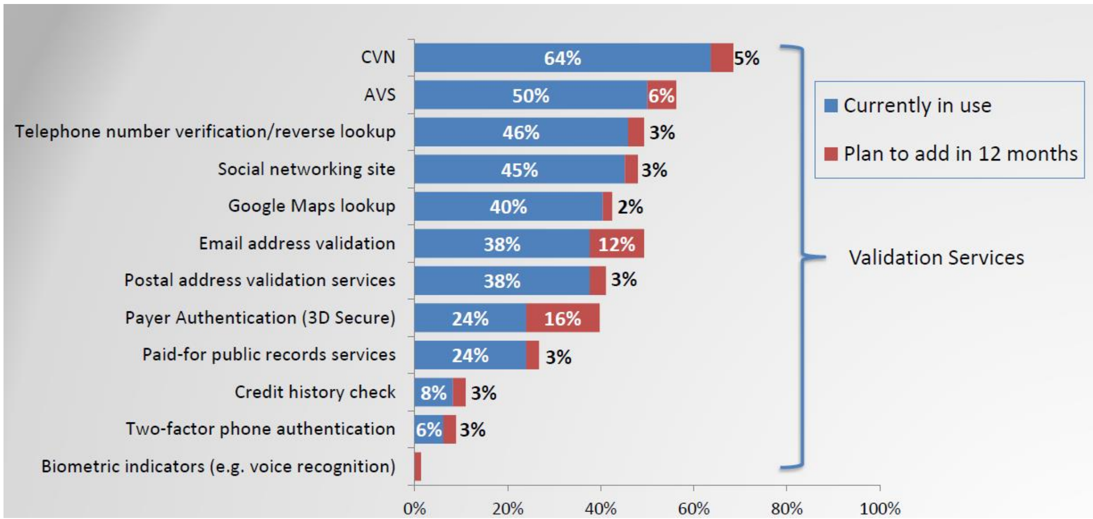
Single Euro Payments Area: http://ec.europa.eu/finance/payments/sepa/index_en.htm

Stay Smart Online: https://www.staysmartonline.gov.au

The Changing Way We Pay: Trends in Consumer Payments, summary results from the 2013 tri-annual consumer payment survey conducted by the Reserve Bank of Australia.

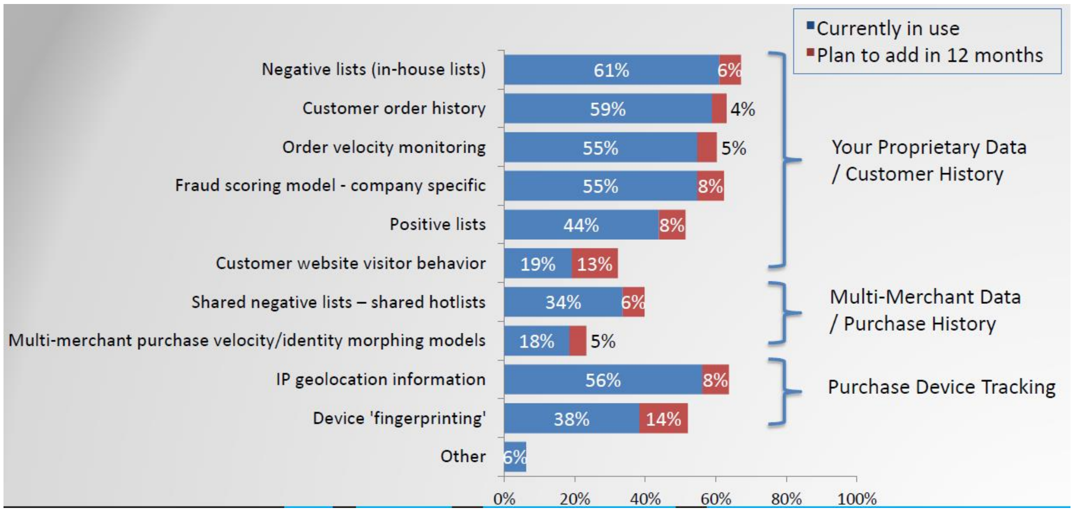
12 Appendix A: Additional Details on CNP Fraud Tools

For mobile transactions, the top fraud detection tools in use today are CVN and negative lists, while merchants are looking to add 3D-Secure and device fingerprinting.



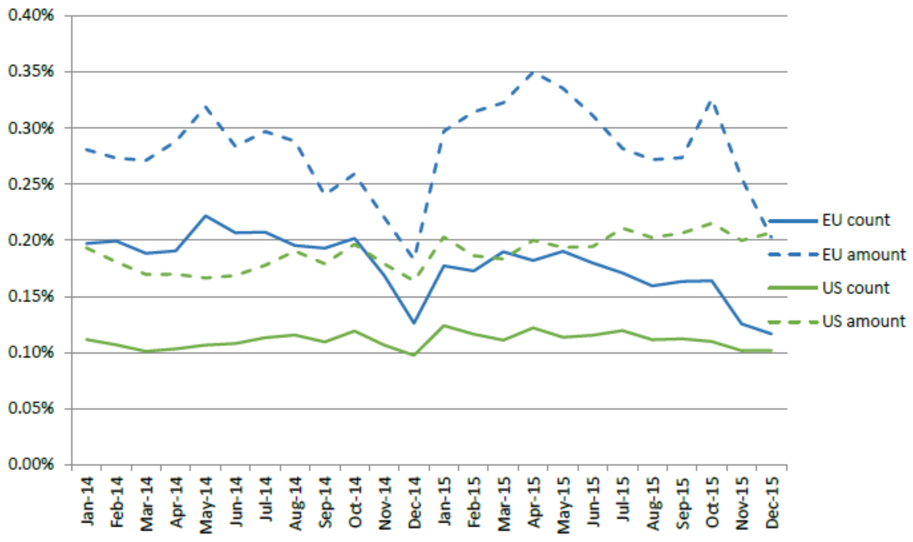
Source: MRC 2015 Global Fraud Survey Results

Figure 28. Tools Used to Protect Mobile Transactions



Source: MRC 2015 Global Fraud Survey Results

Figure 29. Tools Used to Protect Mobile Transactions



Source: MRC Vegas 2016, European Update

Figure 30. Chargeback Trends in the EU and the U.S.