

# **EMV: Lessons Learned and the U.S. Outlook**

**JUNE 2014**

**Julie Conroy**

**COMPLIMENTARY ACCESS TO THIS REPORT FOR NON-AITE GROUP  
SUBSCRIBERS HAS BEEN PROVIDED BY VISA INC.**

## TABLE OF CONTENTS

|                                       |    |
|---------------------------------------|----|
| IMPACT POINTS .....                   | 4  |
| INTRODUCTION .....                    | 5  |
| METHODOLOGY .....                     | 6  |
| LEARNING BY EXAMPLE .....             | 7  |
| UNITED KINGDOM .....                  | 7  |
| AUSTRALIA .....                       | 11 |
| BRAZIL .....                          | 15 |
| MEXICO .....                          | 16 |
| CANADA .....                          | 17 |
| THE U.S. MIGRATION .....              | 20 |
| THE COMPLEXITIES OF DEBIT .....       | 20 |
| U.S. TRAJECTORY .....                 | 21 |
| POST-EMV U.S. FRAUD ENVIRONMENT ..... | 27 |
| CONCLUSION .....                      | 29 |
| RELATED AITE GROUP RESEARCH .....     | 30 |
| ABOUT AITE GROUP .....                | 31 |
| AUTHOR INFORMATION .....              | 31 |
| CONTACT .....                         | 31 |

## LIST OF FIGURES

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| FIGURE 1: PARTICIPATING ISSUERS BY SIZE .....                                     | 6  |
| FIGURE 2: EMV'S IMPACT ON U.K. FRAUD LOSSES .....                                 | 8  |
| FIGURE 3: U.K. POS CARD FRAUD .....                                               | 9  |
| FIGURE 4: U.K. CNP FRAUD LOSSES .....                                             | 10 |
| FIGURE 5: COUNTERFEIT CREDIT CARD FRAUD ON SCHEME-ISSUED CARDS IN AUSTRALIA ..... | 12 |
| FIGURE 6: SCHEME-BASED LOST/STOLEN FRAUD IN AUSTRALIA .....                       | 13 |
| FIGURE 7: EFTPOS DEBIT CARD FRAUD IN AUSTRALIA .....                              | 13 |
| FIGURE 8: FRAUDULENT APPLICATION FRAUD IN AUSTRALIA .....                         | 14 |
| FIGURE 9: CNP FRAUD IN AUSTRALIA .....                                            | 15 |
| FIGURE 10: CANADIAN CNP AND POS CREDIT CARD FRAUD LOSSES .....                    | 18 |
| FIGURE 11: CHANGE IN CANADIAN CREDIT CARD FRAUD LOSSES .....                      | 19 |
| FIGURE 12: INTERAC FRAUD .....                                                    | 19 |
| FIGURE 13: BREAKDOWN OF U.S. CREDIT CARD FRAUD .....                              | 20 |
| FIGURE 14: PLANNED TIMELINE FOR EMV DEPLOYMENT .....                              | 22 |
| FIGURE 15: PLANNED PREFERRED CARDHOLDER VERIFICATION METHOD .....                 | 24 |
| FIGURE 16: FIS' PLANNED USE OF CONTACT CHIP VS. DUAL-INTERFACE CHIP .....         | 25 |
| FIGURE 17: PORTFOLIO PRIORITIZATION FOR EMV MIGRATION .....                       | 26 |

FIGURE 18: PROJECTED NETWORK-BRANDED CREDIT CARDS WITH EMV CAPABILITY ..... 26

FIGURE 19: PROJECTED NETWORK-BRANDED DEBIT CARDS WITH EMV CAPABILITY ..... 27

FIGURE 20: U.S. CNP CREDIT CARD FRAUD LOSSES ..... 28

FIGURE 21: U.S. CARD-PRESENT FRAUD LOSSES ..... 28

**LIST OF TABLES**

TABLE A: EMV ROLLOUTS IN SELECTED COUNTRIES..... 7

TABLE B: PERCENTAGE OF CREDIT CARD PORTFOLIO DEPLOYED BY OCTOBER 2015 ..... 23

## IMPACT POINTS

- Aite Group interviewed card executives in April and May 2014 from U.S. payment networks and 18 of the top 40 U.S. credit card issuers to chart the U.S. EMV trajectory. The participating banks collectively represent 56 % of the outstanding U.S. cardholder base. The report also sources data from a combination of public data and interviews with in-country payments experts to understand other jurisdictions' EMV experiences.
- With U.S. credit card fraud rates at 10 basis points and the uncertainty over the Durbin implications largely resolved, the U.S. EMV migration is once again moving at full speed.
- The issuance process will ramp up in Q4 2014. Eight of the 18 issuers interviewed will begin general issuance to the public by the end of 2014, and three additional issuers will begin general issuance by the end of Q1 2015.
- During the transition period, issuers will need to have nimble and robust analytics that can account for the multiple payment scenarios at the point of sale (POS) and adapt to emerging fraud patterns.
- With a proven answer to counterfeit fraud on its way, the industry will need to focus on bolstering card-not-present (CNP) controls, since CNP fraud has seen a precipitous rise in other countries after the arrival of EMV. The majority of the issuers interviewed either have invested or plan to invest in technologies such as risk-based authentication and/or tokenization for CNP transactions.
- Thirteen of the 18 issuers plan to deploy chip and signature as their preferred cardholder verification method (CVM), one plans to use chip and online PIN, and four are still undecided.
- The majority of issuers are choosing to initially issue contact-chip rather than dual-interface cards; drivers of this decision are cost, a desire to keep the initial deployment as simple as possible, and a belief that the merchant infrastructure will not yet be ready to support contactless transactions in any great scale by the liability shift date.

# INTRODUCTION

Long an outlier, the United States is finally on its way to joining the more than 80 countries around the world in upgrading its payment card security to the EMV standard, a framework for interoperable chip-based payment cards. The computer chip embedded in the card creates a dynamic code that is unique to each transaction and significantly reduces the risk of counterfeit card use at the POS.

Sharply rising counterfeit card fraud is a key reason why the business case finally works for U.S. issuers. Credit card fraud rates doubled from five basis points in 2007 to 10 basis points in 2014. Debit card fraud is also experiencing rapid rates of increase, as criminal rings prove themselves adept at skimming techniques that capture the track data as well as cardholders' PINs. The fraud problem, combined with a number of other factors, prompted the U.S. payment networks to announce a liability shift in the U.S. market, effective at the POS in October 2015.<sup>1</sup> Other contributing factors include the increasing difficulty that U.S. cardholders have in using their magnetic stripe cards overseas, the desire to accelerate an upgrade to the U.S. terminal infrastructure to facilitate NFC-based mobile payments technology, and the decreasing cost of chips and terminals.

The Durbin amendment requirement that all debit cards be able to support at least two debit networks in order to enable merchant routing choice further complicates the U.S. migration, already complex due to the vast size and highly fragmented nature of the market. The EMV specification was not designed to support this, and considerable industry discussion and debate ensued as the industry iterated its way toward a workable solution. Just as a framework for a solution was beginning to emerge in July 2013, Judge Richard Leon of the U.S. District Court dealt the migration another blow when he rejected Regulation II, the Federal Reserve's implementation of the Durbin amendment. In a sharply worded opinion, Leon stated that the dual routing provision is applicable to signature-debit as well as PIN-debit transactions.

This ruling introduced substantial uncertainty that slowed the industry's EMV migration until the high-profile Target data breach, which became public in December 2013. While EMV would not have stopped the breach, it certainly would have impeded the criminals' ability to monetize it, and the lack of EMV technology in the United States took center stage in subsequent media coverage and congressional hearings. This scrutiny, combined with a ruling by the U.S. Federal Court of Appeals striking down Judge Leon's opinion in January 2014, have re-energized the U.S. EMV migration, which once again is moving forward at full speed.

This Impact Report begins with analysis of the migratory experiences of five countries that preceded the United States in adopting EMV: the United Kingdom, Australia, Brazil, Mexico, and Canada. While each of these environments is unique, the U.S. payments industry can glean many lessons from these countries' experiences. The report then describes the U.S. path to EMV, based on interviews with top U.S. issuers and payment networks. It will conclude with a series of recommendations for U.S. issuers based on the lessons learned from other countries.

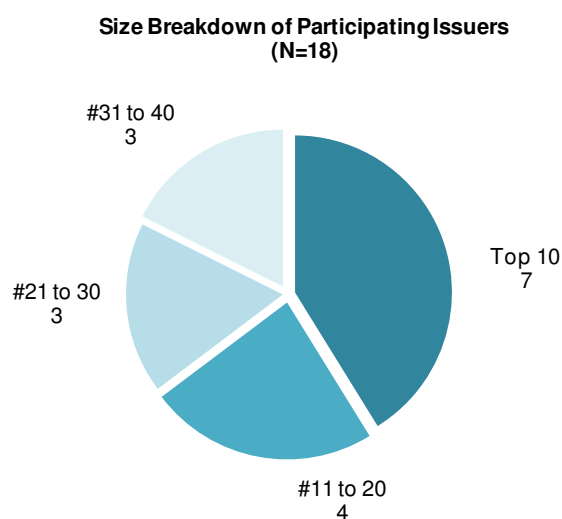
---

1. For more details on the EMV standard, see Aite Group's report *EMV: A Roadmap and Guidebook for the U.S. Market*, June 2013.

## METHODOLOGY

Aite Group interviewed 25 card executives from U.S. payment networks and 18 of the top 40 U.S. credit card issuers (Figure 1) and used a combination of public data and interviews with in-country payments experts to understand other jurisdictions' EMV experiences.

**Figure 1: Participating Issuers by Size**



*Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014*

## LEARNING BY EXAMPLE

While EMV provides a common standard that allows basic interoperability of chip-based payment cards across EMV-enabled countries, there are many different ways in which the technology has been rolled out. Each country's existing local infrastructure, migration drivers, and competitive environment all impacted the way in which EMV was rolled out as well as the results (Table A).

**Table A: EMV Rollouts in Selected Countries**

| Country          | Population (millions) | Preferred credit CVM | POS counterfeit fraud liability shift date |
|------------------|-----------------------|----------------------|--------------------------------------------|
| <b>Australia</b> | 22.7                  | Online PIN           | October 2010—Visa                          |
|                  |                       |                      | April 2012—MasterCard                      |
| <b>Brazil</b>    | 198.7                 | Offline PIN          | March 2008—MasterCard                      |
|                  |                       |                      | April 2011—Visa                            |
| <b>Canada</b>    | 34.9                  | Offline PIN          | March 2011—Visa, MasterCard                |
|                  |                       |                      | October 2012—American Express              |
|                  |                       |                      | October 2015—Discover                      |
| <b>Mexico</b>    | 120.8                 | Signature            | October 2008—MasterCard                    |
|                  |                       |                      | April 2011—Visa                            |
|                  |                       |                      | April 2015—Discover                        |
| <b>U.K.</b>      | 63.2                  | Offline PIN          | January 2005—Visa, MasterCard              |

Source: Aite Group

## UNITED KINGDOM

The United Kingdom was an EMV pioneer. The payments industry tested the concept with a small pilot in Northampton from May to September 2003, involving 600 merchants and 180,000 cards. The nationwide rollout commenced in 2004, and the liability shift took place in January 2005. The U.K.'s migration happened rapidly in comparison to other countries that have migrated to EMV. This is partly thanks to the largely consolidated U.K. banking environment, as well as the U.K. government's support of EMV education and awareness campaigns. The speed was also partially attributable to the fact that the acquirers own the majority of the POS terminals in the United Kingdom and rent the terminals to the merchants, so the acquiring banks largely bore the cost of reterminalization and passed it on to merchants in the form of increased rents.

Fraud was the clear driver for this move; thanks to the high cost of telecommunications in the United Kingdom and continental Europe, credit card authorizations took place largely offline. This meant that merchants did not place a call to the network in real-time to obtain the transaction authorization from the issuer but instead batched up the transactions and sent them to the network for settlement at the end of the day. As a result, the U.K. card fraud rate was 14 basis points in 2004, higher than the U.S. card fraud rate of five basis points during the same time period.

Because the solution initially needed to work in an environment that was primarily offline, the preferred CVM in the U.K. market was offline PIN. This represented a big change, however; the U.K. lacked a domestic debit network, so consumers had never been required to enter a PIN at the POS. The PIN was not initially enforced as the rollout began; due to attrition concerns, consumers were permitted to "fall back" to signature. This transition period lasted more than a year after the liability shift, until PIN enforcement began on February 14, 2006. A strong private-public partnership, heavily supported by the U.K. government, helped to educate consumers and merchants about the switch in a campaign dubbed "I HEART PIN." Even after the proverbial switch was flipped to begin PIN enforcement, issuers still had the latitude to permit fallback to mag stripe.

The EMV protocol, which tackles counterfeit fraud, and the PIN, which addresses lost/stolen fraud, had the desired effect and sharply curtailed counterfeit card fraud and lost/stolen fraud, both of which were at roughly the same level prior to the arrival of EMV (Figure 2).

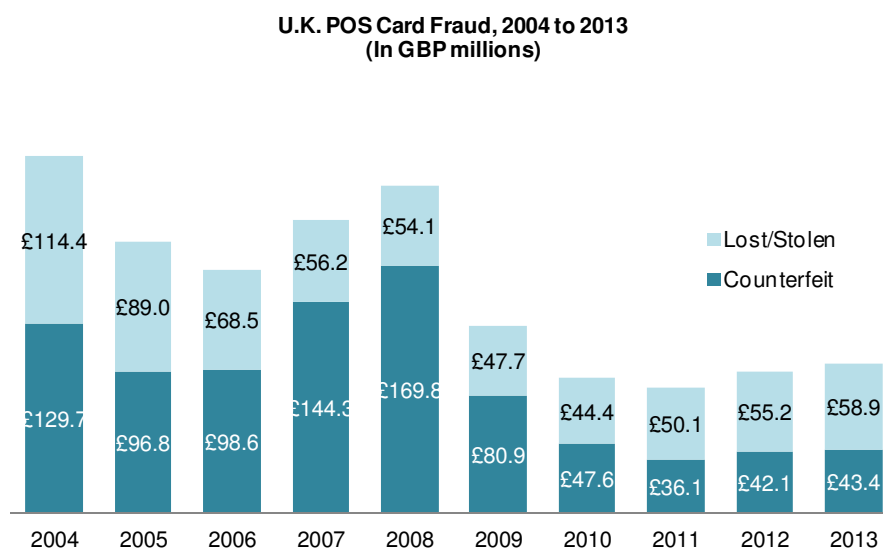
**Figure 2: EMV's Impact on U.K. Fraud Losses**



Source: Financial Fraud Action UK

Counterfeit fraud rates actually saw a spike in the initial years after the U.K. migration, as criminals leveraged stolen card data overseas in countries, such as the United States, that still relied on the mag stripe. As issuers adjusted their fraud strategies, the cross-border fraud declined, and counterfeit fraud rates dropped dramatically. The organized crime rings behind the attacks on the financial services value chain did not take this hit to their revenue lying down, however. They adjusted their tactics and found ways to skim and capture the PIN, and as a result, the U.K.'s lost/stolen fraud increased 2011 through 2013, while counterfeit card fraud increased slightly in 2012 and 2013 (Figure 3).

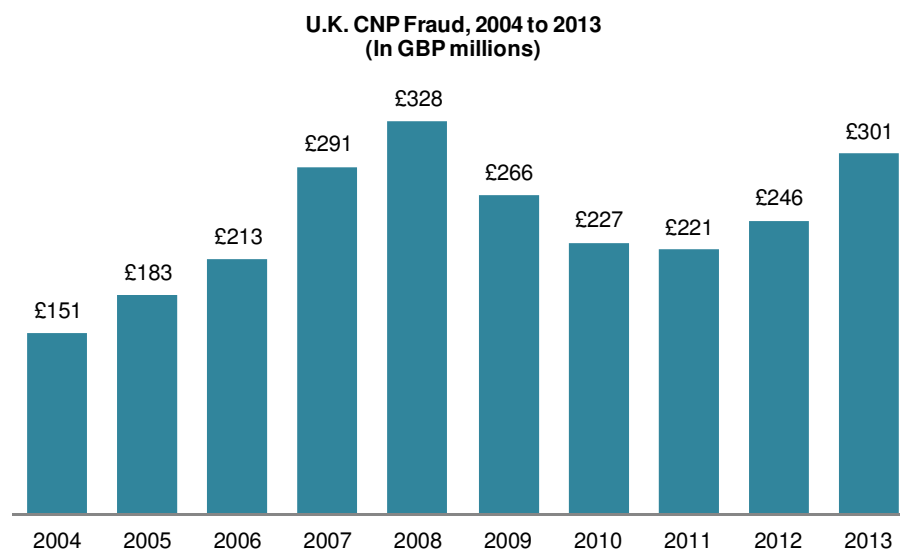
**Figure 3: U.K. POS Card Fraud**



Source: Financial Fraud Action UK

Fraud also migrated to the CNP channel; CNP fraud rose sharply in the wake of the U.K. liability shift, growing by 79% between the liability shift in 2005 and its peak in 2008. Development of more advanced fraud analytics by issuers and merchants, as well as increased use of 3-D Secure technology (i.e., MasterCard SecureCode, Verified by Visa, and American Express SafeKey) helped to rein in the rising problem, although fraudsters' corresponding adjustments are once again causing losses to rise, as shown in Figure 4.<sup>2</sup>

2. For more details on 3-D Secure, see Aite Group's report *3-D Secure: Poised to Live Long and Prosper*, March 2013.

**Figure 4: U.K. CNP Fraud Losses**

Source: Financial Fraud Action UK

Another adjustment that criminals have made just recently is to increase their attacks on the ATM channel. According to Financial Fraud Action UK, there were 7,525 incidents in the first four months of the year in 2013, compared to 2,553 in a similar period in 2012. U.K. ATM fraud losses rose by 11% to GBP16.2 million in the first half of 2013, compared to GBP14.6 million in the first half of 2012.<sup>3</sup> Techniques employed include:

- **Card theft:** A low-tech approach in which the criminal shoulder-surfs to learn a customer's PIN, then steals his or her card as he or she leaves the ATM.
- **Card entrapment:** A device is put in place to trap the card inside the ATM, and the PIN is captured via either a pinpoint camera or shoulder-surfing. Once the victim leaves, the criminal releases the device and retrieves the card.
- **Cash trapping:** A "claw" is inserted into the ATM machine to prevent the cash from being issued to the victim, trapping it inside the machine until the victim leaves.
- **Phishing:** Criminals are employing phishing techniques via email and phone calls to try to trick unwitting consumers into providing their PIN data.

3. Shane Croucher, "Cashpoint Card Fraud Leaps 200% in One Year," *International Business Times*, June 6, 2013.

## AUSTRALIA

Unlike the United Kingdom, fraud was not the primary driver of Australia's migration to EMV. When the Australian card industry held its first chip card migration forum in 2007, card fraud was just six basis points, partly because Australia's credit card authorizations take place online and in real time. Australia's migration was a proactive step; card networks and issuers initiated the migration in anticipation of future fraud and also to facilitate a payment infrastructure that was more compatible with that of the U.K., Europe, and parts of Asia. Without fraud as the driver, however, Australia's journey to EMV lacked the sense of urgency that existed in the U.K. Instead of the clockwork precision and speedy time frame that marked the U.K. migration, the Australian migration took place at a meandering pace over the course of 11 years.

Australia has a fairly concentrated banking ecosystem, with four major banks controlling much of the market: Commonwealth Bank of Australia, ANZ Bank, Westpac, and National Australia Bank. In addition to these banks, Australia has over 100 credit unions and building societies and a handful of regional banks. As of February 2014, Australia had 15.7 million credit and charge cards and 38.3 million debit cards in circulation. Debit card purchase volume was AU\$188.8 million in 2013, while credit card purchase volume for the same time period was AU\$261.9 million.<sup>4</sup> Eftpos is Australia's proprietary debit network, which enjoys a 75% market share of debit transactions. Thanks to Eftpos' strong market share, all of Australia's terminals (except for unattended terminals) were PIN-capable at the outset of the migration.

In 2003, ANZ Bank became the first Australian bank to issue EMV cards to selected portfolios. By 2007, Westpac, Commonwealth, and Macquarie had followed suit, resulting in over 1 million EMV-enabled cards in circulation. In May 2007, the Australian Payments Clearing Association (APCA), Australia's primary payments association, hosted the "Chip for Australia Implementation Forum," which was attended by financial institutions (FIs), retailers, and card networks. As an outcome of this meeting, the APCA established the Chip Payments Programme for Australia in January 2008 to provide industry-wide coordination of the migration.

The terminal upgrade costs were borne by both acquirers and merchants; acquirers own 75% of the terminals in Australia's market, while a handful of very large merchants choose to purchase their own terminals outright. To incent the migration, card networks offered a lower interchange rate for a period of time to subsidize the costs for retailers that committed to upgrade their terminals by January 2009. Another incentive came in the form of a liability shift, with fraud liability at the POS shifting to merchants that had not updated their infrastructure to support EMV. While the card networks initially set their sights on a 2009 transition, concern over merchant and consumer readiness resulted in a postponement to 2014. MasterCard's ATM and POS liability shift took place in April 2012, while Visa set its liability shift date for POS and ATM transactions at April 2013. Eftpos has yet to implement a formal liability shift but intends to migrate the network by the end of 2014.

The final milestone for the Australian migration is to phase out signature and enforce the PIN requirement. The conversion date is set for August 1, 2014, and an education campaign called PINwise is underway. The PIN won't actually be necessary for a sizeable number of transactions.

---

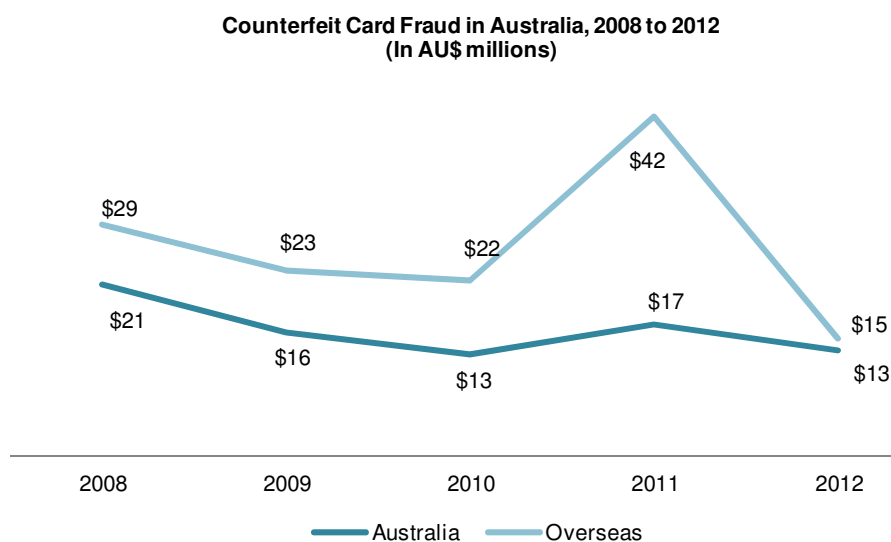
4. Reserve Bank of Australia, <http://www.rba.gov.au/statistics/by-subject.html>.

Contactless capabilities are quite advanced in Australia, and no CVM is required for contactless transactions under AU\$100.

### EMV'S IMPACT IN AUSTRALIA

Because of Australia's slower pace of migration, it is more difficult to look at a single tipping point in analyzing EMV's impact there than it is with the U.K. That said, key trends are emerging. As the penetration of EMV-enabled cards and terminals progressed in Australia, banks began to see declining counterfeit losses on network-branded cards. These gains were temporarily offset by a dramatic spike in cross-border fraud in 2011, as criminals adjusted and increased their use of Australian payment cards in non-EMV-enabled countries. Once issuers adjusted their authorization strategies, losses resumed their downward trend in 2012 (Figure 5).

**Figure 5: Counterfeit Credit Card Fraud on Scheme-Issued Cards in Australia**



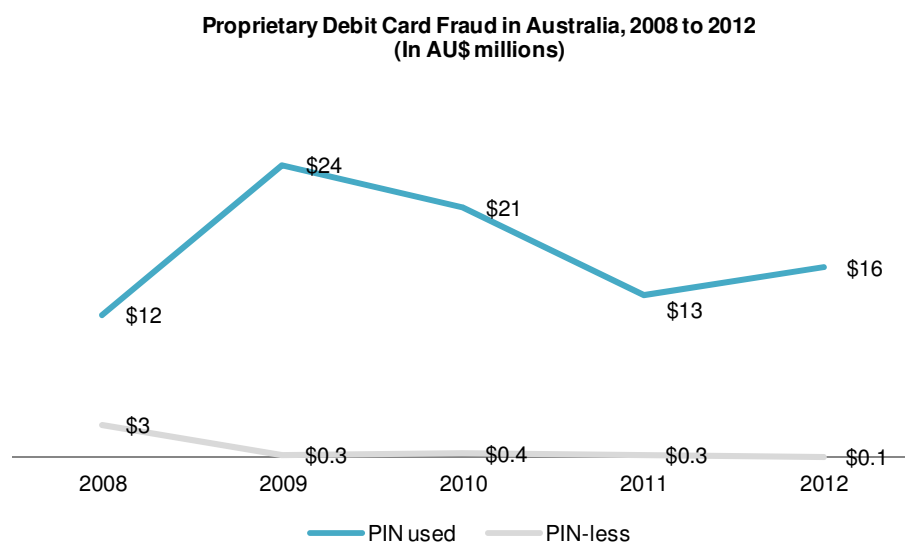
Source: Australian Payments Clearing Association

Australia has seen a slight dip in lost/stolen fraud as it has moved to transactions secured with chip-and-PIN technology, though the benefits have not been as substantial as those experienced in the United Kingdom. 2012 saw an uptick in lost/stolen fraud losses, but this trend should be reversed once PIN is strictly enforced starting in August 2014 (Figure 6).

**Figure 6: Scheme-Based Lost/Stolen Fraud in Australia**

Source: Australian Payments Clearing Association

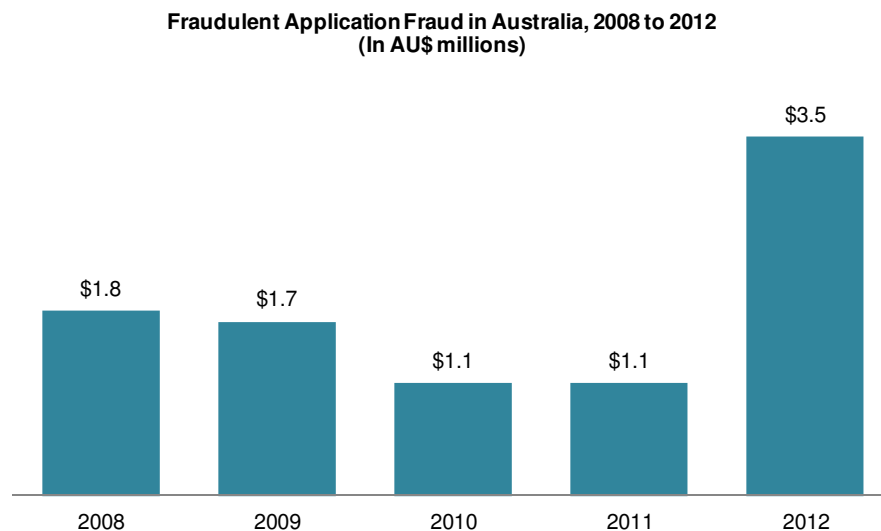
Eftpos was much later to initiate its EMV migration than the international card brands, with efforts only beginning in earnest in 2013. Likely as a result of its less fortified defenses, Eftpos has seen increasing fraud losses. Eftpos-enabled transactions experienced a dramatic spike in the wake of a series of fraud attacks on merchant terminals in 2009. Notably, a PIN was used in the vast majority of Eftpos fraudulent transactions, since it is difficult to effect an Eftpos transaction in a PIN-less environment (Figure 7).

**Figure 7: Eftpos Debit Card Fraud in Australia**

Source: Australian Payments Clearing Association

As fraud at the POS becomes more difficult to perpetrate, criminals adjust their tactics. One way they do this is by submitting applications for credit cards using fraudulent identities. 2012 saw more than a threefold increase in fraudulent application fraud (Figure 8). While one data point is not enough to confirm a trend, it does mirror the experience of large U.K. issuers that saw 450% to 800% year-over-year increases in fraudulent application losses in the wake of their migration.

**Figure 8: Fraudulent Application Fraud in Australia**



Source: Australian Payments Clearing Association

Similar to the U.K. experience, Australia has seen sharp increases in CNP fraud losses as a result of both the growing popularity of digital commerce and a more fortified POS (Figure 9). CNP losses saw a slight decline in 2012, a hopeful sign as merchants and issuers deploy increased fraud analytics to detect CNP fraud and use tools such as 3-D Secure. MasterCard made 3-D Secure a requirement for online purchases over AU\$200; Visa requires that all cards be enrolled in Verified by Visa but does not have an equivalent mandate for merchant use. There is some discussion that the Australian government may issue a mandate of its own requiring 3-D Secure.

**Figure 9: CNP Fraud in Australia**

Source: Australian Payments Clearing Association

## BRAZIL

With more than 625 million cards in circulation, Brazil is one of the largest markets to migrate to EMV. As with the United Kingdom, fraud was the principal driver of Brazil's move; at the outset of the migration, Brazil's card fraud rate exceeded 15 basis points. Statistics released by Banco Real ABN Amro illustrate the extent of the pain: Between 2004 and 2006, Banco Real's counterfeit fraud grew at a 43.5% compound annual growth rate.<sup>5</sup>

The Brazil banking sector is highly consolidated, with five large banks generating 70% of card volume. Credit cards did not take hold in Brazil until 1994, when its prolonged period of hyperinflation came to a close. As card use began to take off, so too did the fraud—by 1996, Brazil had one of the highest card fraud rates in the world. In the late 1990s, a handful of banks began a small smart-card pilot, even though at this early stage of the market smart cards cost US\$16 each, and compatible terminals cost US\$1,800.

This small pilot transitioned into a countrywide EMV rollout by the 2000s. MasterCard set its liability shift date for March 2008, while Visa's liability shift date was set for April 2011. The decision to use offline PIN as the CVM in Brazil was driven by a few factors. Most importantly, as in Europe, the telecommunications infrastructure at the inception of the migration was not robust, so a majority of transactions took place offline. Hybrid debit/credit cards are common in Brazil, making it easier to deploy PIN for credit, since the same PIN is used for both transactions. The choice of offline PIN was due to the complexity involved in upgrading the legacy processing

5. Smart Card Alliance, accessed on May 16, 2014, <http://www.smartcardalliance.org/articles/2008/05/19/latin-american-banks-moving-rapidly-to-smart-cards-news-from-smart-card-alliance-ctst-conference>.

systems to support online PIN. In addition, lost/stolen fraud was a significant problem at the time of the migration.

Acquirers were able to aggressively push the reterminalization forward, thanks to two primary factors: Terminals are largely rented from acquirers in the Brazilian market (as opposed to purchased from the manufacturer), and Visa and MasterCard had ownership stakes in two large Brazilian acquirers. In fact, upgrades to terminals outpaced card issuance: By the end of 2009, 95% of Brazil's terminals were EMV-compliant, while only 60% of scheme-based credit cards and 25% of scheme-based debit cards were EMV-enabled.<sup>6</sup> The fraud-prevention benefits of EMV were also proven in Brazil; by the end of the migration, Brazil's card fraud rate had decreased from 15 basis points to six.

Brazil also provides a good example of a country that went to market with a plain vanilla implementation of EMV and then expanded upon its capabilities as the market progressed. Many Brazilian issuers are reissuing cards with upgraded memory capacity to take advantage of the other benefits smart cards can offer, such as transit applications (Pao de Acucar), Brazil's national program that enables digital signatures using public-key encryption; advanced loyalty programs (Puntos Bancomer); and even public benefits such as meal vouchers (Alelo).

## MEXICO

Of the countries examined in this report, Mexico's card market was the least mature at the inception of its migration. This presented both opportunities and obstacles. While there was less legacy infrastructure to upgrade, Mexico lacked the fraud impetus that pushed other countries rapidly down the path to EMV. As in Brazil, the Mexican banking market is highly consolidated, with the five largest banks enjoying 90% of the credit card market share. Debit cards are issued under the Visa Electron or MasterCard brands, as well as under the domestic brand Carnet.

While Mexico is Latin America's second-largest card market, the electronification of payments is still emerging in comparison to more established card markets such as the U.K., Canada, and Brazil. Empowered by presidential decree, 15 Mexican banks created the Fund of Infrastructure of Electronic Payment Means (FIMPE) in 2004 to promote the electronification of payments in Mexico. At the outset of the initiative, 95% of Mexico's 2.38 million merchants did not have a payment terminal for card acceptance. One of FIMPE's accomplishments was to triple the installed base of credit and debit card terminals from 175,000 to 475,000 in five years. Incentives were also provided to consumers to increase the use of payment cards at the POS (including a lottery that gave away 3,100 cars).

This helped Mexico grow from a market in which only 30% of payments were non-cash in 2005 to 40% card payment penetration just four years later. Card penetration also saw rapid growth in the mid-2000s. In 2009, the number of debit cards issued by Mexican banks was 60.8 million, up from 36 million in 2005, and the number of POS terminals rose from 201,852 in 2005 to 446,792

---

6. EMV Migration Study and Market Analysis on Mexico and Brazil, Smart Card Alliance Latin America, 2009.

in 2009.<sup>7</sup> Credit card penetration grew from 12.5 million cards in 2005 to 22 million in 2009, 5% of which were EMV-capable.

The early presence of EMV in Mexico's credit card market has ensured that POS fraud was not a significant issue. CNP fraud was initially a bigger challenge, but a Mexican government directive set forth a recommendation for 3-D Secure that has been interpreted as a mandate by Mexican banks. It has been successful in decreasing Mexico's CNP fraud rate.

## CANADA

Canada is another consolidated banking market, with five large banks controlling a sizeable share of the market; Canada has another 75 smaller regional banks and 394 credit unions. There were 73.9 million Visa- and MasterCard-branded credit cards in circulation at the end of 2012.<sup>8</sup>

Similar to the United Kingdom and Brazil, fraud was the primary impetus for the Canadian migration to EMV. Canadian issuers had not invested as heavily as their U.S. counterparts in fraud analytics and made the decision to migrate to EMV in response to rising fraud. Visa Canada announced the move in June 2003, and MasterCard and Interac (Canada's proprietary debit network) followed with announcements of their own in 2005. MasterCard's roadmap largely aligned with Visa's, and the initial roadmap had the liability shift taking place in October 2010, but Visa and MasterCard jointly agreed to extend that deadline to March 2011 to provide better merchant readiness. Interac chose not to implement a liability shift but instead required all debit cards to be chip-enabled by December 2012, with ATMs upgraded by the same date.

No fallback was permitted at the ATM. Interac will discontinue support for non-EMV transactions at the POS in 2015. Any issuer that had not chip-enabled its debit portfolio by December 2012 was subject to Interac fines. American Express and Discover did not announce their roadmap until 2010 and 2012, respectively; American Express's liability shift took place in October 2012, and Discover's October 2015 liability shift aligns with its U.S. timeline.

---

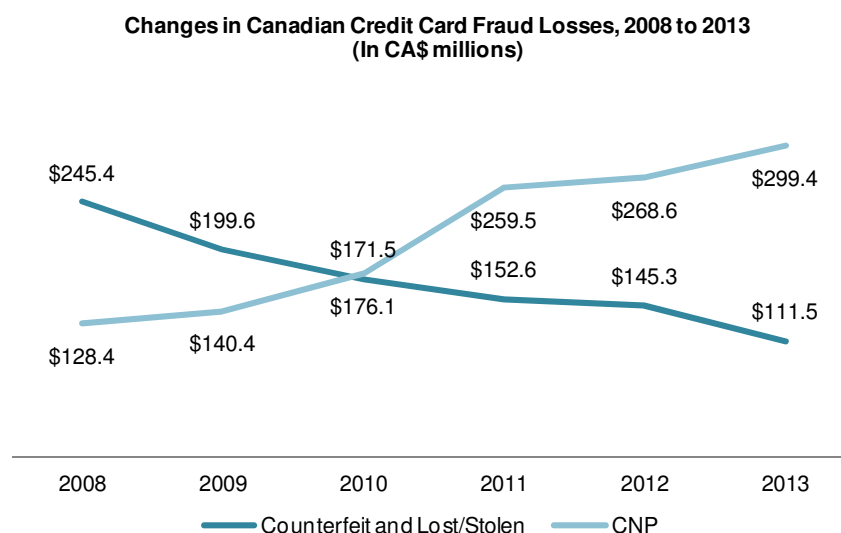
7. "Payment, Clearing, and Settlement Systems in Mexico," Bank for International Settlements, accessed on May 16, 2014, [https://www.bis.org/publ/cpss97\\_mx.pdf](https://www.bis.org/publ/cpss97_mx.pdf).

8. "Credit Card Fraud and Debit Card Fraud Statistics as of December 2013," Canadian Bankers Association, accessed on May 16, 2014, <http://www.cba.ca/en/component/content/publication/69-statistics>.

A 12-month trial took place in 2007, and full rollout began in October 2008. In a sharp departure from the approach taken in Australia and the U.K., chip-and-PIN technology was mandatory from the outset. Fallback to mag stripe was not an option, resulting in a fair amount of disruption to the consumer experience. One issuer that did not yet have the infrastructure to fully enable resetting PINs via the interactive voice response (IVR) system and ATM saw its transaction volume dip as a result of forgotten PINs and declines at the POS.

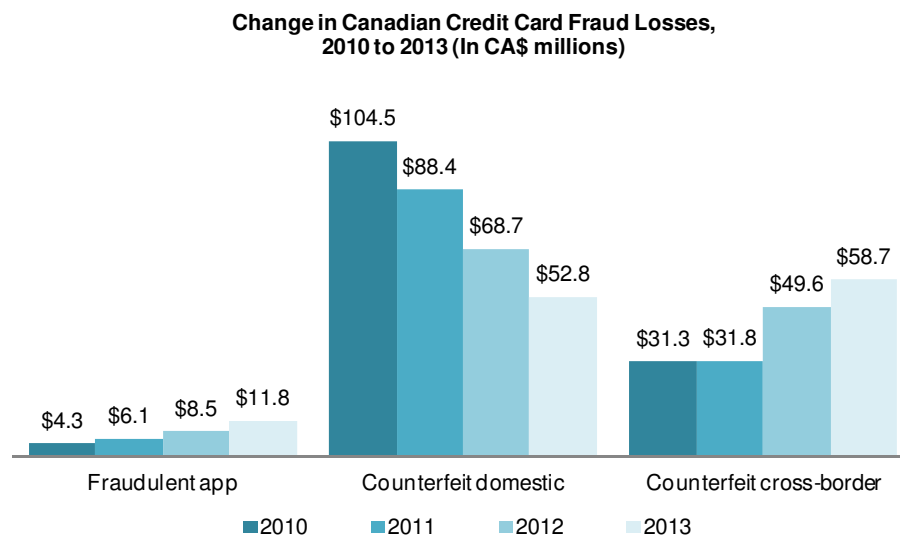
Canada's experience was consistent with that of the United Kingdom—counterfeit and lost/stolen fraud enjoyed a 54% decline from the inception of the migration in 2008 through 2013, while CNP saw a corresponding increase, jumping a whopping 133% over the same time period (Figure 10).

**Figure 10: Canadian CNP and POS Credit Card Fraud Losses**



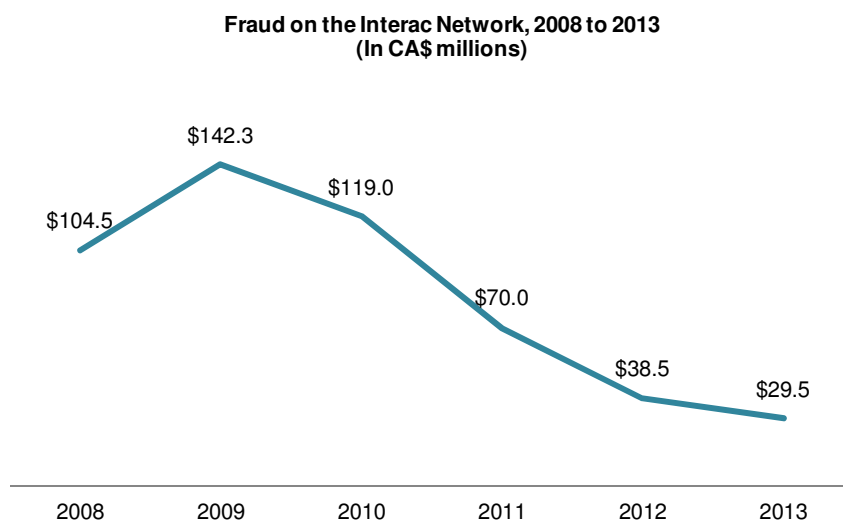
Source: Canadian Bankers Association

The Canadian Bankers Association did not begin to track cross-border counterfeit fraud separately from domestic counterfeit losses until 2010. Data collected since then show that cross-border credit card counterfeit fraud rose by 88%, while domestic counterfeit fraud decreased by 49%. Fraudulent application fraud more than doubled over the same time period as fraudsters successfully sought other means to perpetrate fraud (Figure 11).

**Figure 11: Change in Canadian Credit Card Fraud Losses**

Source: Canadian Bankers Association

Because Canadian issuers were slower to convert their debit portfolios than they were credit, debit card fraud saw an initial spike as the Canadian credit card migration began, rising 36% from 2008 to 2009. As EMV was deployed to debit, the fraud rates quickly lowered (Figure 12).

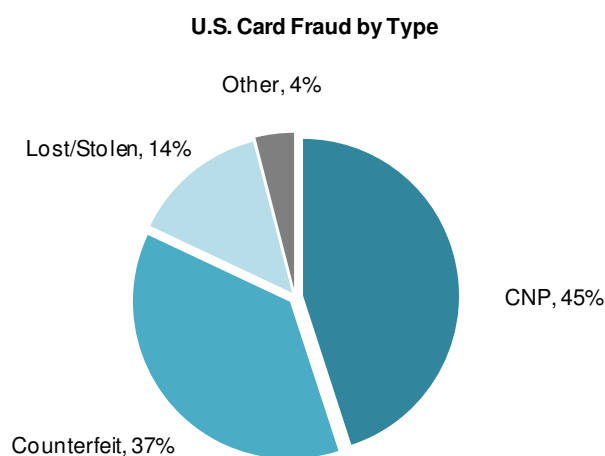
**Figure 12: Interac Fraud**

Source: Interac

## THE U.S. MIGRATION

Because the United States has lagged other countries in migrating to EMV, issuers interviewed for this report cite significant increases in U.S. counterfeit card fraud over the last two to three years. Counterfeit card fraud now represents 37% of U.S. card fraud losses, and aggregate fraud rates have doubled from five basis points in 2007 to 10 basis points in 2014 (Figure 13). For this reason and others, in early 2014 MasterCard and Visa reaffirmed their commitment to the October 2015 liability shift date.

**Figure 13: Breakdown of U.S. Credit Card Fraud**



*Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014*

## THE COMPLEXITIES OF DEBIT

The Durbin amendment requirement that all debit cards be able to support at least two debit networks and enable merchant routing choice further complicates an already complex migration. When an EMV card interfaces with a terminal, the first step is to select the appropriate application on the chip to facilitate the card routing. Each application has at least one unique application identifier (AID), a 16-byte numerical string that helps identify the application provider (e.g., Visa, MasterCard, Star) as well as distinguish between the different network products that are supported (e.g., Visa credit versus Visa Interlink).

Chip cards are issued with the appropriate applications preloaded, and when terminals are deployed, they must be configured to accept the AIDs associated with all supported networks. With 18 U.S. debit networks, this presented the theoretical possibility that issuers would have to preload multiple sets of technology on their debit card chips in order to maintain their option to change debit network relationships. This would significantly increase the cost and memory

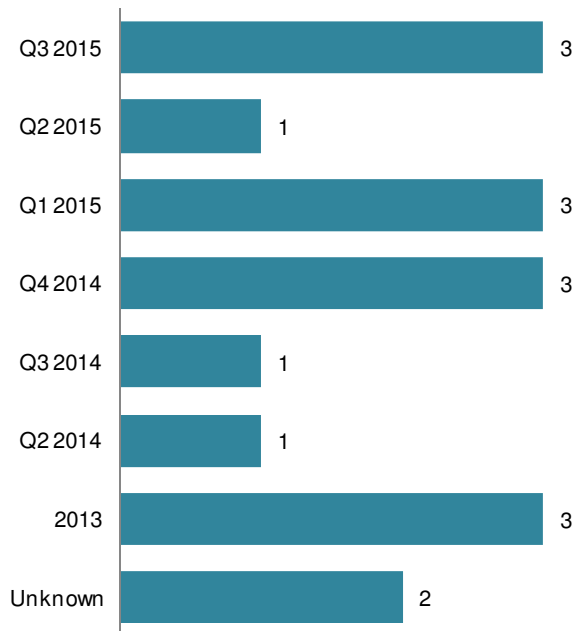
requirement of the chip as well as the complexity of deployment. Alternatively, the issuer would have to reissue the entire card population if it wanted to change its debit network affiliation.

To address this issue, issuers and merchants alike urged the debit networks to align around a common debit AID that could be used for all debit networks. This common AID would prompt the merchant's processor to perform an automated lookup to determine which network the merchant prefers, emulating the current network selection environment. While simple in concept, the devil is in the details. Via the EMV Migration Forum, a committee established to serve as an industry round-table to provide for a more efficient, effective migration to EMV, the industry negotiated for nearly two years before it came up with a workable solution, which it now has. This solution will work whether or not the merchant challenge to Regulation II is upheld by the Supreme Court, thus putting an end to an important point of uncertainty with regard to the U.S. migration.

## **U.S. TRAJECTORY**

October 2015 is just 17 months away, and issuers and merchants alike have a lot of work to do between now and then. While many U.S. issuers began issuing EMV-enabled credit cards to international travelers as early as 2010, very few FIs have begun general issuance. The uncertainty caused by Judge Leon's July 2013 ruling slowed many issuers' planning processes, while others are seeking to strike the right balance between putting cards in the market too early (and risking the additional cost of reissuance in the event of future data breaches) and putting cards in the market too late. As one interviewee aptly put it, the migration is like a game of musical chairs. No bank wants to be the last one relying on the mag stripe, because the fraudsters will soon find out, and losses will soar.

The experience of other countries has shown, however, high rates of fraud losses are a powerful motivator, as is the specter of legislative interference. Legislators in California have already taken the matter into their own hands, and there is a bill before the California Senate, SB 135, that would mandate EMV in California by April 2016. With much of the Durbin-related uncertainty in the past, many issuers are now moving aggressively to get chip-enabled cards in the market ahead of the October 2015 liability shift date. As shown in Figure 14, eight FIs interviewed will begin general issuance by late 2014, while three will begin in Q1 2015.

**Figure 14: Planned Timeline for EMV Deployment****U.S. Issuers' Planned Timelines for EMV General Issuance,  
2013 to Q3 2015 (n=17)**

*Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014*

The larger issuers will be more aggressive with their deployment time frame, as shown in Table B, which provides an overview of the percentage of their credit card portfolio issuers plan to have deployed by the liability shift date. The supply chain may thwart some of these plans; plastics manufacturers, card personalization shops, and the other vendors in the card production process have finite capacity, which will be pushed to its limits if issuers stick to the timelines below.

**Table B: Percentage of Credit Card Portfolio Deployed by October 2015**

| FI size          | Portfolio deployment % by October 2015      | FI size          | Portfolio deployment % by October 2015                      |
|------------------|---------------------------------------------|------------------|-------------------------------------------------------------|
| <b>Top 10</b>    | 80%                                         | <b>#11 to 20</b> | Undecided                                                   |
| <b>Top 10</b>    | 100%                                        | <b>#11 to 20</b> | Undecided                                                   |
| <b>Top 10</b>    | 33% to 50%                                  | <b>#11 to 20</b> | 100%                                                        |
| <b>Top 10</b>    | 60% to 80%                                  | <b>#21 to 30</b> | 10% to 20% (highest risk, equating to 60% of exposure risk) |
| <b>Top 10</b>    | Undecided                                   | <b>#21 to 30</b> | Unknown                                                     |
| <b>Top 10</b>    | 50% (representing 95% of active purchasers) | <b>#21 to 30</b> | 100%                                                        |
| <b>Top 10</b>    | Unknown                                     | <b>#31 to 40</b> | 5% or less                                                  |
| <b>#11 to 20</b> | 100%                                        | <b>#31 to 40</b> | Undecided                                                   |
| <b>#11 to 20</b> | 50% to 75%                                  | <b>#31 to 40</b> | Undecided                                                   |

Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

## CARDHOLDER VERIFICATION MECHANISM

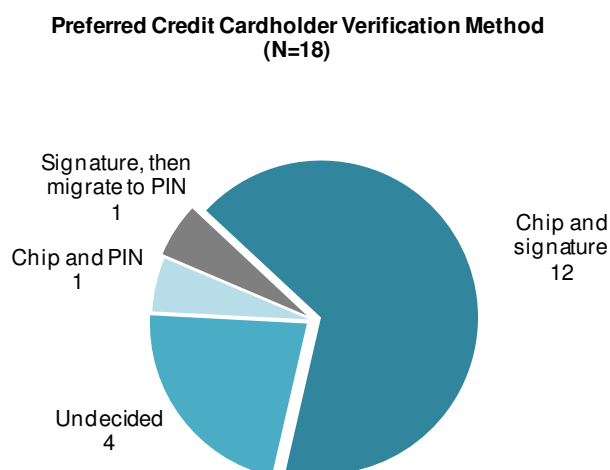
The majority of U.S. FIs interviewed are looking primarily to chip and signature as their preferred CVM for credit card (Figure 15), while nearly all issuers interviewed plan to use chip and PIN as the preferred debit CVM. There are a number of drivers for this choice:

- **Customer experience:** The desire to maintain a seamless transaction experience is a consideration cited by the majority of FIs interviewed. Confusion over the PIN process, forgotten PINs, and inconsistent PIN reset capabilities have all been challenges in previous migrations, which for some FIs directly resulted in declining transactions as their card was sent to the back-of-wallet. If a card is issued as PIN preferred, consumers can't simply hit the cancel button if they forget their PIN and sign for the transaction instead; in this environment, it's no PIN, no transaction. As many FIs weigh their business case, the potential for customer attrition outweighs the opportunity to reduce lost/stolen fraud.
- **Relative ease of implementation:** The issuance of cards preferring online PIN requires upgrades to the supporting infrastructure in order to make the PIN workable for consumers. PIN mailers need to be sent to notify the consumer of their initial PIN. IVR systems and ATMs need to be upgraded to support PIN resets. Some processing systems aren't capable of supporting online PIN validation, requiring either upgrades to the system or an offline PIN implementation, which has its own set of infrastructure upgrade requirements and additional ongoing overhead. Consumers need to be educated. All of this adds a considerable amount of work to an already tight deployment timeline.

- **Reduced cost:** The overhead associated with the use of PIN for credit card also has incremental one-time and ongoing costs, which chip and signature does not entail.
- **Increased use of No CVM:** The card networks have increasingly pushed terminal manufacturers and acquiring banks overseas to include the option to initiate a transaction without a cardholder verification mechanism such as PIN or signature (i.e., No CVM). With No CVM as an option, chip-and-signature cards increasingly work in a variety of environments, even unmanned kiosks. One issuer reported that its international travel EMV pilot relied on chip and signature, and the increased use of No CVM addressed 95% of the prior rejection issues. No CVM will also be the preferred method in the United States for contactless transactions less than US\$50.
- **Pain points:** Contrary to the case in the U.K., where counterfeit fraud and lost/stolen fraud were roughly even at the outset of the migration, counterfeit fraud is far more problematic for U.S. issuers. Under Visa's rules, issuers remain responsible for lost/stolen fraud regardless of which CVM is deployed.

Many issuers acknowledged that the post-EMV environment will be dynamic, and they plan to keep a close eye on fraud patterns and consumer sentiment. If there is another watershed event such as the Target breach, and consumers start clamoring for the PIN, issuers will respond. One top 10 FI has card stock that is PIN-capable in order to facilitate an easy transition should consumer demand for PIN surge, but this issuer's initial deployment will be chip and signature.

**Figure 15: Planned Preferred Cardholder Verification Method**

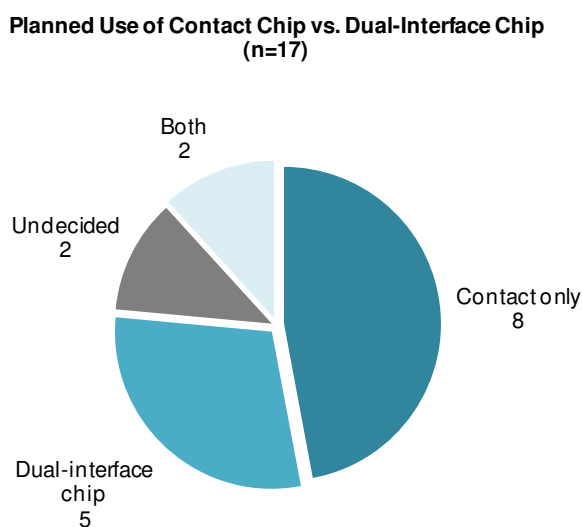


Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

## CONTACT CHIP VS. DUAL-INTERFACE CHIP

The market is a bit wary of initially deploying dual-interface chips, which can facilitate either contact or contactless transactions (Figure 16). Those issuers that plan to deploy dual interface see it as a migration path to mobile payments, as well as a competitive differentiator. Issuers that plan to start with contact-only cite a desire to keep the initial deployment as streamlined as possible, given the rapidly approaching liability shift date. As one issuer aptly put it: "We'll go to market with plain vanilla, then we'll think about adding the toppings." Other issuers are planning to go with the somewhat cheaper contact chip out of the gate because they do not believe that the merchant infrastructure will be in place in 2015 to support widespread use of contactless technology. Some issuers are hedging their bets, going to market with contact chip for the majority of their cards but deploying dual interface for select portfolios.

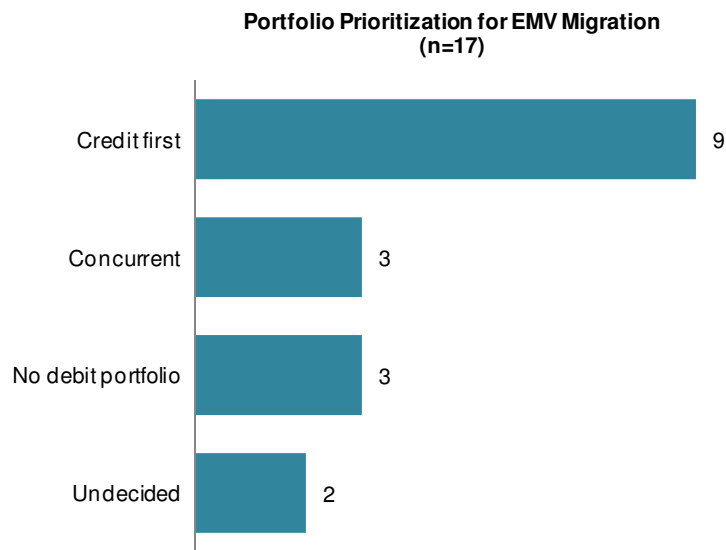
**Figure 16: FI's Planned Use of Contact Chip vs. Dual-Interface Chip**



*Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014*

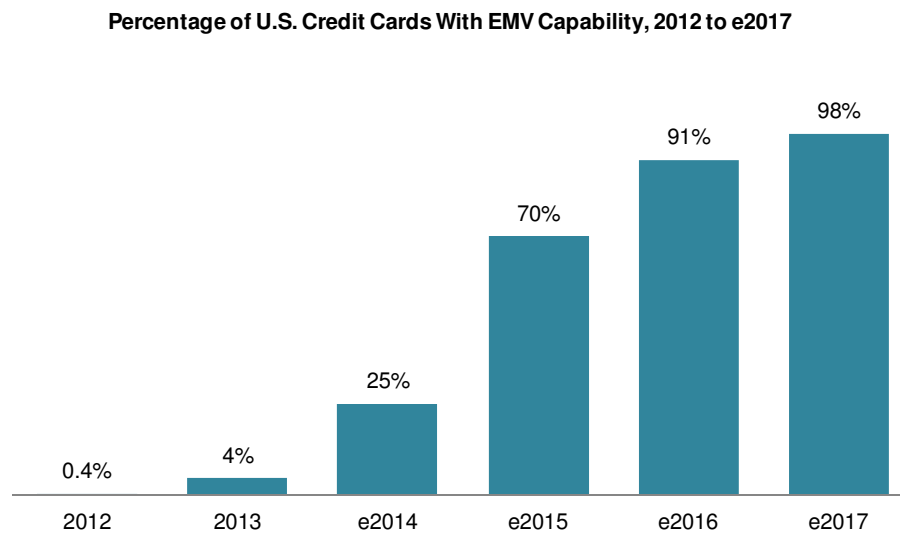
## CREDIT CARDS WILL COME FIRST

Credit cards will be the first recipients of the EMV chip, but debit cards will closely follow (Figure 17). The majority of FIs interviewed say that credit cards will come first, primarily due to the increased complexity associated with debit's dual routing provisions. In addition, many debit networks do not yet have their specifications published, owing in part to the delayed solution of the debit AID issue. Most FIs do not expect the debit migration delay to be significant, however, for fear of a fraud shift to debit.

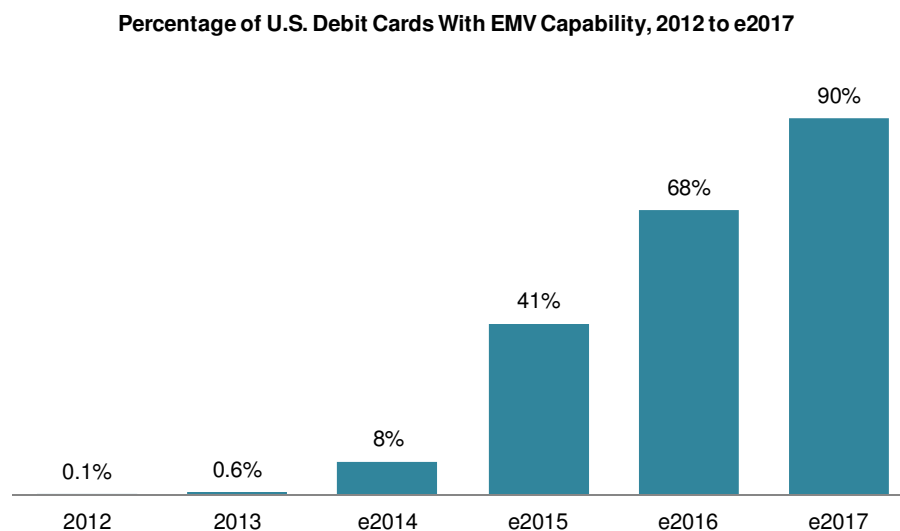
**Figure 17: Portfolio Prioritization for EMV Migration**

Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

Figure 18 and Figure 19 show the projected EMV upgrade time frame of the 1.1 billion network-branded credit and debit cards in the U.S. market.

**Figure 18: Projected Network-Branded Credit Cards With EMV Capability**

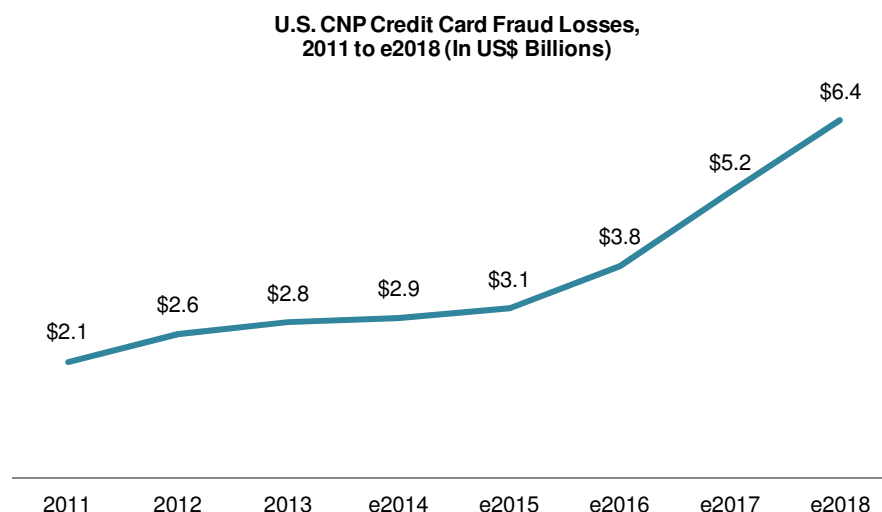
Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

**Figure 19: Projected Network-Branded Debit Cards With EMV Capability**

*Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014*

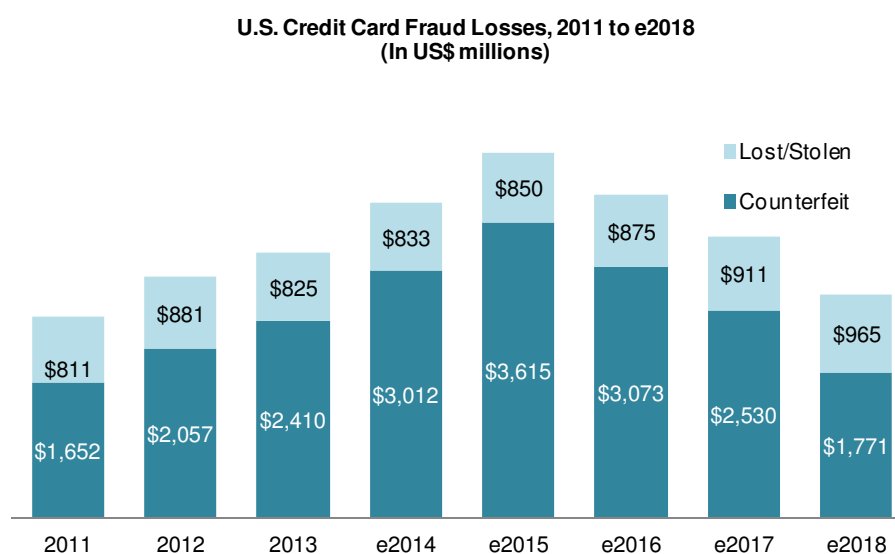
## POST-EMV U.S. FRAUD ENVIRONMENT

So how will the U.S. migration to EMV impact fraud? As in other markets, CNP fraud will increase as fraudsters use stolen card data and other tactics in the online channel. While the increase in CNP fraud has the potential to be even more extreme than other countries experienced, increased investments over the last couple of years in fraud-prevention technologies by issuers and merchants will help blunt the impact (Figure 20). Many issuers interviewed either have or are planning to invest in fraud-prevention technologies such as transactional alerts, risk-based authentication for 3-D Secure, tokenization, or other CNP fraud mitigation technologies ahead of the liability shift date.

**Figure 20: U.S. CNP Credit Card Fraud Losses**

Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

Card-present fraud, which has risen 31% from 2011 to 2013, will be effectively addressed by EMV. Lost/stolen levels will remain at roughly the same level as today, since most issuers are going to market with chip and signature as the primary CVM, while counterfeit card fraud losses will see a significant decline (Figure 21).

**Figure 21: U.S. Card-Present Fraud Losses**

Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

## CONCLUSION

Taking the world's largest card market from mag stripe to EMV is a massive undertaking, and the 17 months before the liability shift takes effect will pass by quickly. Here are a few recommendations for issuers, based on lessons learned from other countries:

- **Consider the migration paths for fraud.** As the EMV deployment progresses, fraudsters will adapt their tactics. With the ATM and fuel dispenser liability shifts one to two years after the POS liability shift, issuers should expect to see fraud attempts ramp up considerably in both of these environments. Social engineering, card theft at the ATM, application fraud, and of course CNP fraud will also see sharp increases; issuers will need to adjust their fraud defenses accordingly.
- **Don't underestimate the consumer and merchant education challenge.** People are creatures of habit, and the process of changing their behaviors is rarely painless. With two different CVMs in the U.S. market, the confusion will be heightened; issuers will need to educate consumers and merchants about the need to dip rather than swipe as well as explain why some credit cards prompt for PIN and others do not.
- **Set achievable goals for your initial migration.** Given the complexity of the EMV migration and the rapidly approaching liability shift date, copying the strategy taken by FIs in many other countries and starting with the basics, assessing the market response, and expanding the use of the EMV chip from there appears to be the prudent course of action.
- **Look to third-party expertise.** One benefit of being the last G-20 country to migrate to EMV is that many experts have already guided FIs in other countries through the process. Consider outsourcing portions of your EMV support infrastructure, at least initially, to streamline the implementation process and help with the knowledge transfer.
- **Adjust your fraud mitigation strategies.** Many countries saw a spike in card-present fraud as the migration took place. Given the prolonged period during which the U.S. transition will occur, issuers will need to have multiple fraud analytic models deployed, reflective of the wide variety of POS payment scenarios that will exist. They will need to have technology that can detect new fraud patterns and adjust rapidly.
- **Don't delay.** If your FI has not begun working on its migration plan, it is imperative that it does so now. The industry is moving, and FIs that lag will suffer increased fraud rates as fraudsters focus their attacks on the weakest link in the chain.

## RELATED AITE GROUP RESEARCH

*POS EMVy: Making the Mobile POS Work in Europe*, January 2014.

*How Long Will It Take? EMV and NFC Reterminalization in the United States*, July 2013.

*EMV: A Roadmap and Guidebook for the U.S. Market*, June 2013.

*3-D Secure: Poised to Live Long and Prosper*, March 2013.

## ABOUT AITE GROUP

Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, securities & investments, and insurance, Aite Group's analysts deliver comprehensive, actionable advice to key market participants in financial services. Headquartered in Boston with a presence in Chicago, New York, San Francisco, London, and Milan, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

## AUTHOR INFORMATION

**Julie Conroy**

+1.617.398.5045

[jconroy@aitegroup.com](mailto:jconroy@aitegroup.com)

## CONTACT

For more information on research and consulting services, please contact:

**Aite Group Sales**

+1.617.338.6050

[sales@aitegroup.com](mailto:sales@aitegroup.com)

For all press and conference inquiries, please contact:

**Aite Group PR**

+44.(0)207.092.8137

[pr@aitegroup.com](mailto:pr@aitegroup.com)

For all other inquiries, please contact:

[info@aitegroup.com](mailto:info@aitegroup.com)