Chip-and-PIN: Success and Challenges in Reducing Fraud

Douglas King

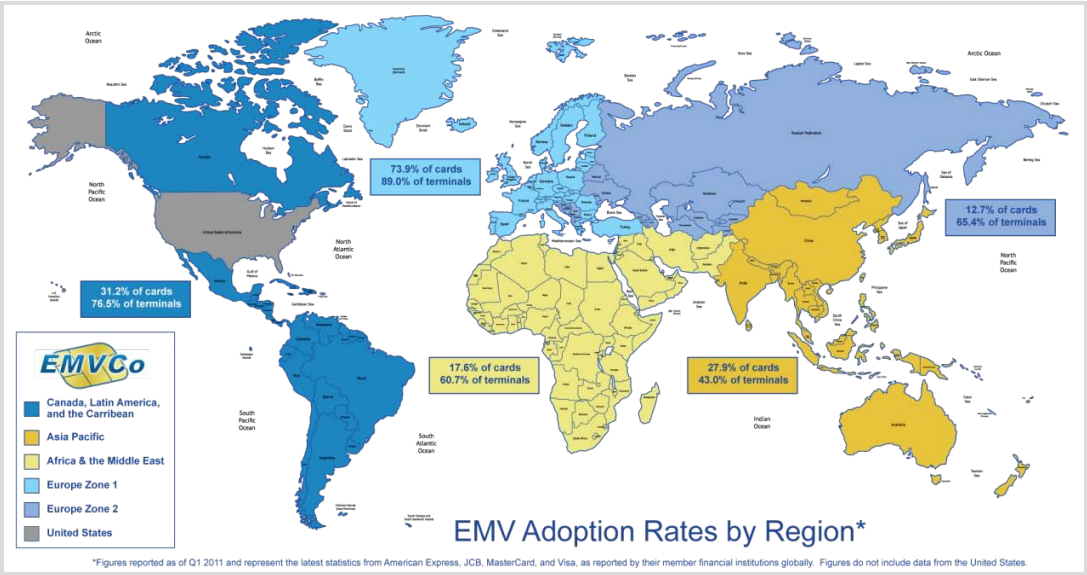
Retail Payments Risk Forum Working Paper
Federal Reserve Bank of Atlanta
January 2012

Abstract: Traditional payment cards have evolved in much of the world and now rely on the EMV global standard using chip technology. However, this evolution of payment cards has yet to occur in the United States payment card industry, which continues to rely on magnetic stripe technology. Transactions conducted with EMV chip-embedded cards that use PIN verification are more secure than transactions conducted using magnetic stripe technology. This paper explores the experience of multiple European, Asian-Pacific, and North American countries in fraud reduction by migrating away from magnetic stripe payment cards to EMV chip cards using PIN verification. Where information and data are available, the paper reviews the reason behind the particular country's migration to chip-and-PIN, the actual migration process, and the migration's success in reducing payment card fraud. It also examines the pattern of fraud migration from chip-enabled payment transactions to non-chip-enabled payment transactions. Finally, the paper closes by examining current payment card fraud trends in the United States and potential implications of prolonging a migration to chip-enabled payment technology.

I. Introduction

As the rest of the globe moves to EMV's global standard[a] using chip technology, the United States remains the last developed country reliant on magnetic stripe (mag stripe) cards. Based on available data from countries around the globe with EMV experience, chip-and-PIN cards have successfully reduced fraud on face-to-face transactions. However, these cards have had less impact on overall fraud levels as fraudsters have shifted their focus to non-chip transactions. Fraud has simply shifted to different products (from credit to debit), other channels (from card-present to card-not present, or CNP), or other geographies (cross-border fraud).

Figure 1: EMV Adoption Rates by Region[1]



As the EMV standard and chip-and-PIN cards mature in adopting countries, the United States could be prone to increased fraud as long as it continues to rely on mag stripe technology. Should the U.S. payments industry decide to abandon mag stripe technology in favor of chip-and-PIN, a coordinated effort from issuers, networks, and merchants will be needed to prevent fraud from shifting to other products and channels. Fortunately for the United States, fraud shifting cross-border should be less of an issue than it was for early EMV adopters since all developed countries will have converted to chip-and-PIN.

Many industry stakeholders argue that a business case based on current fraud loss costs versus chip-and-PIN deployment costs in the United States has yet to fully crystallize, although data within this paper suggests a business case is emerging. However, this paper focuses on the impacts EMV chip-and-PIN has had on card fraud in markets that have adopted the technology.

[a] EMV stands for Europay, MasterCard, and Visa. EMV is a standard for the inter-operation of chip-embedded cards with POS terminals and ATMs used to authenticate payment card transactions.

Furthermore, it analyzes card fraud trends in the United States during this nearly global EMV chip-and-PIN migration.

II. EMV and Chip-and-PIN Explained

EMV is a global standard for payment cards based on chip technology established in 1994 by Europay International SA (acquired by MasterCard in 2002), MasterCard, and Visa. Today, the EMV standard is managed by EMVCo, which is a joint venture of MasterCard, Visa, JCB, and American Express. As of early 2011, 1.2 billion EMV cards were deployed across the globe along with 18.7 million EMV terminals.[2]

A cardholder's confidential data is more secure on a chip-embedded payment card than on a mag stripe card. Chip-embedded cards support dynamic authentication where as data on mag stripe cards is static. Thus, data from traditional mag stripe cards can be easily copied (skimmed) with a simple and inexpensive card reading device. Skimming enables criminals to make counterfeit cards for use at Point-of-Sale (POS) devices or in the CNP environment. Chip technology is effective in combating such counterfeiting through the introduction of dynamic values for each transaction.

PIN verification provides superior protection against fraud losses, especially those losses from lost or stolen cards, compared to signature verification. Based on 2008 debit card fraud data collected by the Federal Reserve Board of Governors, total fraud losses to all parties on signature-based transactions per dollar volume were .13 percent, or 13 basis points. PIN-based transactions experienced a significantly lower fraud loss rate of .035 percent, or 3.5 basis points, per dollar volume.[3] In the event that a card is lost or stolen, PIN verification is more effective in combating fraud than signature verification.

The EMV specification can be used in both online and offline environments[b] and supports both signature and PIN verification with PIN being the dominant verification method used to-date. In fact, the "Chip and PIN" brand name adopted by UK banks for the rollout of EMV cards has become nearly synonymous with EMV, despite the fact that the EMV specification supports signature authorization. The EMV standard evolves with the payments industry and now also includes specifications for contactless payments and mobile payments.

Whether or not the U.S. payments industry adopts the EMV specifications or develops new specifications, a move to chip technology is needed to avoid increased fraud levels. Although there have been multiple reports of security issues with chip technology using the EMV standard,[4] it is reasonable for the United States to adopt the global EMV standard that is

[b] In an online environment, the transaction authorization uses telecommunications at the time of sale to route a merchant's authorization request to the issuer to approve or decline. In an offline environment, transactions are not authorized at the time of sale, but rather are batched throughout a given time period and transmitted to the issuer to approve or decline. For an offline EMV chip–and-PIN transaction, the PIN is authorized through communication between the terminal and chip without the need for telecommunications.

supported by the three largest card networks in this country. EMV chip-based cards offer superior protection of cardholder data compared to mag stripe cards and PIN verification is far superior to signature verification in preventing fraud.[5] Also, as seen with the additional contactless and mobile specifications to the EMV standard, chip-based technology is scalable along the payment evolution continuum into contactless cards and mobile.

III. EMV and Chip-and-PIN in the United States today

The first U.S. payment card utilizing the EMV standard was issued by the United Nations Federal Credit Union (UNFCU) in October 2010. These cards, issued to approximately 5,000 high-value credit card customers, are chip-and-PIN cards. Although payment security was a factor in UNFCU's decision to issue EMV cards, the primary rationale was to provide its members, many of whom reside outside the United States, with a globally accepted card. Mag stripe cards are becoming less accepted outside of the United States, especially in offline applications such as unattended parking and ticketing kiosks. State Employees' Credit Union (SECU) announced in February 2011 that it was issuing EMV chip-and-PIN debit cards to all of its 1.6 million debit cardholders with the migration to be completed by the end of 2011.[6]

Following SECU's announcement, EMV issuance gained some momentum with larger U.S. issuers, albeit for some very small card portfolios. During the second quarter of 2011, Wells Fargo, JPMorgan Chase, and U.S. Bancorp all announced plans to migrate certain credit card portfolios to the EMV standard. Again, the reason for the technology migration by these financial institutions had less to do with risk and was more about global acceptance of the cards. Interestingly, the larger institutions have primarily opted for signature cardholder verification while the credit unions have opted for PIN cardholder verification.

Table 1: EMV Consumer Cards in the United States[*]

Issuer	Approximate Date of First Issuance	Portfolio	Approximate Portfolio Size	Network	Cardholder Verification
United Nations Federal Credit Union	October 2010	Platinum Elite	7,000	Visa	PIN
State Employees' Credit Union	March 2011	Debit	1,600,000	Visa	PIN
JPMorgan Chase & Co.	June 2011	Palladium	Don't Know[1]	Visa	Signature
Wells Fargo & Co.	Mid-Summer 2011	N/A[2]	15,000	Visa	Signature & PIN
U.S. Bancorp	July 2011	FlexPerks Travel Reward	20,000	Visa	Signature

[*] Information through June 30, 2011.

[1] No reports of portfolio size, but likely smaller than other credit card portfolios listed.

[2] The Wells Fargo card is a pilot program that will be issued to high frequency international traveling cardholders.

On the acquiring side of the equation, there is currently no merchant acceptance in the United States of EMV chip-embedded cards. Most EMV chip cards issued abroad and domestically also contain a mag stripe and thus are accepted at all U.S. merchant locations that accept cards. However, several large U.S. merchants have expressed an interest in chip-and-PIN technology to replace mag stripe technology and signature verification.

Perhaps both the issuance and acceptance of EMV chip cards (and potentially other chip-enabled devices such as mobile phones) will increase with a recent announcement by Visa.[7] This announcement specified incentives and deadlines to urge U.S. merchants to accept both contact and contactless chip-enabled cards. One merchant incentive includes the elimination of the requirement for annual PCI[c] compliance validation if 75 percent of a merchant's transactions originate from chip-enabled terminals effective October 1, 2012. For the largest merchants, savings from an annual PCI compliance validation would average approximately $225,000 a year.[8] Further, Visa set October 1, 2015 as the date when a card-present counterfeit fraud liability shift from issuers to merchant acquirers will be implemented if fraud occurs in a transaction that could have been prevented with a chip-enabled payment terminal. While the announcement lays a path towards EMV chip card migration, it does not necessarily set a path to chip-and-PIN as Visa will continue to support both signature and PIN cardholder verification methods.

In the interim, the U.S. card industry continues to wrestle with the decisions of chip card adoption, as well as signature versus online or offline PIN verification, despite evidence that fraud in the card-present environment is significantly reduced in EMV chip-and-PIN adopting countries.

IV. The Chip-and-PIN Experience in the UK

Background

In the early 1990's, the Association for Payment Clearing Services (APACS),[d] consisting of financial institutions and payment clearing and settlement companies, created the Plastic Fraud Prevention Forum (PFPF). This Forum represents all of the UK's major card issuers and works to develop card fraud prevention initiatives. The PFPF launched a major project in the mid-1990's to obtain a better understanding of systemic fraud on payment card transactions. Card fraud in the UK was relatively high compared to other developed markets. The authorization environment was a key driver for the UK's high card fraud figures.

[c] PCI is a security standards council launched in 2006 by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. This council is responsible for the development, management, education, and awareness of payment card security standards for issuing and acquiring participants of these card networks.

[d] As of July 6, 2009, APACS was replaced by its successor organization, The UK Payments Administration Ltd. This organization supplies services to multiple payments-related trade associations including The UK Cards Association.

Unlike the United State's online card authorization environment, the UK has primarily been an offline authorization market. Because of this difference in authorization environments, UK card fraud rates have historically been much higher than the rates in the United States. For example, card fraud for 2004 in the UK stood at .14 percent per transaction value[9] compared to an estimated .05 percent of bankcard fraud per transaction value in the US.[10]

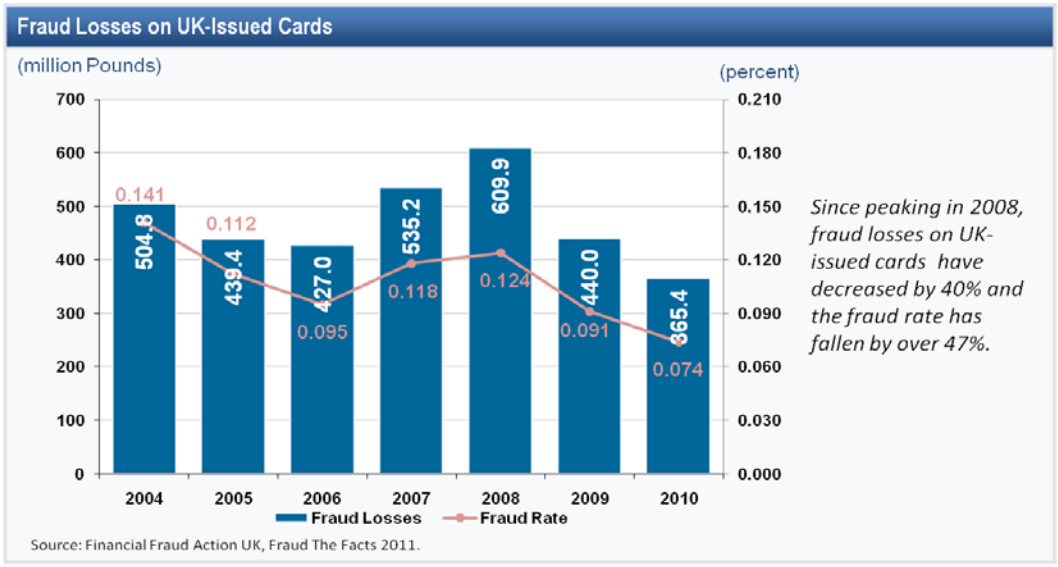
Since EMV chip-and-PIN supports authorization at the time of sale in either an online or offline environment, it was viewed as a key driver of reducing card fraud in the UK given the country's offline authorization market. Following several successful chip-and-PIN trials in the mid- to late-1990s, the APACS decided on a national rollout of EMV chip-and-PIN in 2002. Implementation of chip-and-PIN gained traction in 2004, and by the end of August 2006, the UK was close to full migration (99.8 percent of chip transactions were PIN-verified).[11]

Much like in the United States, UK bank card issuers were saddled with the majority of the fraud loss burden, yet the migration was going to be costly for merchants to install new hardware and software to accept chip-and-PIN cards. Merchants did not find the benefits of migration to chip-and-PIN to be very equitable as the bulk of the investment landed with the merchants, while the benefits of reduced fraud losses flowed to the issuers. In order to encourage merchants to migrate to chip-and-PIN enabled terminals, the card networks instituted a liability shift which places the fraud loss burden on the non-EMV compliant party. Beginning in July 2005, any merchant that had not upgraded their terminals to be chip-and-PIN compliant would be liable for fraudulent transactions using chip-and-PIN cards which could have been avoided by upgrading the terminal. The card issuer remains liable for fraudulent transactions if the transaction is conducted using a mag stripe card or if both parties are chip-and-PIN enabled.

Impact on Fraud

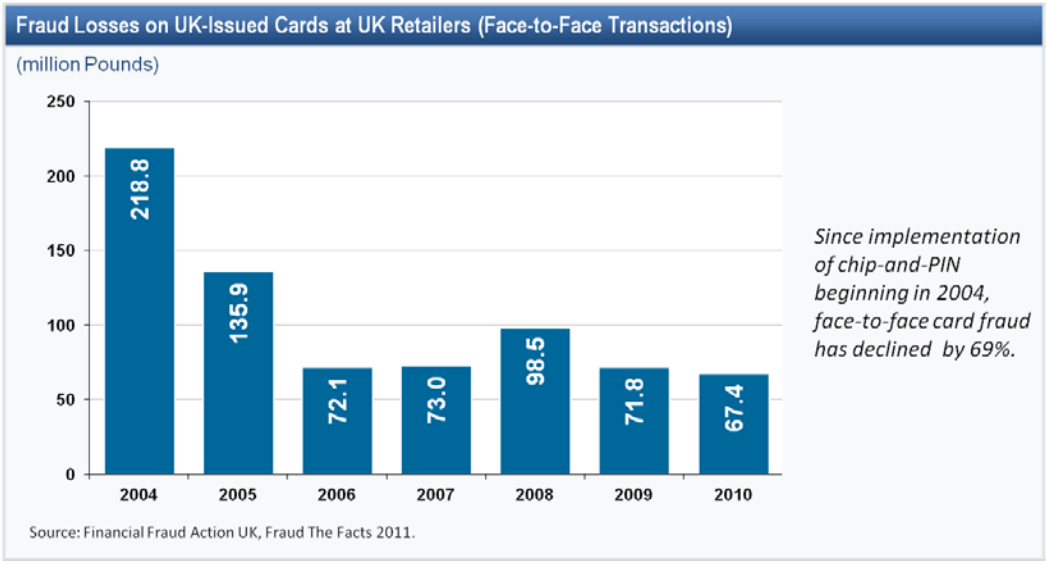
According to data from the UK Payments Administration, EMV chip-and-PIN has been successful at reducing certain types of card fraud, especially domestic counterfeit and lost or stolen card fraud. Total card fraud in the UK began declining in 2005 as the chip-and-PIN movement gained traction. However, with widespread chip-and-PIN adoption completed by 2006, total card fraud increased significantly in 2007 and 2008 due to significant increases in CNP and cross-border fraud. Few viable chip-and-PIN solutions for online merchants have emerged, leading to the migration of fraud to the CNP channel. Also, since chip-and-PIN cards still contain mag stripes for use at merchant locations not equipped to handle chip transactions, fraud has migrated abroad through the use of counterfeit cards in countries primarily using mag stripe technology. As more countries have adopted chip-and-PIN and CNP fraud prevention measures have been increased, total card fraud has been on a significant decline since 2009.

Chart 1: Fraud Losses on UK-Issued Cards



EMV chip-and-PIN has been highly successful reducing domestic fraud in the UK Since 2004, domestic fraud losses on UK-issued cards has fallen by over 34 percent. Chip-and-PIN has successfully thwarted the primary fraud losses it was designed to prevent, counterfeit and lost or stolen card fraud.

Chart 2: Fraud Losses on UK-Issued Cards at UK Retailers (Face-to-Face Transactions)

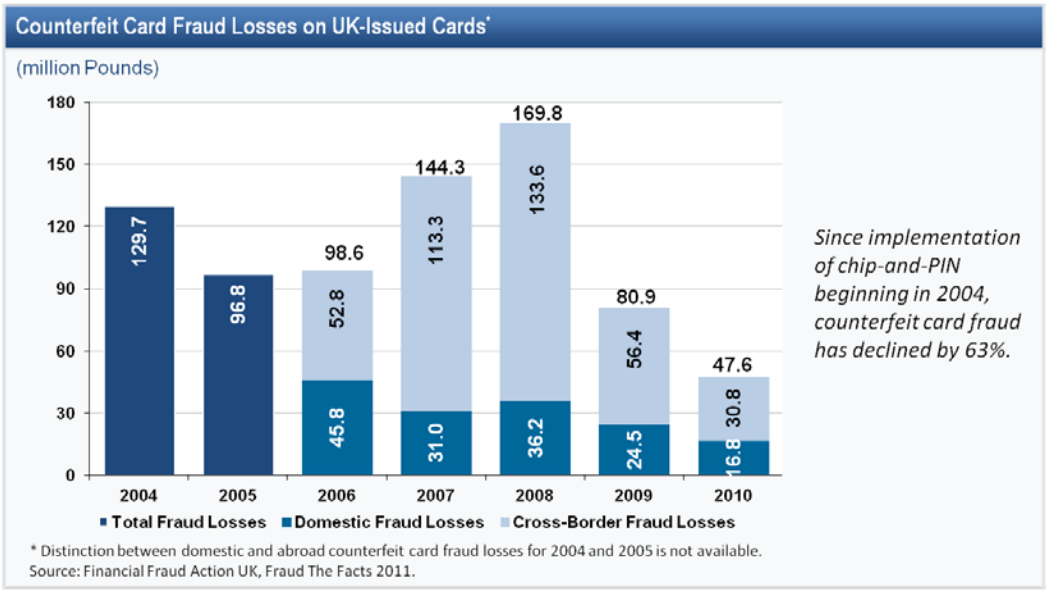


Since widespread implementation of EMV chip-and-PIN in 2004, counterfeit fraud declined drastically on UK-issued cards. Fraud losses from counterfeit cards have fallen by over 63 percent. In fact, in 2004 counterfeit card fraud accounted for over 25 percent of all card fraud on UK issued cards compared to 13 percent by the end of 2010. Domestic counterfeit card fraud fell

to £17 million in 2010 from £46 million in 2006 and now represents only 6 percent of all domestic card fraud.

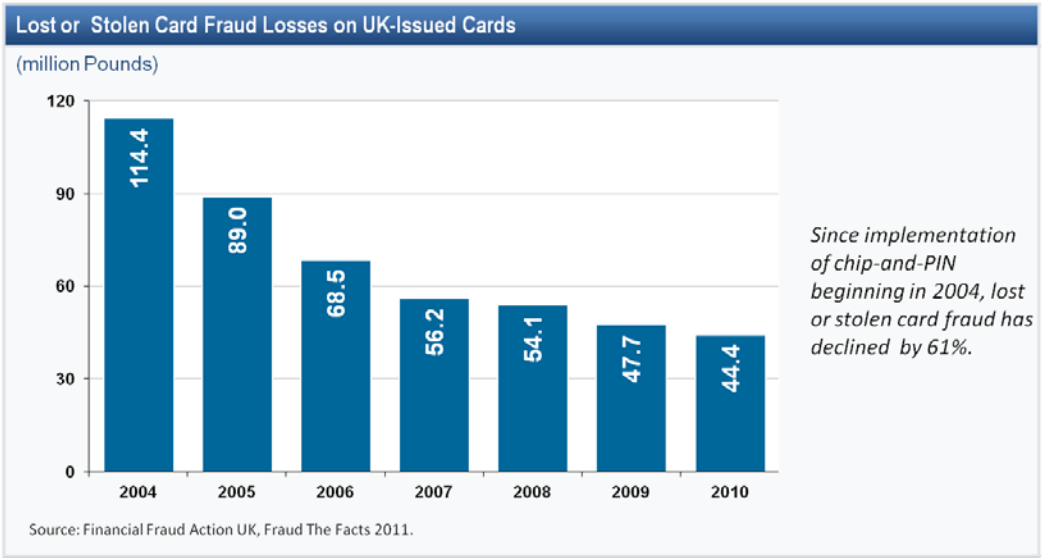
However, counterfeit fraud on UK-issued cards has not been on a continuous decline since chip-and-PIN implementation in 2004. Interestingly, counterfeit fraud rose significantly in 2007 and 2008 as UK card issuers experienced a dramatic increase in cross-border counterfeit fraud. Since UK-issued chip cards still contain a mag stripe, fraudsters are able to capture card data off the mag-stripe and commit fraud in countries that have yet to migrate to chip-and-PIN. As migration of chip-and-PIN increased in other countries, especially other European countries, losses from counterfeit cards abroad began to abate. Today, nearly 75 percent of cards and 90 percent of POS terminals in Western Europe have adopted the EMV chip-and-PIN standard.[12]

Chart 3: Counterfeit Card Fraud Losses on UK-Issued Cards



Much like counterfeit fraud, lost or stolen card fraud in the UK has declined significantly since the implementation of EMV chip-and-PIN in 2004. The 61 percent decline in lost or stolen card fraud losses from 2004 to 2010 exhibits a much different pattern of decline than the decline witnessed in fraud losses from counterfeit cards. While counterfeit fraud losses increased significantly in 2007 and 2008 due primarily to cross-border fraud committed on UK-issued cards, lost or stolen card fraud has decreased every year since 2004 and now stands at its lowest level since the industry began collecting fraud loss data in 1991.

Chart 4: Lost or Stolen Card Fraud Losses on UK-Issued Cards



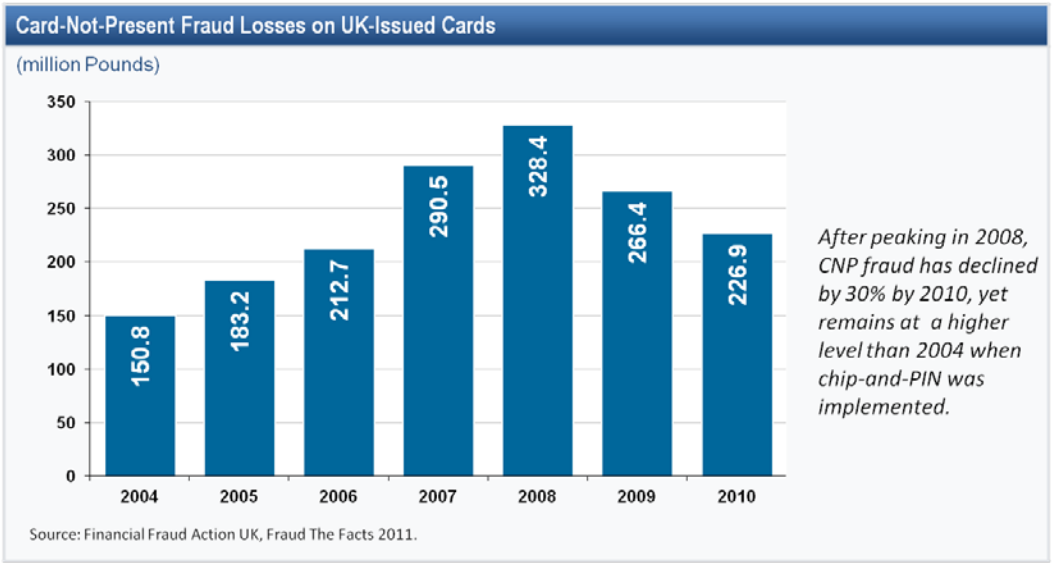
While immense strides against fraud losses have been made seven years into chip-and-PIN implementation, counterfeit and lost or stolen card fraud still exists in the UK. Chip-and-PIN has been successful at reducing both of these fraud types, but contrary to some reports circulating in the US,[13] the technology has not completely eliminated any one type of fraud, and has actually pushed fraud to CNP and cross-border transactions.

The success of EMV chip-and-PIN at thwarting fraud at the POS in the UK has led the fraudsters to seek the lowest common denominator in terms of perpetrating fraud, transactions not protected by chip-and-PIN. These transactions most commonly occur in the CNP environment and in countries that still rely on mag stripe technology. Consequently, since the introduction of chip-and-PIN in 2004, both CNP and cross-border fraud rose dramatically through 2008, before falling in 2009 and 2010.

CNP fraud now accounts for 62 percent of all fraud on UK-issued cards, up from 30 percent in 2004. Although solutions for chip-and-PIN transactions exist in the CNP environment, they have yet to gain much adoption by either merchants or cardholders due to cost and consumer adoption concerns. These hardware-based solutions, often attached through a USB device, create a secure connection and generate dynamic data in a manner similar to a card-present transaction. The recent decline in CNP fraud on UK-issued cards has primarily been due to the growth in the use of a non-chip-and-PIN solution, 3-D secure[e] by both merchants and cardholders.

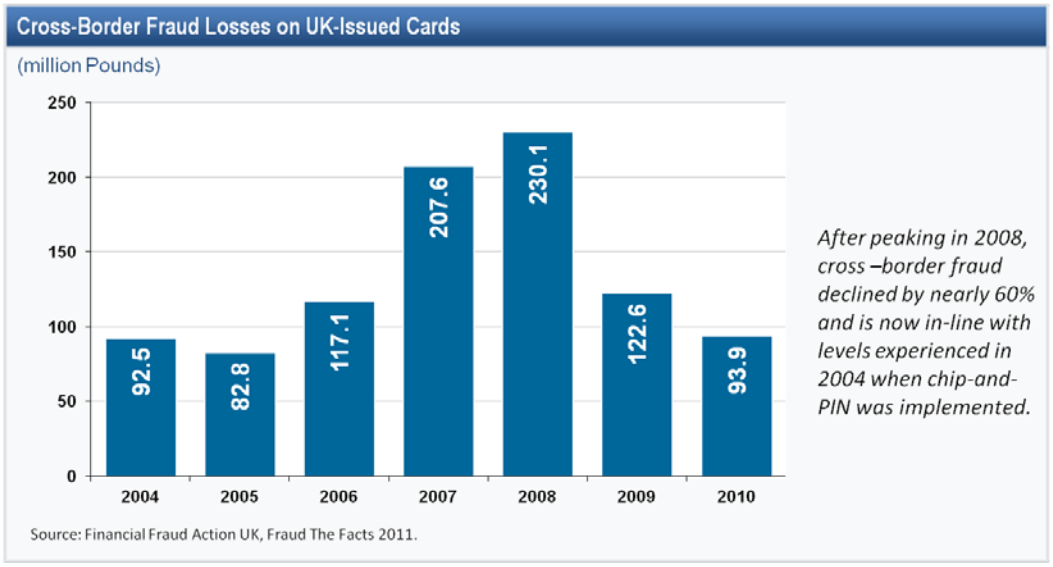
[e] 3-D Secure is an XML-based protocol designed to be an added layer of authentication for Internet-based payment card transactions. Visa, MasterCard, American Express, and JCB all offer the 3-D Secure protocol. This protocol requires that a cardholder enter a unique PIN to complete a CNP transaction as an additional identity verification process.

Chart 5: Card Not Present Fraud Losses on UK-Issued Cards



As the EMV chip-and-PIN standard became more prevalent around the globe, and especially in Europe, cross-border fraud on UK-issued cards began declining in 2009 after peaking in 2008.

Chart 6: Cross-Border Fraud Losses on UK-Issued Cards



However, fraud occurring in the United States on UK-issued cards stands at a higher level in 2010 than it did in 2005. In fact, fraud in the United States accounted for 14 percent of cross-border fraud losses on UK-issued cards in 2005, and today accounts for 23 percent of all cross-border fraud losses. Interestingly, as most of Europe has migrated, or is in the process, to EMV chip-and-PIN, no European country is part of the top 5 countries for cross-border fraud on UK-issued cards in 2010.

V. The Chip-and-PIN Experience in France

Background

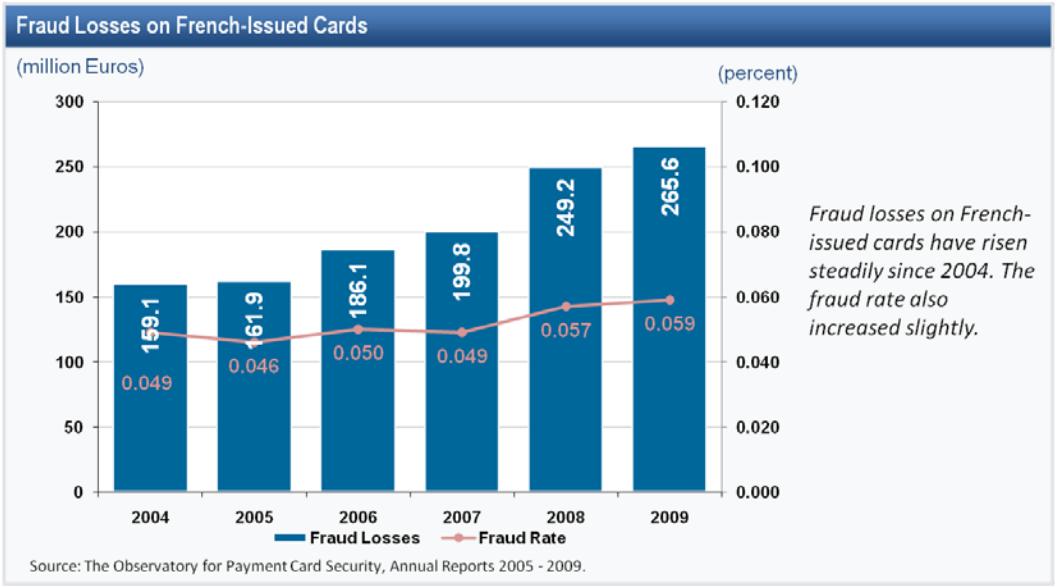
France was an early adopter of chip card technology. By the mid-1980's, the fraud rate on French-issued cards was extremely high, reaching .27 percent by 1987,[14] according to data from Groupement des Cartes Bancaires. With fraud rates on the rise, French banks issued the first chip-embedded smart cards in 1986. By 1992, all French bank cards were embedded with a chip resulting in a sharp decline in fraud. The fraud rate on French-issued payment cards was down to .03 percent in 1995.

Even though card fraud levels were already extremely low, France followed the UK card industry's lead and began migrating to EMV chip-and-PIN cards in 2002 with several trials. By October of 2003, a national rollout was launched with the migration to chip-and-PIN finalized by the end of 2006. Since 2005, all French-issued cards use chips that support dynamic data authentication.

Impact on Fraud

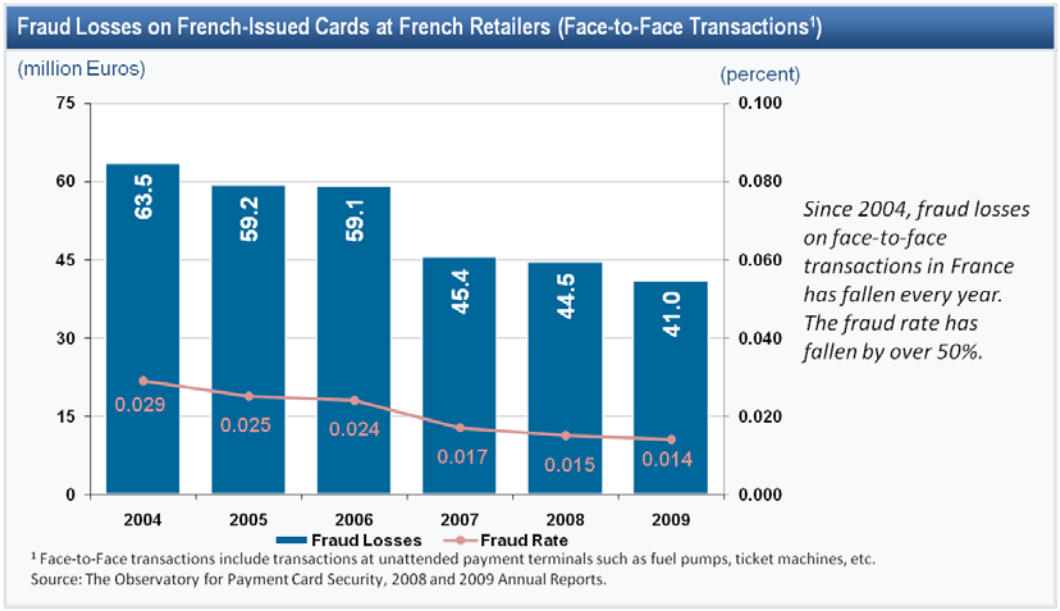
Since implementation of chip-and-PIN, both fraud losses and fraud rates in France have actually increased slightly from low levels of fraud losses and rates prior to EMV chip-and-PIN. However, a noticeable shift in fraud has taken place that is the primary driver of the higher fraud losses and rates. As witnessed in the UK following that country's migration to chip-and-PIN, domestic fraud losses and rates on face-to-face transactions experienced significant declines. Yet, cross-border and CNP fraud increased significantly.

Chart 7: Fraud Losses on French-Issued Cards



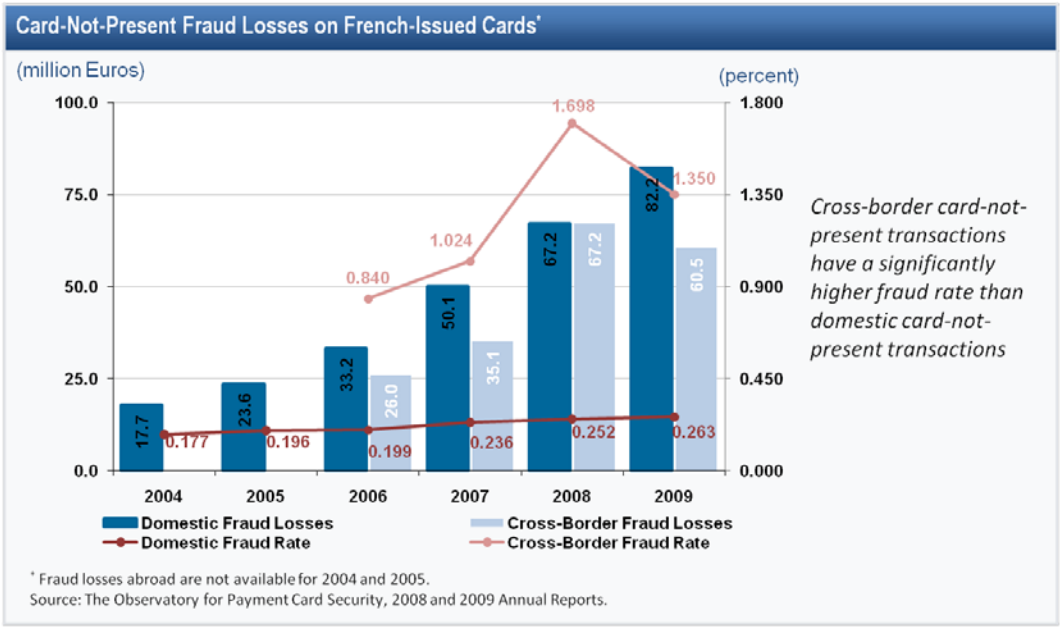
Though total fraud incurred by French issuers has increased since the introduction of EMV chip-and-PIN, domestic face-to-face fraud has significantly declined to extremely low levels. Between 2004 and 2009, fraud losses from domestic face-to-face transactions fell by over 35 percent. Even more impressive though, is the fraud rate on these transactions fell by over 50 percent and by 2009 stood at .01 percent. So during a time of increasing card usage for face-to-face transactions in France, fraud losses decreased significantly.

Chart 8: Fraud Losses on French-Issued Cards at French Retailers



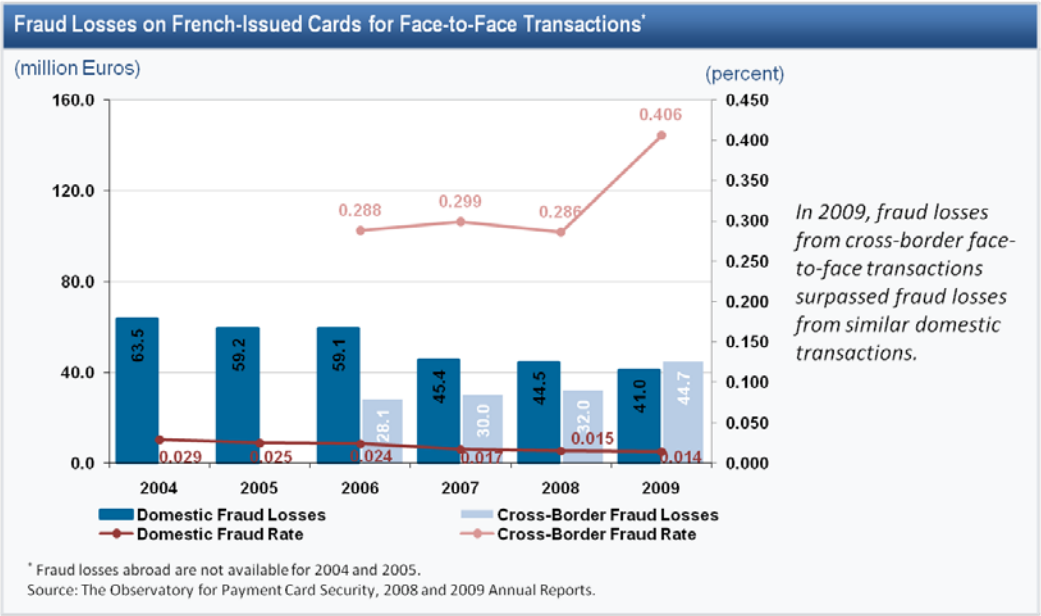
With fraudsters moving away from domestic face-to-face transactions in France, they are focusing their attention on transactions not supported by chip-and-PIN. As such, CNP fraud has experienced a significant increase since the introduction of EMV chip-and-PIN. While transaction volume has increased in the CNP channel with the growth of online commerce, fraud losses in the CNP channel have grown at even a more rapid pace, especially in cross-border CNP transactions. CNP fraud now represents almost 54 percent of all card fraud on French-issued cards up from 25 percent in 2006. The comparison of fraud rates for in-person versus CNP transactions is striking. While face-to-face transactions in France have a fraud rate of .01 percent, domestic CNP transactions have a fraud rate of .26 percent and cross-border CNP transactions have an alarmingly high 1.35 percent fraud rate.

Chart 9: Card-Not-Present Fraud Losses on French-Issued Cards



Not only do cross-border CNP transactions carry a higher rate of fraud than domestic CNP transactions, cross-border face-to-face transactions also have a higher fraud rate than domestic face-to-face transactions. By the end of 2009, the fraud rate on cross-border face-to-face transactions stood at .41 percent compared to .01 percent for domestic face-to-face transactions. In fact, the amount of losses in 2009 from cross-border transactions (€45 million) actually surpassed the losses from domestic transactions (€41 million). And while domestic transactions have experienced a decline in both total fraud losses and rate since the introduction of EMV chip-and-PIN, both total fraud losses and the fraud rate on cross-border transactions have increased.

Chart 10: Fraud Losses on French-Issued Cards for Face-to-Face Transactions



VI. The Chip-and-PIN Experience in Canada

Background

Although Canada's payment card fraud rates were not high by global standards, issuers were becoming concerned by the increasing rate of card fraud experienced during the early to mid 2000's. Issuers had not invested heavily in fraud monitoring and prevention systems like their counterparts in the United States, and agreed in 2006 that a move to chip-and-PIN was needed to reduce the growing rate of fraud. The move to chip-and-PIN is near completion today, but the on-going migration process has been long and slow.

In June 2003, Visa Canada announced that it was committed to chip-and-PIN. Following Visa's lead, MasterCard announced similar plans and guidelines in 2005. Interac, Canada's national debit payment network, announced in October 2005 that it was also committed to chip-and-PIN with a target date of 100 percent migration by the end of 2015. In March 2006, members of the Canadian payments industry[f] announced alignment and "commitment to a broad industry migration to chip technology."[15] Finally, in October of 2007, an EMV chip-and-PIN trial was launched in Kitchener-Waterloo and continued until October 2008 when a national roll-out of chip-and-PIN began.[16] American Express did not announce its EMV chip-and-PIN guidelines until August 2010, but it expects a quick migration with a liability shift date set for October 31, 2012.[17]

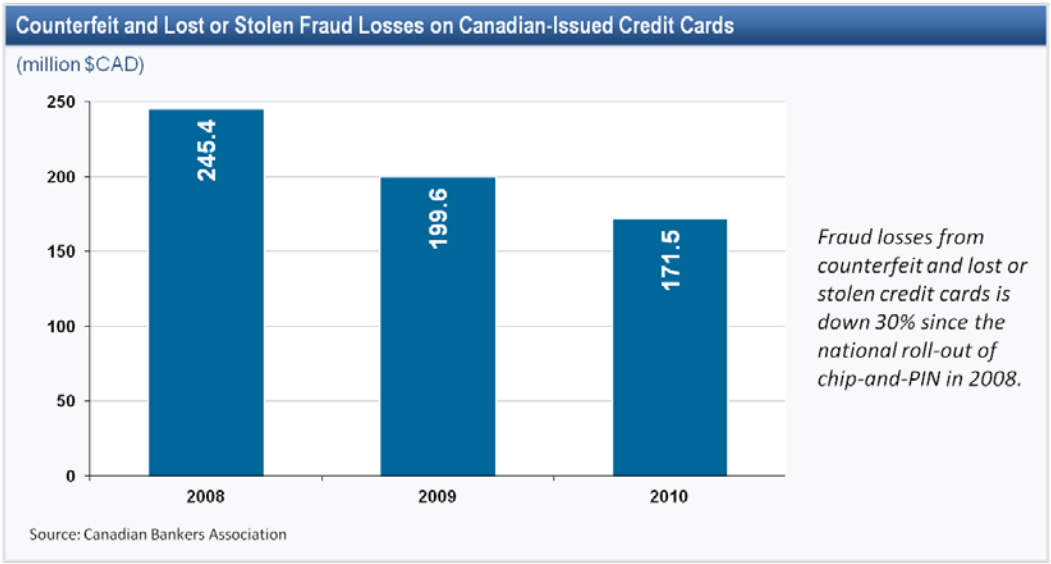
[f] Members of the Canadian payments industry consist of MasterCard Canada, Visa Canada, Interac Association, and many of their respective card issuers, payment processors, and merchants.

Today, Canada is far along the process of migrating to EMV chip-and-PIN. Visa and MasterCard are all but complete with the migration. Liability shift on both Visa and MasterCard transactions went into effect at the end of March 2011. American Express has set a date of October 2012. With a longer time horizon for migration than the credit card networks, Interac's migration to EMV chip-and-PIN has been slower and thus the Canadian debit network remains more reliant on mag stripe technology today than the credit networks.

Impact on Fraud

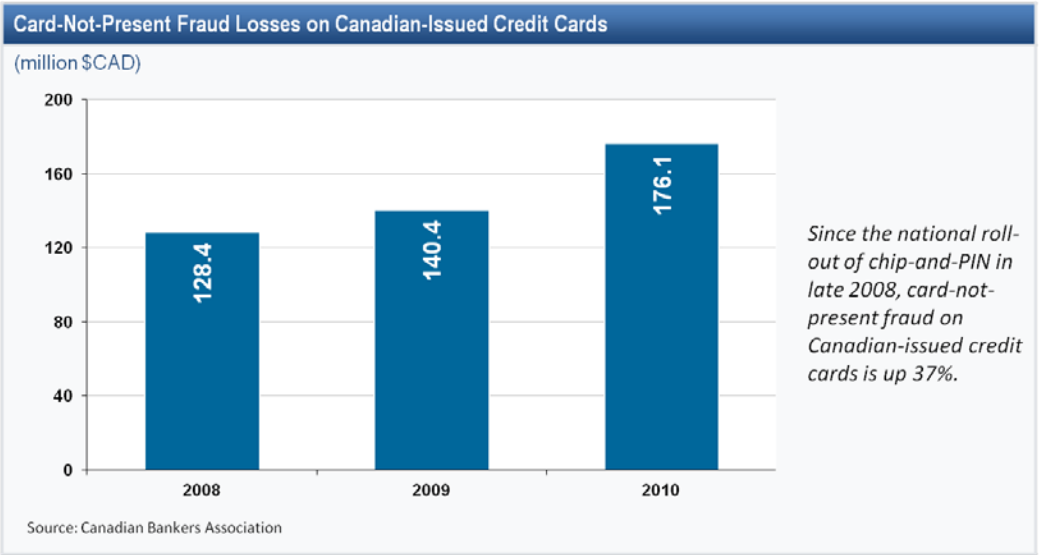
Although the national roll-out of chip-and-PIN did not begin until late 2008, similar fraud migration trends experienced in other chip-and-PIN markets are appearing in Canada. Although total card fraud losses have only decreased by 5 percent from $CAD512 million in 2008 to $CAD485 million in 2010, fraud is migrating to non-chip enabled transactions. In the case of Canada, these transactions are occurring in the CNP environment and with debit cards. Unfortunately, cross-border fraud migration trends are not available as the Canadian Bankers Association did not begin reporting cross-border counterfeit fraud until 2010, presumably because it is becoming a growing issue. And since the roll-out of chip-and-PIN, the EMV chip-and-PIN standard has been effective at reducing the types of fraud it is best suited to prevent -- counterfeit and lost or stolen credit card fraud has decreased by 30 percent.

Chart 11: Counterfeit and Lost or Stolen Fraud Losses on Canadian-Issued Credit Cards



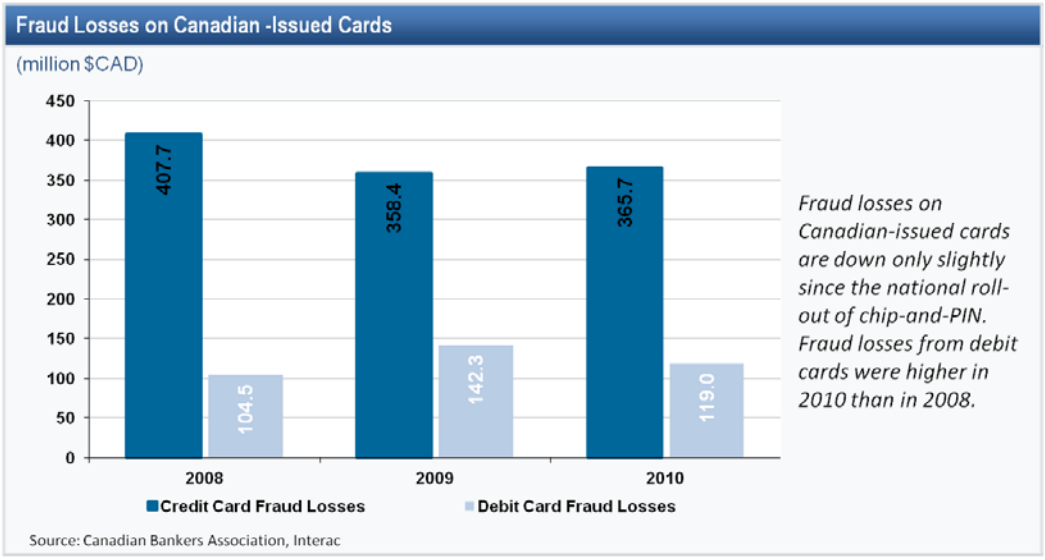
As seen in other chip-and-PIN countries, while fraud losses from counterfeit, lost or stolen cards as well as face-to-face domestic transactions have declined, fraud losses in the CNP environment have increased significantly. And this is no different in Canada. In fact, fraud losses on credit cards in the CNP environment have increased by 37 percent since 2008 when CNP fraud accounted for 31 percent of fraud losses on Canadian-issued credit cards. By the end of 2010, CNP fraud losses account for nearly 50 percent of credit card fraud in Canada.

Chart 12: Card-Not-Present Fraud Losses on Canadian-Issued Credit Cards



Although debit card fraud losses remain significantly lower than credit card fraud losses, fraud committed using debit cards has increased. Between 2008 and 2010, debit card fraud increased while fraud committed using credit cards declined since the chip-and-PIN roll out in 2008. This phenomenon can be explained in large part due to Interac's much slower migration to chip-and-PIN than the credit networks in Canada - MasterCard, Visa, and American Express. As has been the case in every market that has migrated to chip-and-PIN, fraudsters have sought the easiest method for perpetrating card fraud. And in Canada, with debit cards' migration to chip-and-PIN lagging credit cards, fraudsters have taken notice. Debit card fraud spiked in 2009, reaching $CAD142 million up from $CAD104 million in 2008. Fraud on debit cards fell in 2010 to $CAD119 million as Interac advanced its chip-and-PIN migration efforts, but still remains higher than levels seen during 2008, the year of the national roll-out of chip-and-PIN.

Chart 13: Fraud Losses on Canadian-Issued Cards



VII. The Chip-and-PIN Experience in Australia

Background

Australia has traditionally enjoyed a comparatively low rate of card fraud. However, with the movement to EMV chip-and-PIN underway in many European countries and some Asia-Pacific countries, the Australian Payments Clearing Association (APCA)[g] held an initial Chip for Australia Implementation Forum in May 2007. In the absence of significant fraud losses, chip implementation in Australia is being spurred by credit card network incentives and liability shifts. Rather than implement a mass roll-out of chip-and-PIN, APCA agreed to a progressive roll-out to take place over a number of years.

In January 2008, APCA established the Chip Payments Programme for Australia (CPPA)[h] to manage the migration to chip-and-PIN. By the end of 2008, approximately 12 percent of payment cards in Australia were embedded with an EMV chip.[18] In June 2010, EFTPOS Payments Australia Limited (EPAL),[i] Australia's national debit network, announced a move to chip technology beginning in 2011 with completion set for 2014.[19]

The migration to chip-and-PIN is well underway for the credit and scheme[j] debit networks. According to the "MasterCard Roadmap" released at the end of March 2011, all new and reissued MasterCard cards must be EMV capable beginning October 2011. All POS terminals

[g] APCA is the payments industry's principal self-regulatory body and the vehicle for payments industry collaboration. The Association's members include banks, building societies, credit unions, the Reserve Bank, and other payment organizations in its five payment clearing systems.
[h] The CPPA is comprised of card issuers, acquirers, and networks.
[i] EPAL is a joint venture company established in 2009 by Australia's major retail financial institutions and retailers to manage promote and develop Australia's PIN debit card system (EFTPOS) on a commercial basis.
[j] MasterCard and Visa

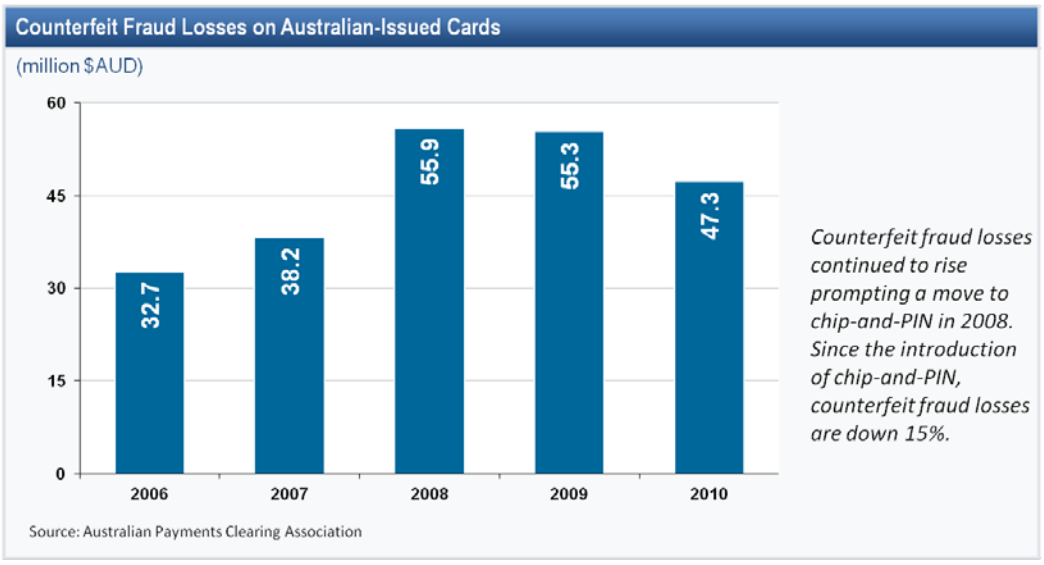
need to be EMV compliant by April 2012 to coincide with a liability shift. And by April 2013, all cards and payment terminals must be EMV capable.[20] Visa's migration timeline is similar to MasterCard's. All newly issued credit cards beginning in 2010 had to be EMV compliant. Debit and prepaid card EMV issuance began in 2011 and by April 2013 all Visa cards must be EMV compliant with Visa's liability shift set to take place.[21]

Impact on Fraud

With migration to EMV chip-and-PIN in Australia still in its early stages, data from the APCA is already showing similar patterns of fraud trends observed in more mature chip-and-PIN markets. Fraud from counterfeit cards has been declining since the migration to chip-and-PIN began; however, total fraud has increased largely due to the significant increase in CNP fraud.

Since rolling out chip-and-PIN cards in 2008 when fraud from counterfeit cards peaked at $AUD56 million, fraud from counterfeiting fell to $AUD47 million in 2010. While the 15 percent decline in counterfeit fraud is promising, it is more modest than the decline in counterfeit fraud in other chip-and-PIN markets. However, the Australian payments market has taken a more methodical and progressive approach to chip-and-PIN implementation. The APCA recently wrote that "chip technology is proving effective in driving skimming [counterfeit] fraud down….notwithstanding unusual spikes, chip technology is expected to combat skimming fraud in Australia over the long-term."[22]

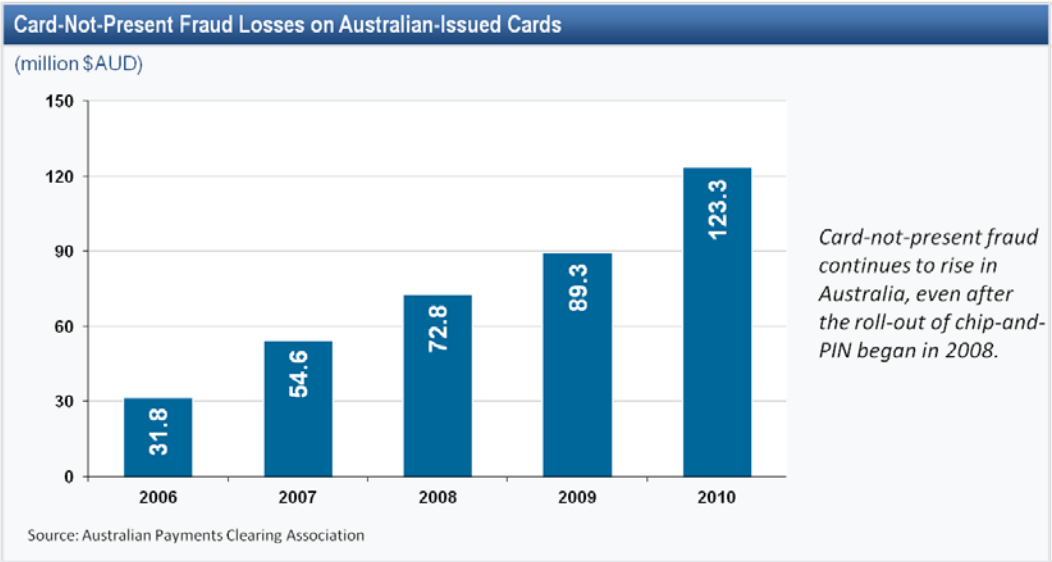
Chart 14: Counterfeit Fraud Losses on Australian-Issued Cards



Although counterfeit fraud is down 15 percent from 2008 to 2010 on Australian-issued cards, CNP fraud has increased by nearly 70 percent during the same time period. And while there are both chip-enabled and non-chip solutions to reduce CNP fraud, they do not appear to be gaining traction in the Australian market. According to the APCA, "financial institutions, card schemes

and retailers are working to implement additional security for online payments using 3D Secure and to increase awareness of the importance of using anti-fraud tools."

Chart 15: Card-Not-Present Fraud Losses on Australian-Issued Cards



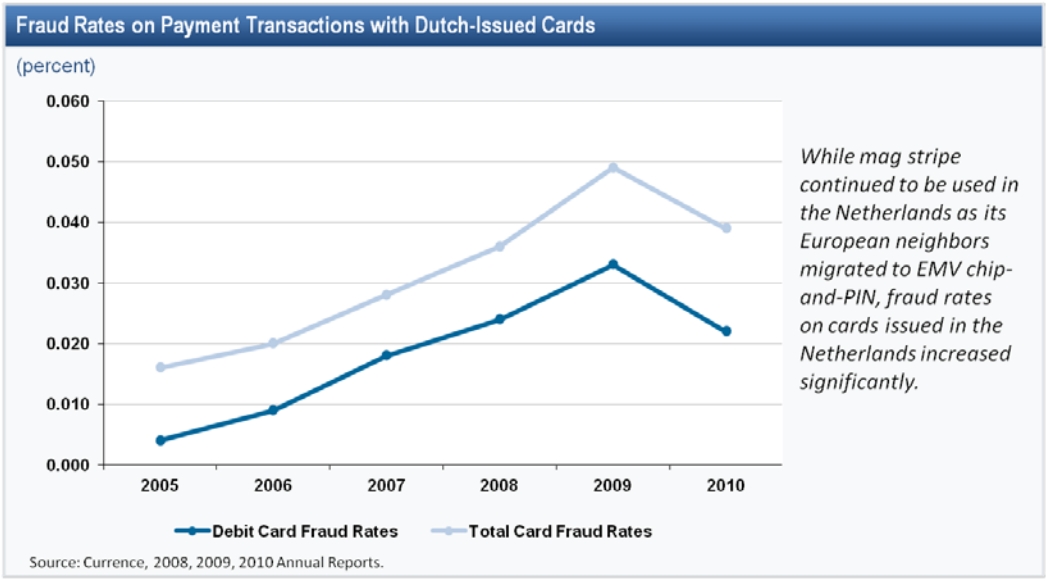
VIII. The Netherlands

The Netherlands provides an interesting glimpse into a country that was slow to migrate to EMV chip-and-PIN at the same time that a majority of its European neighbors were moving to chip-and-PIN. The Netherlands differs from early European adopters of chip-and-PIN in that debit cards are much more popular than credit cards. All debit transactions are authorized online and require a PIN for cardholder verification.[23] Finally, debit cards cannot be used for CNP transactions in the Netherlands.[24]

With online authorization, PIN verification of all debit card transactions, and no CNP debit card transactions, the fraud rate on card transactions in the Netherlands has been historically low. In 2005, a period when many European countries were migrating to chip-and-PIN, the Netherlands experienced a fraud rate of only 0.02 percent. This fraud rate is comparable to France's current fraud rate using chip-and-PIN. Given the low fraud rate, there was not a business case for chip-and-PIN in the Netherlands. Hence, the Dutch initially took a cautious and slow approach to migrating to chip-and-PIN.

However, as the rest of Europe migrated to chip-and-PIN, fraud loss rates climbed in the Netherlands, but still remained relatively low. By the end of 2009, fraud loss rates rose to 0.05 percent. The debit card fraud rate rose to over 0.03 percent in 2009 from less than 0.01 percent in 2005 as skimming of card data for use to counterfeit cards increased significantly. This trend reversed in 2010 as the industry took added measures such as the use of anti-skimming devices to lower the incident of skimming.

Chart 16: Fraud Rates on Payment Transactions with Dutch-Issued Cards



In the 2005 Currence[k] Annual Report, the association stated that it "has established the PIN [the Netherland's debit network] EMV requirements for payment terminals and cards…This will be achieved in part by natural replacement of payment devices and cards over a maximum period of eight years. Given the agreements reached between banks and retailers, Currence expects that the entire operation will be completed by 2013." Given the significant rise in card fraud and the initially slow implementation of chip-and-PIN, the Netherlands' banking industry is now rushing to implement chip-and-PIN. In May 2009, banks and collective POS institutions agreed to accelerate the implementation of chip-and-PIN and on March 2, 2011, the Minister of Finance officially launched the national roll-out of chip-and-PIN in the Netherlands with the expectations that all retailers and consumers will be using chip-and-PIN by the end of 2011.

While fraud rates in the United States are not as low as those historically experienced in the Netherlands, the current situation in the United States is similar to that of the Netherlands. To-date in the United States, the business case for chip-and-PIN has been lacking due to low fraud rates. Also, as our neighboring countries Canada and Mexico move to chip-and-PIN along with the rest of the developed world, the U.S. card industry is slow and late to migrate away from the mag stripe.

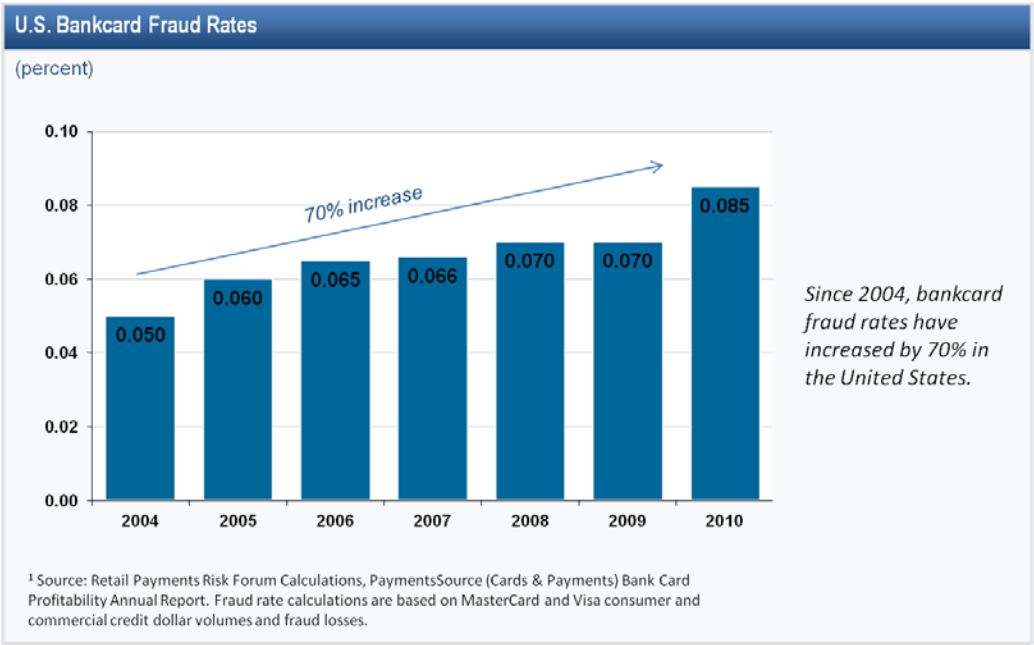
[k] Currence was founded in 2005 through an initiative by eight Dutch banks. Its purpose is to facilitate a competitive market and transparency while preserving the quality and security of the payment systems of the Netherlands.

IX. Card Fraud Trends in the United States

While markets that have migrated, or are in the process of migrating, to EMV chip-and-PIN have seen a significant decrease in fraud on chip-and-PIN transactions, overall fraud levels in the United States are trending upward. Unlike the other countries discussed in this paper, the United States does not have a single entity that collects and reports comprehensive card fraud data. Therefore, it is difficult to fully measure total fraud losses and fraud losses by specific types of fraud such as CNP or counterfeit fraud. However, there are limited studies and anecdotal evidence that point to rising fraud losses and rates for U.S. payment cards. And while no single factor can be attributed to the rising fraud trend on payment cards in the United States, the card industry's reliance on mag stripe technology is certainly a factor in this trend.

Since 2004, the fraud rate on bankcards[l] issued in the United States has increased by 70 percent. The fraud rate on bank cards in 2004 was .05 percent, and by the end of 2010, the fraud rate on bank cards stood at .09 percent. In fact, 2010 represented the first year that the fraud rate on U.S.-issued bankcards exceeded the fraud rate on UK-issued cards.

Chart 17: U.S. Bankcard Fraud Rates

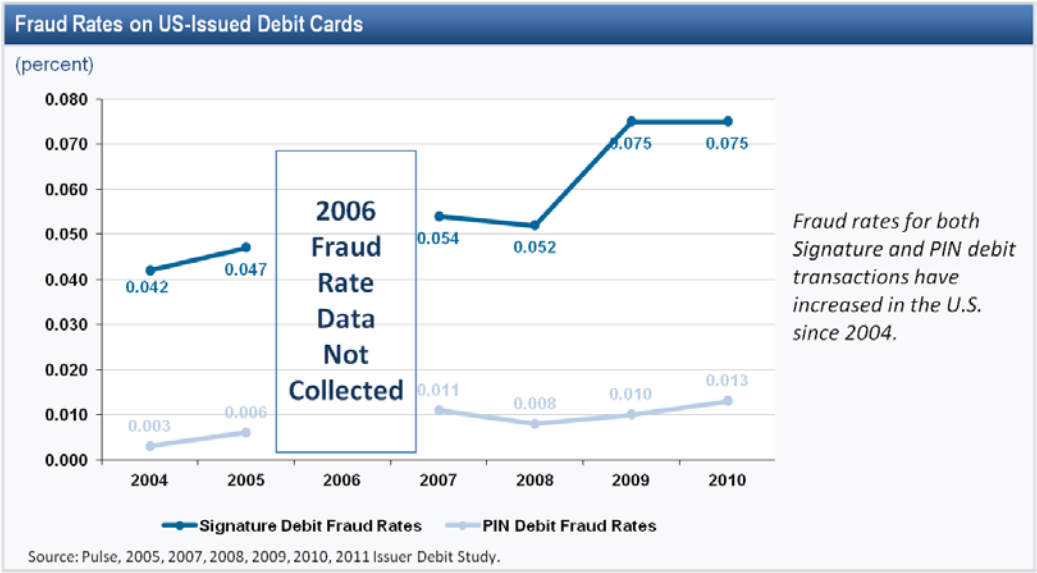


Debit cards are also experiencing an increase in fraud rates. According to annual debit issuer studies conducted for Pulse,[m] both signature and PIN debit fraud rates have increased significantly since 2004. Signature debit fraud rates have increased by nearly 80 percent since 2004, climbing from .04 percent to .08 percent by 2010. The fraud rate on signature debit

[l] Bankcards are MasterCard and Visa-branded consumer and commercial credit cards issued by financial institutions. Bankcards do not include credit cards issued by American Express and Discover or any debit cards.
[m] Pulse is an ATM/debit network owned by Discover Financial Services. The network serves more than 4,400 financial institutions in the United States.

transactions is closely aligned with the fraud rate of bankcards. Fraud rates on PIN debit transactions are significantly lower than those of signature debit or bankcards. However, PIN debit fraud rates have increased more than threefold since 2004, growing from 0.003 percent to 0.013 percent by 2010.

Chart 18: Fraud Rates on US-Issued Debit Cards



Coinciding with rising fraud rates, the reported incidences of card data breaches remain high. These breaches have been highly prominent in the news, culminating most recently in May with the announcement from Michaels Stores Inc. Michaels announced that PIN debit payment terminals had been tampered with by fraudsters, resulting in a breach of debit card and PIN data at its stores across the United States. According to a 2011 Data Breach Report, "these attacks have been occurring for years, but are on rise in many areas according to both public reports and the caseload of the U.S. Secret Service."[25]

Card skimming is becoming more widespread in the United States as payment cards issued here continue to rely on mag stripe technology while the rest of the world moves to chip technology. In fact, physical tampering/skimming threats accounted for nearly 30 percent of the data breaches received by the U.S. Secret Service in 2010 up from approximately 10 percent in 2007. In 2010, only Malware threats accounted for more data breaches than tampering/skimming threats.[26] As seen in available data from countries that have adopted EMV chip-and-PIN, chip cards have been highly effective at reducing card skimming and ultimately counterfeit card fraud.

X. Conclusion

Chip-and-PIN cards have been successful in thwarting counterfeit and lost or stolen card fraud in the card present environment. However, a clear pattern of fraud migration from chip-and-PIN enabled transactions to non-chip-and-PIN transactions, namely CNP and mag stripe (be it another market or another product within market) transactions exists. For a chip-and-PIN migration in the United States to have a successful impact on reducing total card fraud, the entire payment card industry needs to be coordinated with regards to product issuance and acceptance as well as solutions for mitigating CNP fraud.

As evidenced in every country where data was available, CNP fraud increased as face-to-face fraud fell, initially resulting in little to no impact in overall card fraud. In countries where CNP fraud is now being lowered, merchants have adopted fraud prevention measures that require 3-D Secure for CNP transactions. However, the 3-D Secure protocol is not unique to chip-and-PIN cards as it can also be integrated with mag stripe cards. Though new technology specific to chip-and-PIN cards to reduce CNP fraud is available, it has not been widely deployed due in part to the success of the 3-D Secure protocol. It will be imperative for the U.S. payments industry to adopt CNP fraud solutions in order to combat this fraud migration phenomenon should the industry decide to migrate to chip-and-PIN.

Cross-border card fraud is increasing as fraudsters seek an opportunity to counterfeit cards in chip-and-PIN markets and then use these cards in markets still relying on mag stripe technology. Should the U.S. industry continue to rely on mag stripe cards, it is reasonable to expect fraud committed in the United States on foreign-issued cards to increase as long as foreign issuers continue to issue cards with both chips and mag stripes. In response to this dynamic, the European Central Bank is recommending that beginning in 2012, all newly issued Single Euro Payments Area payment cards should be issued as chip-only cards.[27] If the U.S. payments industry decides to migrate to chip-and-PIN, cross-border fraud on U.S.-issued cards should be a minimal issue given the mass migration to chip-and-PIN in the rest of the world.

Based on the experiences of chip-and-PIN migrations in other countries, it is imperative that all card based products should be migrated at, or near, the same time to have a positive impact on reducing face-to-face fraud within a country's borders. As witnessed in Canada, migrating credit before debit resulted in a significant increase in fraud perpetrated with debit cards, ultimately resulting in a minimal reduction of total card fraud. If the United States migrates to chip-and-PIN without market consensus, agreement, or in a timely and concerted effort; those issuers, networks, or merchants who are slow to migrate will see increased fraud levels and the impact on overall fraud levels could be minimal.

Complicating a full U.S. migration to chip-and-PIN is the prevalence of signature verification in the United States. In fact, the largest card issuers that have announced plans to issue EMV cards will be issuing chip cards that support signature verification. And in Visa's plan to move its

network participants to the EMV standard, the network remains committed to both signature and PIN verification. A move away from mag stripe cards to chip cards would have a positive impact on counterfeit card fraud in the United States. Maintaining signature as a cardholder verification method for EMV chip cards might not have a similar positive impact on lost or stolen card fraud as experienced in chip-and-PIN countries. However, a U.S. migration to an EMV chip-based environment, regardless of the cardholder verification method, will provide a more secure payment environment.

Finally, should the U.S. payments industry continue to rely on mag stripe technology as long as possible, a scenario similar to the Netherlands experience could occur in the United States. While the business case didn't exist for the Dutch when its European counterparts were migrating, the business case rapidly changed by the time most of Europe had migrated and fraud in the Netherlands subsequently increased significantly. With a clear pattern of fraudsters targeting non-chip transactions, the United States faces a significant risk of continued escalating fraud rates as long as the payments industry relies on mag stripe technology.

References

[1] EMVCo.

[2] IBID.

[3] IBID.

[4] Murdoch, S.J, S. Drimer, R. Anderson, and M. Bond, "Chip and PIN is Broken." 2010 IEEE Symposium on Security and Privacy, http://www-test.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf, accessed on October 4, 2011.

[5] "Debit Card Interchange Fees and Routing," 12 CFR Part 235 Regulation II; Docket No. R-, December 16, 2010, http://www.federalreserve.gov/boarddocs/meetings/2010/20101216/20101216_InterchangeFeeProposedRuleDRAFTFRNotice.pdf, accessed October 4, 2011.

[6] "SECU leads in the US with the addition of EMV Card Chip Technology," State Employees' Credit Union Press Release, February 17, 2011, https://www.ncsecu.org/PDF/Press/20110217_EMVCardChipTechnology.pdf, accessed October 4, 2011.

[7] "Visa Announces Plans to Accelerate Chip Migration and Adoption of Mobile Payments," Visa Inc. Press Release, http://corporate.visa.com/media-center/press-releases/press1142.jsp, accessed October 4, 2011.

[8] Ponemon Institute, "PCI DSS Trends 2010: QSA Insights Report," March 2010, http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/PCI%20DSS%20Trends%20-%20QSA%20Insights%20010310.pdf, accessed on October 4, 2011.

[9] Financial Fraud Action UK, "Fraud the Facts 2011 The Definitive Overview of Payment Industry Fraud and Measures to Prevent It," http://www.financialfraudaction.org.uk/Publications/#, accessed on October 4, 2011.

[10] Jeffrey Green, "2006 Bankcard Profitability Study & Annual Report, *Cards & Payments*, May 2006, pp. 31-32.

[11] APACS Reports UK Chip and PIN Success, August 14, 2006, Payments News Glenbrook Partners, http://www.paymentsnews.com/2006/08/apacs_reports_u.html, accessed on November 3, 2011.

[12] EMVCo.

[13] Bell ID, "Six Myths Preventing EMV Migration in the U.S. Fact vs. Fiction, http://www.finextra.com/Finextra-downloads/featuredocs/White%20Paper%20-%20EMV%20Migration%20US%201.9.pdf, accessed on October 4, 2011.

[14] Nathalie Ha, "EMV: Challenges & Best Practices" (presentation, Banking Vietnam 2009 Conference, Hanoi, Vietnam, May 27-29, 2009).

[15] "Payment industry comes together to ensure smooth migration to chip technology in Canada," Interac Association Press Release, March 13, 2006, http://www.interac.ca/media/press_5.php, accessed on October 4, 2011.

[16] Philip Andreae and Associates, "The Canadian Migration to EMV," September 2006, http://www.andreae.com/presentation/The%20Canadian%20Migration%20to%20EMV%20sept%202006.pdf, accessed on October 4, 2011.

[17] Kate Fitzgerald, "Amex Sets Date of Canada EMV Liability," *American Banker*, August 27, 2010, http://www.americanbanker.com/issues/175_166/amex-emv-canada-1024728-1.html, accessed October 4, 2011.

[18] John Hill and Victoria Conroy, "EMV: the story so far," *Cards International*, April 13, 2009, http://www.vrl-financial-news.com/cards--payments/cards-international/issues/ci-2009/ci419/emv-the-story-so-far.aspx, accessed on November 3, 2011.

[19] "EFTPOS Moves to Chip For Enhanced Security and Functionality," EFTPOS Payments Australia Limited Press Release, June 3, 2010, http://www.eftposaustralia.com.au/docs/media-releases/eftpos-moves-to-chip-for-enhanced-security-and-functionality.pdf, accessed on October 4, 2011.

[20] "MasterCard Announces Five Year Plan to Change the Face of the Payments Industry in Australia," MasterCard Worldwide Press Release, March 29, 2011, http://www.mastercard.com/au/general/en/aboutus/press/payment_industry_fiveyearplan.html , accessed on October 4, 2011.

[21] "Visa International Operating Regulations April 10, 2011," Visa Inc., p. 181.

[22] "Payments Monitor," Australia Payments Clearing Association, Second Quarter 2011, http://www.apca.com.au/PM/2011_Quarter2/index.html, accessed on October 4, 2011.

[23] "From Stripe to Chip: EMV (January 2004 version)," Technology Study Group of the Social Forum on the Payments System, http://www.dnb.nl/en/binaries/From%20stripe%20to%20chip%20-%20EMV_tcm47-145653.pdf, accessed on October 4, 2011.

[24] Currence, 2010 Annual Report, p. 26, http://cloud.reportsir.com/reports/41/2011622173740/default.htm, accessed on October 4, 2011.

[25] "2011 Data Breach Investigations Report," A Study Conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit, http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf, accessed on October 4, 2011.

[26] IBID.

[27] "Seventh Progress Report Beyond Theory Into Practice," European Central Bank, Single Euro Payments Area, October 2010, http://www.bundesbank.de/download/zahlungsverkehr/sepa_fortschrittsbericht.en.pdf, accessed on October 4, 2011.