Congressional Research Service
Informing the legislative debate since 1914

The EMV Chip Card Transition: Background, Status, and Issues for Congress

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

February 26, 2015

Congressional Research Service
7-5700
www.crs.gov
R43925

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Consumer financial card fraud due to data breaches of card information is an ongoing problem in the United States. The majority of breaches are carried out against point-of-sale (POS) systems, and are facilitated by what many consider to be the weak link in the U.S. retail sales payment process: the continued use of magnetic stripe cards (also referred to as stripe-and-signature cards). These cards are what most U.S. consumers think of when referring to financial cards.

In much of the rest of the world, cards that provide a much higher level of security for conducting sales transactions are used: *EMV cards*, named for the coalition of Europay, MasterCard, and Visa (the EMV Coalition or EMVCo) that developed the specifications for the system in the 1990s. EMV cards store card information on an embedded microchip and are more commonly called *chip cards*. With these cards, instead of swiping and signing to make a payment, the cardholder inserts the card into the POS machine, then either enters a personal identification number (PIN) or signs to verify the transaction. Fraud is significantly more difficult to carry out against chip cards, but financial institutions in the United States have until recently issued stripe cards almost exclusively.

In an effort to decrease fraud, MasterCard and Visa set a deadline of October 1, 2015, for U.S. financial card issuers (e.g., banks, credit unions) to replace magnetic stripe cards with EMV cards and for merchants to begin accepting them. Other card brands followed suit and have also imposed the October 1, 2015, deadline. The transition will also make U.S.-issued cards compatible with POS systems and automated teller machines in much of the rest of the world. After the deadline, the liability for fraudulent transactions involving magnetic stripe cards will be shifted to the party that has not switched to chip cards. As the date approaches, exploring the ramifications of the transition—or the failure to transition—will become increasingly important.

A number of issues delayed transition planning and still could possibly delay a full transition: the high cost of the transition, the minimal implementation to date, technical and regulatory uncertainty, and disagreement over the verification method to be implemented.

In the 113th Congress, the Senate held one hearing and the House held two hearings related to data breaches. During each of those hearings, Members asked questions related to how EMV technology could affect the frequency and seriousness of data breaches and the progress being made towards a full EMV migration in the United States. There were four bills that addressed credit card theft and data breach reporting, specifically, although none were enacted. The 114th Congress may examine the transition and its effectiveness to determine whether any legislative action is needed, especially if major breaches continue to occur despite the transition.

Contents

Figures

Contacts

Introduction

MasterCard and Visa—also called "payment brands"[1]—have set a deadline of October 1, 2015, for U.S. card issuers—banks and credit unions—to replace existing credit and debit magnetic stripe cards with chip cards, and for merchants to begin accepting them.[2] Chip cards are formally known as "EMV" cards, named for the coalition of three companies, Europay, MasterCard, and Visa, that developed the specifications for the standard. EMVCo membership has now expanded to include the payment brands of American Express, JCB, Discover, and UnionPay.[3]

The EMV chip carries cardholder and account data, and is programmed to make decisions about a transaction and control its outcome, i.e., approve or decline it.[4] Chip cards can be produced as "chip-and-PIN," "chip-and-signature," or "chip-and-choice" (which allows the use of either a personal identification number (PIN) or signature). Transactions are verified in the method programmed into the chip.[5] If the card is to have a PIN associated with it, the PIN is programmed into the chip before it is embedded in the card and sent to the cardholder.

EMV[6] is the global standard for the chip technology embedded in financial payment cards. Much of the rest of the world—Europe, Canada, Latin America, and the Asia-Pacific region—is already in the process of transitioning to chip cards. In the fourth quarter of 2012, there were 1.62 billion chip cards in use across 80 countries,[7] leaving the United States as the last major country to implement what is now the de facto global standard.

U.S. consumers increasingly rely on credit and debit cards to pay for goods and services. Between 1997 and 2011, card payments rose from accounting for 23% of payments to 48%.[8] During the same period, payment by cash and checks dropped from 70% to 35%.[9] In 2011, consumers made 49 billion debit transactions totaling $1.8 trillion and 26 billion credit transactions totaling $2.1 trillion.[10] This shift makes card security and fraud prevention more important than ever, and EMV

[1] The payment brands do not issue credit or debit cards. The cards themselves are issued by card issuers.

[2] Visa announced the deadline in August 2011 and MasterCard did so in January 2012.

[3] EMVCo FAQ, http://www.emvco.com/faq.aspx?id=37. The transition also applies to the 16 independent regional debit networks (e.g., NYCE, STAR, Shazam).

[4] The program can also require an "offline" transaction to go "online" to get approval depending on various risk situations defined on the chip. An offline transaction does not require the use of telecommunications, while an online transaction does. In other words, an offline transaction does not necessarily require the POS reader to contact the card issuer's system for approval—but, depending on what rules have been embedded on the chip, it may force the transaction online for a decision on whether to approve it.

[5] Chip-and-signature cards are generally accepted everywhere chip-and-PIN cards are, with the exception of certain unmanned payment terminals equipped to take chip cards (e.g., gas stations, parking payment kiosks).

[6] Because the specifications were developed by EMVCo, chip cards—whether they use a PIN or signature for authentication—are also commonly called "EMV cards."

[7] "Continued Market Adoption of EMV Technology," *EMVCo Newsletter*, May 2013, http://www.emvco.com/newsletters/2013-May.html#section2. (Hereinafter "Continued Market Adoption of EMV Technology," *EMVCo Newsletter*.)

[8] "Debit Card Interchange Fee Regulation: Some Assessments and Considerations," *Federal Reserve Bank of Richmond Economic Quarterly*, Third Quarter 2012, http://www.richmondfed.org/publications/research/economic_quarterly/2012/q3/pdf/wang.pdf. (Hereinafter "Debit Card Interchange Fee Regulation," *FRB-Richmond Economic Quarterly*.)

[9] "Debit Card Interchange Fee Regulation," *FRB-Richmond Economic Quarterly*.

[10] "Debit Card Interchange Fee Regulation," *FRB-Richmond Economic Quarterly*.

cards offer a significantly higher level of data security than stripe cards: Data on the chip is secured using both hardware and software security measures, so even if the card data is compromised, the chip itself will still be difficult to counterfeit.

The cost of the transition in the United States is expected to be at least $6 billion,[11] but the costs for issuers and merchants that do not meet the adoption deadline could be even greater: After the deadline, the liability for fraudulent transactions will shift to the party that has not switched to chip cards.[12] For example, if a merchant does not accept chip cards and the customer has a chip card, the transaction will still be processed using the magnetic stripe still present on the back of the card, but the merchant will bear responsibility for any fraudulent activity. If the merchant has a chip point-of-sale (POS) terminal, but the bank has not issued a chip card to the customer, the bank will be liable. If neither or both parties have complied, the fraud liability will remain the same as it is today. Historically, the issuer has paid about 60% of losses and retailers have paid 40%. Issuers picked up most of the losses when the card was present but was fraudulent, while merchants picked up the bulk of losses when cards were not present.[13]

As the October 1, 2015, deadline approaches, exploring and understanding the ramifications of the transition—or the failure to transition—is likely to become increasingly important for Congress, especially if additional major breaches occur.[14] There are many policy issues related to EMV adoption in the United States and elsewhere in the world. This report describes the financial harm caused by data breaches and explains how those breaches are carried out. It provides information about the effect of the transition in selected foreign countries. The report also discusses resolved and remaining impediments to completing the EMV transition in the United States and identifies areas of potential congressional interest.[15]

The Financial Impact of Card Fraud

Globally, card fraud totaled $11.3 billion in 2012, an increase of 15% from 2011. In the United States, although fraud constituted less than 1% of total expenditures, credit card losses totaled $5.33 billion, an increase of 14.5% from 2011.[16]

[11] "Will Losses in Consumer Confidence in Payments Accelerate EMV?," *n>genuity Journal*, March 18, 2014, http://www.tsys.com/ngenuity-journal/will-losses-in-consumer-confidence-in-payments-accelerate-emv.cfm. (Hereinafter "Will Losses in Consumer Confidence in Payments Accelerate EMV?," *n>genuity Journal*.)

[12] Gasoline retailers have been given an October 1, 2017, deadline due to the difficulty and cost of upgrading.

[13] Cardholders have historically been held responsible for less than 2% of fraudulent charges. "Who Pays When Merchants Are Victims of Credit Card Fraud?," NerdWallet Finance, June 3, 2014, http://www.nerdwallet.com/blog/tips/merchants-victims-credit-card-fraud/.

[14] The transition is more formally referred to as the "Debit/Credit U.S. Domestic and Cross-Border Counterfeit EMV Liability Shift for POS Transactions."

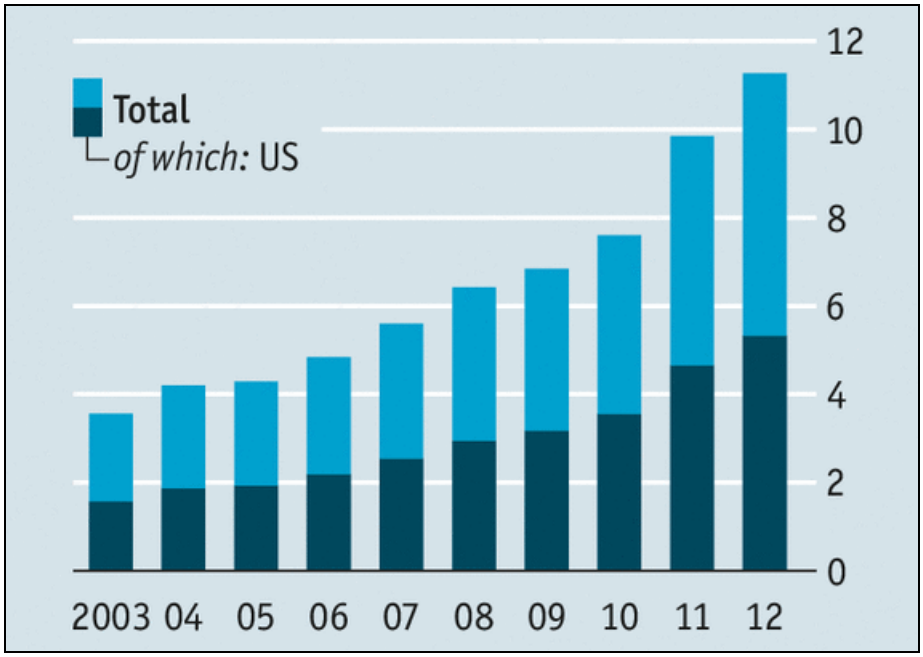
[15] This report addresses only "contact" payments made by swiping or inserting a credit or debit card. It does not address "contactless" payments made, for example, by holding a card (such as Visa's "payWave") or a mobile device in front of a reader.

[16] "Credit Card and Debit Card Fraud Statistics," CardHub, no date given, http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/, citing "2013 Federal Reserve Payments Study: Recent and Long-Term Payment Trends in the United States: 2003 – 2012," Federal Reserve System, December 19, 2013, http://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf.

The United States has been disproportionately affected by fraud: Since 2003, the United States has consistently accounted for about half of the total global loss, but for only about a quarter of the total volume of card payments (**Figure 1**).[17]

Figure 1. Global Losses Due to Card Fraud, 2003-2012

In Billions of Dollars



Source: "Skimming off the Top: Why America Has Such a High Rate of Payment-Card Fraud," Economist.com, February 15, 2014, http://www.economist.com/news/finance-and-economics/21596547-why-america-has-such-high-rate-payment-card-fraud-skimming-top, citing 2013 Nilson Report. The Nilson Report delivers global news and statistics about the payment industry.

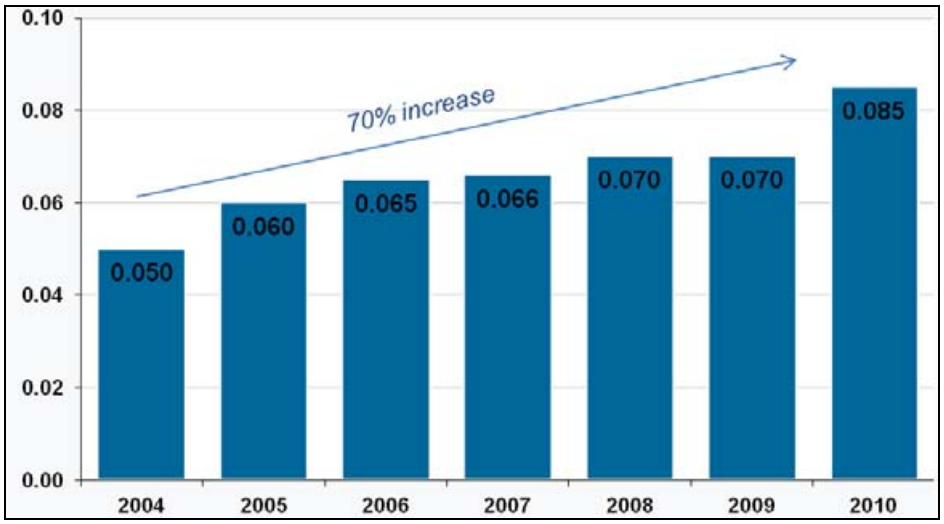
Between 2004 and 2010, fraud committed on U.S.-issued bank credit cards rose 70% (**Figure 2**). Debit card fraud also rose, with cards using a signature for verification accounting for 91% of the fraud and cards using a PIN for verification accounting for 9% (**Figure 3**).[18]

[17] "Skimming off the Top: Why America Has Such a High Rate of Payment-Card Fraud," Economist.com, February 15, 2014, http://www.economist.com/news/finance-and-economics/21596547-why-america-has-such-high-rate-payment-card-fraud-skimming-top. (Hereinafter "Skimming off the Top," Economist.com.)

[18] "PIN Authentication Versus Signature Authentication," Retail Payments Risk Forum, January 23, 2012, http://portalsandrails.frbatlanta.org/2012/01/pin-authentication-vs-signature-authentication.html.

Figure 2. U.S. Bank Credit Card Fraud Rates, 2004-2010

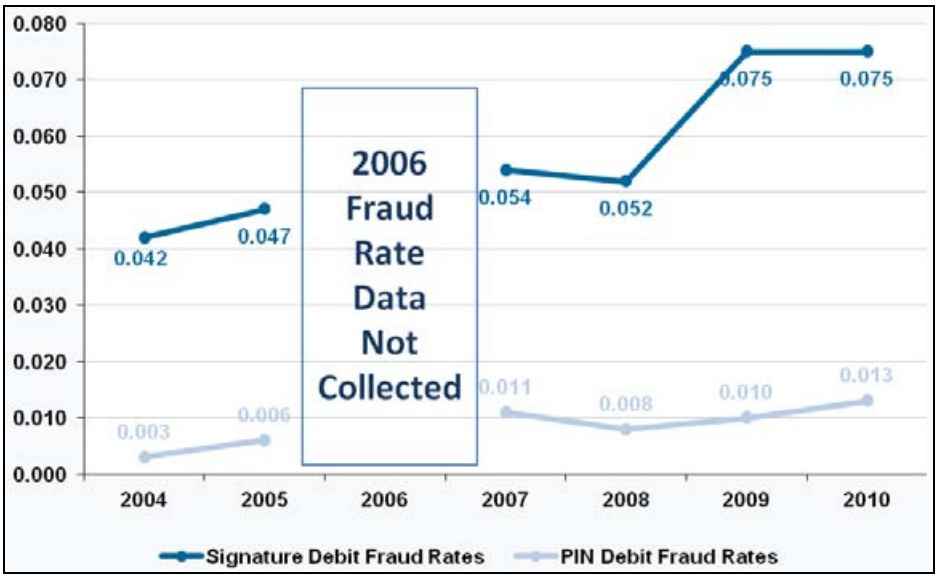
Fraud Rate as Percent of Total Transactions, by Year



Source: *Chip-and-PIN: Success and Challenges in Reducing Fraud*, Douglas King, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, January 2012, http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf.

Figure 3. U.S. Debit Card Fraud Rates: Signature vs. PIN Verification, 2004-2010

Fraud Rate per Card Type, Percent of Total Transactions, by Year



Source: *Chip-and-PIN: Success and Challenges in Reducing Fraud*, Douglas King, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, January 2012, http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf.

Card Fraud and Point-of-Sale Intrusion Data Breaches

Card fraud can be conducted in a number of ways, but it always begins with the theft of card information. The scale of the theft can range from small, such as stealing a wallet, to large, such as skimming or a data breach. Data breaches can be carried out in more than one way (and for reasons other than committing fraud), but the most common method is hacking into a POS system used to make card-based purchases. These breaches are called "POS intrusions."[19] In 2013, 75% of breaches in the travel/hospitality sector and 31% in the retail sector were POS intrusions aimed at stealing credit and debit card data.[20]

POS intrusions and the ensuing card fraud are facilitated by what many consider to be the weak link in the U.S. card payment process: the continued use of magnetic stripe cards that carry unencrypted data. A hacker can gain access to a company's POS systems in a number of ways. Sometimes the hacker will use a "brute force" approach, systematically checking all possible keys or passwords until the correct one is found, or exploiting inadequately managed Internet connections to the POS system. Another common way is through the use of stolen third-party (vendor) credentials (sign-on information).[21] For example, some POS system vendors do not change the default password to access the system. That password is often included in the system documentation, making it easy for anyone, especially a hacker, to find the information online.

Once the hacker has gained access to the computer system used to manage the POS system, he or she installs malware[22] that copies the unencrypted data on cards as they are swiped. The most common type of malware used in POS intrusions is called a "RAM scraper," so named because it allows the hacker to "scrape" data out of the memory of the POS system. The RAM scraper exploits the very brief period that the card data is in the POS reader, before it is encrypted and sent to complete the payment process.

[19] POS intrusion data breaches are not the only method available to steal card information, and they are not solely committed for the purpose of card fraud. Data breaches can also be carried out by (1) hacking into databases that store customer information (e.g., grocery store discount cards); (2) compromising web-based applications to steal logon credentials or other user or account information (e.g., a banking website); and (3) "skimming," carried out with hardware installed on individual POS readers to steal information as individual cards are swiped (e.g., ATMs, gas stations, unsupervised kiosks). Although chip cards can also reduce the theft of card information through web application attacks and card skimming, POS intrusions are the most significant threat in the retail and travel/hospitality sectors. While still conducted for the purpose of committing fraud, web application attacks and skimming are a greater threat in the financial sector and are more often intended to collect account credentials rather than card data. Data breaches are also conducted for reasons other than financial card fraud, specifically, (1) government and corporate cyber-espionage; (2) identity theft; and (3) attacks driven by ideology or politics. Verizon Corporation, *2014 Data Breach Investigations Report*, May 2014, http://www.verizonenterprise.com/DBIR/2014/. (Hereinafter *2014 Data Breach Investigation Report*, Verizon.)

[20] The most common type of intrusions into retail websites are web app attacks that allow the hacker to carry out denial of service (DoS) attacks. DoS attacks are intended, in general, to keep customers or other users from accessing the site. These attacks are more often carried out for ideological, rather than financial purposes (65% versus 33%). *2014 Data Breach Investigation Report*, Verizon.

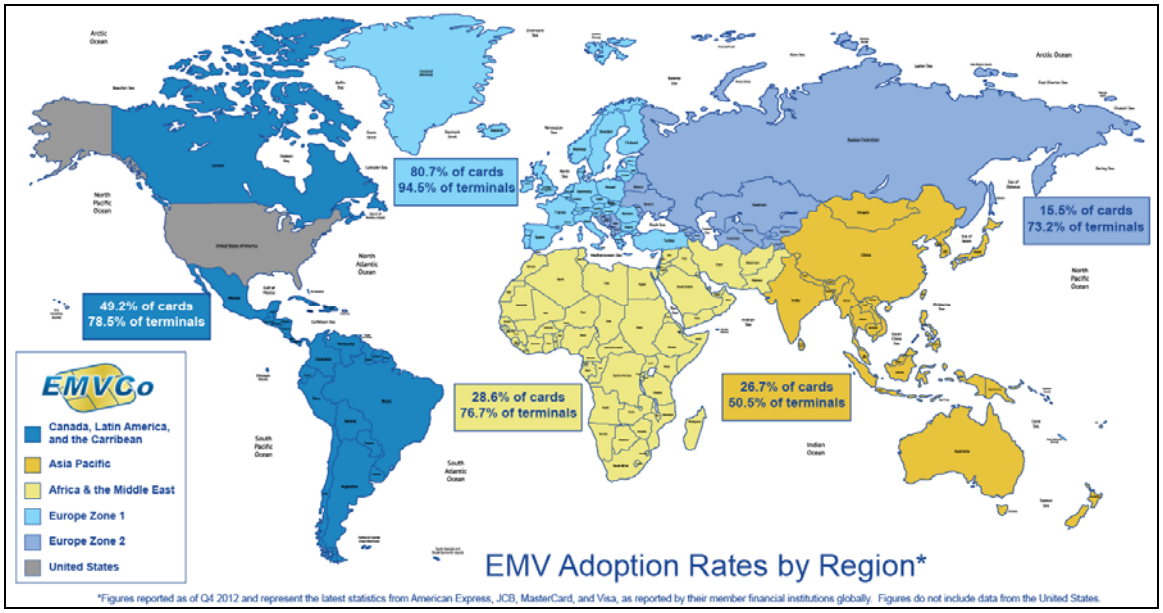
[21] A third way is to attack and infect a corporate site with malware and gain access to the POS system in that manner. This is not a common method used to steal financial card data. *2014 Data Breach Investigations Report*, Verizon.

[22] Malware is short for "malicious software." It is software designed to cause damage or carry out other unwanted actions on a computer system.

EMV Adoption in Selected Countries: Impact on Fraud

Europe has transitioned between about 73%[23] and 80%[24] of cards and about 95% of POS terminals to EMV technology.[25] Other regions around the world have transitioned to varying degrees (**Figure 4**).

Figure 4. Status of Worldwide EMV Adoption Rates by Region, Fourth Quarter, 2012



Source: EMVCo, Worldwide EMV Card and Terminal Deployment, Fourth Quarter, 2012, http://www.emvco.com/about_emvco.aspx?id=202.

A 2012 study of five countries by the Federal Reserve Bank (FRB) of Atlanta examined fraud trends experienced by the United Kingdom, Canada, France, Australia, and the Netherlands as they transitioned from stripe cards to chip-and-PIN cards; none of the countries studied issued chip-and-signature cards.[26] Three of the five countries studied in the report experienced decreases in both the rates and total amounts of card fraud (**Figure 5**), with some exceptions attributed to factors other than the security of the chip itself. For example, when the United Kingdom began issuing chip cards, the cards continued to carry a magnetic stripe, too. If the card was swiped to make a purchase and the card data was compromised, it could be used in card-not-present (CNP) environments or to make counterfeit cards for use in non-chip countries.

[23] *Chip-and-PIN: Success and Challenges in Reducing Fraud*, Douglas King, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, January 2012, http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf. (Hereinafter *Chip-and-PIN: Success and Challenges*, Federal Reserve Bank of Atlanta.)

[24] "Continued Market Adoption of EMV Technology," *EMVCo Newsletter*.

[25] "Continued Market Adoption of EMV Technology," *EMVCo Newsletter*.

[26] *Chip-and-PIN: Success and Challenges*, Federal Reserve Bank of Atlanta.

Figure 5. Country Trends in Card Fraud After Adopting Chip-and-PIN Cards

	United Kingdom	Canada	France	Australia	Netherlands
Overall Trend	Decrease after initial increase	Decrease after initial increase	Increase	Increase	Decrease after initial increase
Card-Present Fraud	Decrease after initial increase	Decrease	Decrease	Not Reported	Not Reported
Counterfeit Card Fraud	Decrease after initial increase	Decrease	Not Reported	Decrease after initial increase	Not Reported
Lost and Stolen Card Fraud	Decrease		Not Reported	Not Reported	Not Reported
Domestic CNP Fraud	Decrease after initial increase	Increase	Decrease	Increase	Not Reported
Cross-Border CNP Fraud	Decrease after initial increase		Increase	Not Reported	Not Reported

Source: Data collated by CRS from *Chip-and-PIN: Success and Challenges in Reducing Fraud*, Douglas King, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, January 2012, http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf. Data was collected over different spans of time between 2004 and 2010.

Note: Green cells indicate that a particular type of fraud decreased after the introduction of chip-and-PIN cards. Red cells indicate that a particular type of fraud increased after the introduction of chip-and-PIN cards. "Decrease after initial increase" means that fraud initially increased for a period of one to three years and then decreased significantly.

Fraud Reduction

The data analyzed in the study[27] showed that chip-and-PIN is most effective in reducing certain types of fraud, notably—

- *card-present fraud*;
- *domestic counterfeit card fraud*, committed by manufacturing cards created with valid information from lost or stolen cards, but most often carried out using data stolen in a data breach or "skimming"; and
- *lost and stolen card fraud*, committed using an original, activated, and valid card after it is lost or stolen, in both "card present" (e.g., retail) and certain "card-not-present" (e.g., Internet purchase) scenarios.

Additionally, *mail non-receipt fraud,*[28] committed by stealing a card before it is activated by the rightful owner, has also decreased with the introduction of chip cards. For example, since 2004, this type of fraud has decreased 91% in the United Kingdom.[29]

[27] *Chip-and-PIN: Success and Challenges*, Federal Reserve Bank of Atlanta.

[28] Mail non-receipt fraud is also called "Not Received as Issued (NRI)" fraud. This type of fraud was not specifically addressed in the FRB Atlanta study.

[29] EMV FAQ, EMV Connection, no date provided (but published after 2012), http://www.emv-connection.com/emv-faq/#q12.

Most U.S. issuers have stated that they plan to issue chip-and-signature credit cards, rather than chip-and-PIN cards. It is uncertain how this decision may affect fraud in the United States.[30]

Fraud Migration

In all but one of the countries studied (France), the switch to chip cards caused two types of fraud to increase:

- *domestic CNP fraud*, e.g., catalog or Internet purchases, and
- *cross-border counterfeit card fraud*.[31] This type of fraud uses data stolen from cards issued in chip countries to produce physical counterfeit cards for use in non-chip countries.

This is a phenomenon referred to as "fraud migration," with the fraud migrating primarily to the United States, the last major market to transition to chip cards.

Mitigating CNP Fraud

In the countries where CNP fraud eventually decreased, many merchants have adopted fraud prevention measures. There are two simple prevention measures: requiring cardholders to authenticate their identities by entering the card's

- verification/security code and/or
- expiration date.

A card's security code and expiration are shown only on the card and are not encoded on either the magnetic stripe or the EMV chip. An additional measure is "Address Verification Service" (AVS). AVS matches the billing address information provided at check-out with that on file with the card issuer.[32]

Other options to mitigate CNP fraud are also available and have been adopted in varying degrees. Some of these are discussed below.

[30] The only data available are for stripe debit transactions. Between 2004 and 2010, signature verification accounted for 10 times the amount of fraud than PIN verification (91% versus 9%). However, those figures cannot be used to reliably predict chip card impact on fraud: even with signature verification, chip cards will still offer greatly improved security and are expected to eliminate much of the counterfeit card fraud currently being conducted in the United States. "PIN Authentication Versus Signature Authentication," Retail Payments Risk Forum, January 23, 2012, http://portalsandrails.frbatlanta.org/2012/01/pin-authentication-vs-signature-authentication.html. (Hereinafter "PIN Authentication Versus Signature Authentication," Retail Payments Risk Forum.) Also see **Figure 1**.

[31] *Chip-and-PIN: Success and Challenges*, Federal Reserve Bank of Atlanta.

[32] AVS is used predominantly in the United States. Quattro Processing Services, *Mitigating Fraudulent CNP Transactions: Examination of Safeguards*, est. 2013, http://www.quatrroprocessing.com/whitepapers/Whitepaper-CNP-Transactions.pdf. (Hereinafter *Mitigating Fraudulent CNP Transactions: Examination of Safeguards,* Quattro Processing Services.)

3-D Secure

Visa, MasterCard, and American Express have developed and adopted proprietary security measures to make CNP fraud more difficult to perpetrate: Verified by Visa, SecureCode, and SafeKey, respectively. All three are based on the 3-D Secure protocol and are only used for Internet-based purchases.[33] They work by redirecting the payment transaction to the issuer's website to perform user authentication by requiring the cardholder to provide additional credentials before approving a transaction. The merchant, the cardholder, and the card issuer all must use the system for it to work. In 2013, only about 3% of U.S. merchants employed an authentication method based on 3-D Secure.[34]

The 3-D Secure protocol allows the card issuer to define what those credentials will be. For example, the cardholder might be required to enter a password. The password can be permanent or transaction specific. Transaction-specific passwords can be generated in a number of ways. Issuer-generated passwords can be sent via text message and email to the cardholder's registered mobile device and email account. This method can be used with both stripe and chip cards. With a chip card, the cardholder can generate a password by inserting the card into a cardholder-owned reader and entering the card's permanent PIN. The reader will then generate a one-time PIN for use with that specific transaction. In Europe, about 30 million people use chip cards and readers for Internet transactions.[35]

Although 3-D Secure provides an extra layer of security for CNP transactions, it still has vulnerabilities. For example, in the past, hackers successfully used malware to direct cardholders signing up for 3-D Secure to a fake enrollment window, allowing theft of the card data. While this specific vulnerability can be avoided using additional security methods, hackers are likely to continue looking for any vulnerability they can find and exploit in POS systems.

Other Options

There are also new security measures available that were developed by third-party companies not associated with the card companies. Two such examples are "D-FACTOR,"[36] by DeviceAuthority, and "TranSecure,"[37] a partnership between Quatrro and NorseCorp. Using D-FACTOR, cardholders link their credit cards to one or more devices, such as a mobile phone or home computer. Before a CNP purchase is approved, D-Factor verifies that the purchase is being made using a cardholder-registered device. TranSecure is not a transaction authentication method, but provides ongoing monitoring for fraud. This system uses fraud-detection software paired with

[33] 3-D Secure was originally developed by VISA. "3-D Secure: Verified by VISA / Mastercard Secure," PSBill, no date given, https://www.psbill.com/3-d-secure-verified-by-visa-mastercard-securecode.html.

[34] "EMV Is Not Enough: Considerations for Implementing 3-D Secure," TSYS, 2013, http://www.tsys.com/Downloads/upload/2013_TSYS_EMV_3D_Secure_Report_PC_Video_FinalV1.pdf.

[35] "Chip-and-PIN vs. Chip-and-Sig," Bankrate.com, August 13, 2013, http://www.bankrate.com/financing/credit-cards/chip-and-pin-vs-chip-and-sig/.

[36] "Information Technology Brief: Stronger User Security with Device-centric Authentication," published by XYPRO, provides a thorough overview of D-Factor, as well as many other multi-factor authentication measures. There is no publication date provided. The paper is available at https://www.xypro.com/whitepapers/Device-centric_Authentication_2013.pdf.

[37] *Mitigating Fraudulent CNP Transactions: Examination of Safeguards*, Quattro Processing Services.

fraud analysts to thwart CNP and other types of card fraud. Neither of these systems has been widely adopted at this time.

Mitigating Cross-Border Counterfeit Fraud

Cross-border counterfeit fraud increased in the countries studied by FRB Atlanta, as counterfeiters used data stolen in chip-and-PIN markets and produced stripe cards for use in those markets still using them. The FRB Atlanta report attributed the increase to issuers providing cards with both chips and magnetic stripes. For instance, when the United Kingdom transitioned to EMV cards, credit and debit cards were issued with both a chip and a magnetic stripe, which rendered them as easy to exploit and clone as stripe cards. The stolen data could then be used to manufacture counterfeit stripe cards for use in places such as the United States that still rely on magnetic stripe readers.[38] To mitigate this vulnerability, cards issued in the U.K. now include a small "flag" on the magnetic stripe to indicate that the card has a chip on it. When swipe card data is stolen, the flag would be copied along with the other stolen data onto the cloned card. The POS system would then recognize the flag when the card was swiped, alerting the merchant that a cloned card was being used.

The United Kingdom and Australia reported an initial increase in counterfeit fraud after EMV implementation, but it later decreased. The United States could have some "immunity" from such an increase: Since the United States is the only remaining major market still using stripe cards, there will not be any other major markets where stolen information can be used. Unlike CNP fraud, counterfeit fraud appears to diminish as more countries eliminate stripe cards.

EMV Adoption in the United States: Drivers

There are four significant drivers of EMV adoption in the United States:

- **Liability Shift.** The October 1, 2015, deadline shifting liability to the party that has not switched to chip cards is expected to be a strong incentive for merchants and issuers to make the switch.
- **Increasing Financial Impact of Fraud.** In 2012, credit card losses in the United States totaled $5.33 billion, an increase of 14.5% from 2011.[39] Between 2004 and 2010, fraud using U.S.-issued bank credit cards rose 70%. Merchants, card issuers, and consumers are adversely affected by increases in fraud.[40]
- **Increasing Concern over Data Breaches.** Although the number of breaches dipped significantly between 2011 and 2012, there has been a modest increase between 2012 and 2013.[41] Although the number of incidents in 2013 (198) is small compared to 2011 (855),[42] a lot of attention has been paid to those breaches

[38] *Chip-and-PIN: Success and Challenges*, Federal Reserve Bank of Atlanta.

[39] "Skimming off the Top," Economist.com.

[40] *Chip-and-PIN: Success and Challenges*, Federal Reserve Bank of Atlanta.

[41] *2014 Data Breach Investigations Report*, Verizon.

[42] Verizon Corporation, *2012 Data Breach Investigations Report*, May 2012, http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf.

in the news. That attention appears to have created the perception that the number of breaches is increasing more than it actually is, raising concern among consumers, as well as policymakers.

- **Better Security for Cards and Transactions.** Chip cards make data stolen in a breach much more difficult to use: Counterfeiting is significantly more difficult than with stripe cards. Most observers, including the FRB, agree that chip cards, "regardless of the verification method used, will provide a more secure payment environment."[43]

EMV Adoption in the United States: Impediments

The cost of the EMV transition and the current slow pace of adoption, as well as other issues in varying stages of being resolved, may hamper efforts to meet the October 2015 deadline.

Disagreements over transaction verification methods for credit transactions, chip programming, and the fee structure for debit transactions have all played roles in delaying EMV transition planning and adoption over the past year. Most issues appear to have been resolved through industry negotiation or litigation.[44]

High Cost of Implementation

Both card issuers and merchants in the United States have balked at transitioning to chip cards. They have already made significant financial investments in existing technology, and the transition will impose immediate, short-term costs on them. The cost of the transition to chip cards for financial institutions and businesses that use POS readers will be significant. Although opinions differ greatly as to the actual amount, most industry observers agree that it will cost between $6 billion[45] and $8 billion.[46] Of that amount, 75% is likely to be paid by merchants, making the transition three times as expensive for them as for the issuers.[47]

Costs for Card Issuers: Chip and Card Production

Some analysts have stated that manufacturing chip cards costs between $1.00[48] and $4.00[49] per card—2 to 16 times as much as traditional stripe cards, which cost about 25¢[50] to 50¢ each.[51]

---

[43] *Chip-and-PIN: Success and Challenges*, Federal Reserve Bank of Atlanta.

[44] The legal case is discussed in "Debit Transaction Fees: Regulatory Uncertainty," pp. 12-13.

[45] "Will Losses in Consumer Confidence in Payments Accelerate EMV? " *n>genuity Journal*.

[46] "EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions," First Data Corporation, 2011, http://www.firstdata.com/downloads/thought-leadership/EMV_US.pdf.

[47] For example, Target expects its total cost, including installing terminals in its 1,800 U.S. stores, to be about $100 million. "Will Losses in Consumer Confidence in Payments Accelerate EMV? " *n>genuity Journal*.

[48] "Littleton Firm Chips in on Security Solution," *Denver Business Journal*, May 9, 2014, http://www.bizjournals.com/denver/print-edition/2014/05/09/cover-story-littleton-firm-chips-in-on-security.html?page=all. (Hereinafter "Littleton Firm Chips in on Security Solution," *Denver Business Journal*.)

[49] "From Stripes to Chips," Wallaby Blog, February 10, 2014, https://www.walla.by/blog/76236922959/from-stripes-to-chips-an-evolution-of-our-plastic. (Hereinafter "From Stripes to Chips," Wallaby Blog.)

[50] "Littleton Firm Chips in on Security Solution," *Denver Business Journal*.

Adding to that cost, personalizing the card with the holder's name and other details is about twice as expensive with chip cards as with stripe cards.[52] While the issuing institution would pay initially for the chip and personalization of the card, those costs might be passed down to the consumer. Issuers will also face consideration of the one-time and ongoing costs associated with each type of implementation.

Costs for Merchants: POS System Replacement

In addition to the costs to issuers of producing the cards, merchants will have to purchase new POS equipment (i.e., chip readers) able to process chip card transactions. Cost estimates range from about $100[53] to $600[54] each, depending on the number ordered and specific product features. Current stripe readers cost approximately $50 to $100 when purchased individually,[55] but less than $20 when purchased in bulk.[56]

Minimal Implementation to Date

There are about 1.1 billion credit and debit cards in use in the United States. Estimates of the share of cards with EMV chips stand between 7%[57] and 15%.[58] Some believe that issuers would have to replace, on average, about 2 million cards every day until the deadline to achieve 100% transition.[59] Despite the slow start, some experts have predicted that by the beginning of 2016, 90%-95% of cards could be chip cards.[60]

About 33% of POS machines are now EMV compliant and that figure would have to increase significantly before the benefits of the chip cards can be realized.[61]

(...continued)

[51] "Hack-Resistant Credit Cards Bring More Safety—at a Price," Bloomsberg BusinessWeek Technology, February 24, 2014, http://www.businessweek.com/articles/2014-02-14/hack-resistant-credit-cards-bring-greater-security-at-a-big-price. (Hereinafter "Hack-Resistant Credit Cards Bring More Safety—at a Price," Bloomsberg BusinessWeek Technology.)

[52] "Will Losses in Consumer Confidence in Payments Accelerate EMV?," *n>genuity Journal*.

[53] "From Stripes to Chips," Wallaby Blog.

[54] "Retail IT Gets Ready for Chip-and-PIN Tech," *Forbes*, May 29, 2014, http://www.forbes.com/sites/centurylink/2014/05/29/retail-it-gets-ready-for-chip-and-pin-tech-2/.

[55] A Google search of the term "magnetic stripe card POS reader" returned a wide range of prices. Many of the readers fell within this range. Stripe card readers were also available used on eBay for about $15.

[56] "From Stripes to Chips," Wallaby Blog.

[57] "Will Losses in Consumer Confidence in Payments Accelerate EMV?," *n>genuity Journal*.

[58] "Hack-Resistant Credit Cards Bring More Safety—at a Price," Bloomsberg BusinessWeek Technology.

[59] "Encrypted Chips Help Fight Credit Card Fraud," *USA Today*, January 9, 2014, http://www.usatoday.com/story/news/nation/2014/01/09/encrypted-chips-help-fight-credit-card-fraud/4400347.

[60] "Encrypted Chips Help Fight Credit Card Fraud," *USA Today*, January 9, 2014, http://www.usatoday.com/story/news/nation/2014/01/09/encrypted-chips-help-fight-credit-card-fraud/4400347.

[61] This is an increase from about 10% since the end of 2013. Updated information provided by Mr. Randy Vanderhoof, Executive Director, SmartCard Alliance, September 23, 2014.

Transaction Verification: PIN versus Signature[62]

Most card issuers have made the decision to issue chip-and-signature cards. Over the last year, merchants have expressed disapproval of this decision, asserting that PIN verification is far more likely to reduce fraud. Since the decision is solely up to the card issuers, the remaining dissent may not hinder implementation.

Dual Debit Applications

Visa and MasterCard use one proprietary debit processing application, and the major PIN debit networks[63] use another. After lengthy negotiations, both sides finally agreed to cross-license their applications in July 2013, resolving most of the technical issues hampering transition planning. This issue is no longer a matter of contention.

Debit Transaction Fees: Regulatory Uncertainty

In 2010, as part of a larger financial reform law, the Federal Reserve Board (FRB) was charged with developing rules setting maximum transaction fees ("interchange fees") that merchants can be charged for debit card transactions. In addition, the law specificed the framework the FRB was to use in developing those rules.[64] The rules went into effect in October 2011, but the National Retail Federation, representing merchants, appealed the ruling, stating that it believed the fee ceiling had been set too high.

In July 2013, a judge for the U.S. District Court for the District of Columbia (D.C.) rejected the FRB's regulations, stating that the agency had set the cap too high on debit-card transactions, and that it had disregarded congressional intent in its proceeding. However, in March 2014, the Court of Appeals for the D.C. Circuit reversed the lower court's decision and upheld the FRB's rules. The merchants again appealed the decision, this time to the U.S. Supreme Court, filing for a writ of certiorari in August 2014.[65] On January 20, 2015, the Court denied the merchants' petition, allowing the FRB's original rules to go into effect.

Because of the long-running court case and the other problems described, card issuers lost more than three years of planning time to meet the October 2015 deadline for debit cards (credit cards are unaffected by the fee structure under consideration by the Court). Some issuers were thought to be hesitant to replace their stripe-based debit cards until the issue was resolved. The delay has the potential to cause a lag between when chip-based credit cards are issued and chip-based debit

[62] A third approach is "chip-and-choose." Chip-and-choose cards are capable of both verification methods, allowing the cardholder to enter a PIN if the retailer supports that type of transaction.

[63] For example, Pulse, NYCE, MAC, Tyme, SHAZAM, and STAR.

[64] The regulations also allow merchants to choose the debit network to which they route a transaction, rather than having it imposed on them.

[65] NACS, aka National Association of Convenience Stores, et al., Petitioner vs. Board of Governors of the Federal Reserve System, 2014 U.S. Briefs 200, docketed August 20, 2014, http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/14-200.htm. The petition is available online at http://sblog.s3.amazonaws.com/wp-content/uploads/2014/11/14-200_nacs_v_federal_reserve.pdf. See also "Retailers File Interchange Appeal with Supreme Court," *Credit Union Times*, August 19, 2014, http://www.cutimes.com/2014/08/19/retailers-file-interchange-appeal-with-supreme-cou.

cards are issued.[66] Issuing debit and credit chip cards simultaneously was cited by the FRB as a key to maximizing the benefits of chip cards in reducing fraud:

> 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.[67]

Ultimately, it remains to be seen what impact the court case will have on debit card replacement.

113th Congress: Legislation

No legislation was introduced in the 113th Congress that would have directly affected the manner in which the transition is taking place, but four bills[68] contained language that would have addressed concerns about improving protection from credit card data theft in other ways. These bills would have, for example—

- increased protection for consumers whose card data had been compromised (e.g., free credit monitoring for a year);
- increased penalties for those convicted of identity theft and certain other violations of data privacy and security;
- provided for criminal penalties against entities that fail to provide required notice of a breach of personally identifiable information;
- defined thresholds for when public notification would be required after a breach; and/or
- defined thresholds for when notification of law enforcement or other government entities (e.g., Secret Service, Federal Bureau of Investigation, Congressional Judiciary Committees, Federal Trade Commission) would be required.

[66] "Will Losses in Consumer Confidence in Payments Accelerate EMV?," *n>genuity Journal*.

[67] *Chip-and-PIN: Success and Challenges*, Federal Reserve Bank of Atlanta.

[68] The bills were: (1) S. 1995, Personal Data Protection and Breach Accountability Act of 2014 (Senator Richard Blumenthal), introduced February 4, 2014, and referred to the Senate Committee on the Judiciary the same day; (2) H.R. 3990, Personal Data Privacy and Security Act of 2014 (Representative Carol Shea-Porter), introduced February 4, 2014, and referred to the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, on March 20, 2014; (3) S. 1897, Personal Data Privacy and Security Act of 2014 (Senator Patrick Leahy), introduced January 8, 2014, and referred to the Committee on the Judiciary the same day; and (4) H.R. 1121, Cyber Privacy Fortification Act of 2013 (Representative John Conyers), introduced March 13, 2014, and referred to the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, on April 15, 2014.

A resolution was also introduced that would have expressed "the sense of the Senate that the President should pursue extradition authority for international cybercriminals committing credit card theft targeting United States citizens." No further action was taken.[69]

113th Congress: Hearings

The 113th Congress held three hearings that addressed data breaches, both generally and in response to specific breaches. Each hearing included questions and discussion about the status of EMV adoption in the United States, such as how the transition was expected to affect the frequency and seriousness of data breaches and the progress being made towards a full EMV migration in the United States.

- **Privacy in the Digital Age—Preventing Data Breaches and Combating Cybercrime.**[70] This hearing was held by the Senate Committee on the Judiciary on February 4, 2014. It consisted of two panels of witnesses, the first composed of representatives from the consumer protection, retail, and data security sectors, and the second composed of representatives from federal government agencies charged with investigating the breaches. Of particular interest to Committee Members was the Target Corporation data breach, as well as the Personal Data Privacy and Security Act, which was reintroduced by Senator Leahy, Judiciary Committee Chair, on January 8, 2014. Among other issues, the hearing explored how quickly companies inform their customers after a data breach, and whether current reporting requirements are adequate or whether legislation is needed.
- **Protecting Consumer Information: Can Data Breaches Be Prevented?**[71] This hearing was held on February 5, 2014, by the House Committee on Energy and Commerce and its Subcommittee on Commerce, Manufacturing, and Trade. This hearing was prompted by the Target Corporation data breach. Among other issues, the hearing explored:

[69] S.Res. 563 (Senator Mark Steven Kirk), introduced September 18, 2014, and referred to the Senate Committee on Foreign Relations, https://www.congress.gov/bill/113th-congress/senate-resolution/563.

[70] The hearing page, including witness testimony and the hearing transcript, is online at http://www.judiciary.senate.gov/hearings/hearing.cfm?id=138603a26950ad873303535a6300170f. Panel I witnesses were: Delara Derakhshani, Policy Counsel, Consumers Union; Michael R. Kingston, Senior Vice President and Chief Information Officer, The Neiman Marcus Group; John J. Mulligan, Executive Vice President and Chief Financial Officer, Target Corporation; and Fran Rosch, Senior Vice President, Security Product and Services, Endpoint and Mobility, Symantec Corporation. Panel II witnesses were: The Honorable Edith Ramirez, Chairwoman, Federal Trade Commission; William Noonan, Deputy Special Agent in Charge, Criminal Investigative Division, Cyber Operations, U.S. Secret Service; and Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice.

[71] The hearing page, including witness testimony and the hearing transcript, is online at https://energycommerce.house.gov/hearing/protecting-consumer-information-can-data-breaches-be-prevented. Witnesses were: The Honorable Edith Ramirez, Chairwoman, Federal Trade Commission; The Honorable Lisa Madigan, Attorney General, State of Illinois; William Noonan, Deputy Special Agent in Charge, Criminal Investigations Division, Cyber Operations, U.S. Secret Service; Lawrence Zelvin, Director of the National Cybersecurity and Communications Integration Center, Department of Homeland Security; Michael R. Kingston, Senior Vice President and Chief Information Officer, The Neiman Marcus Group; John J. Mulligan, Executive Vice President and Chief Financial Officer, Target Brands Incorporated; Bob Russo, General Manager, PCI Security Standards Council; and Phillip J. Smith, Senior Vice President, Trustwave Holdings.

- the relationship between federal law enforcement and the private sector in tracking and responding to breaches of consumer information;
- how private sector entities work amongst themselves and with the federal government to develop and maintain best practices;
- how the tactics and efforts of cybercriminals have changed over time;
- whether it is possible or realistic for a company to be impervious to data breaches; and
- whether additional regulation of data security might be necessary.

- **Protecting Consumer Information: Can Data Breaches Be Prevented?**[72] **Can Technology Protect Americans from International Cybercriminals?**[73] This hearing was held on March 6, 2014, by the House Committee on Science, Space, and Technology Subcommittee on Oversight and Subcommittee on Research and Technology. This hearing focused on the consumer privacy and national security aspects of data breaches. Witnesses included federal government officials, payment industry representatives, and a privacy advocacy organization.[74] Members were particularly interested in whether the payments industry was on track to meet the October 1, 2015, deadline. Other issues discussed included the current state of technology and standards to protect consumers from international cybercriminals, and the evolution of cyber-attacks against the U.S. industry from rogue hackers to sophisticated international crime syndicates and foreign governments.

Issues for Consideration in the 114th Congress

Questions and concerns remain that Congress might choose to monitor. Some of these are related directly to the transition itself, while others are related more generally to the larger issue of data breaches.

[72] The hearing page, including witness testimony and the hearing transcript, is online at https://energycommerce.house.gov/hearing/protecting-consumer-information-can-data-breaches-be-prevented. Witnesses were The Honorable Edith Ramirez, Chairwoman, Federal Trade Commission; The Honorable Lisa Madigan, Attorney General, State of Illinois; William Noonan, Deputy Special Agent in Charge, Criminal Investigations Division, Cyber Operations, U.S. Secret Service; Lawrence Zelvin, Director of the National Cybersecurity and Communications Integration Center, Department of Homeland Security; Michael R. Kingston, Senior Vice President and Chief Information Officer, The Neiman Marcus Group; John J. Mulligan, Executive Vice President and Chief Financial Officer, Target Brands Incorporated; Bob Russo, General Manager, PCI Security Standards Council; and Phillip J. Smith, Senior Vice President, Trustwave Holdings.

[73] The hearing page, including witness testimony and the hearing transcript, is online at http://science.house.gov/hearing/subcommittee-oversight-and-subcommittee-research-and-technology-joint-hearing-can-technology.

[74] Witnesses were Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology; Bob Russo, General Manager, Payment Card Industry Security Standards Council, LLC; Randy Vanderhoof, Executive Director, Smart Card Alliance; Justin Brookman, Director, Consumer Privacy, Center for Democracy and Technology; and Steven Chabinsky, Senior Vice President of Legal Affairs, CrowdStrike, Inc., and Former Deputy Assistant Director, Federal Bureau of Investigation—Cyber Division.

Transition Issues

The most complex challenges appear to have been largely resolved through industry negotiation, clearing the path to completing the transition. However, as with many technical upgrades conducted on such a vast scale and involving so many players, challenges emerged during transition planning. These challenges had threatened—and might still threaten—to delay the transition or impact its effectiveness. Given that the October 1, 2015, EMV transition deadline is in place, the congressional role will likely be one of oversight and assessment to ensure that the two remaining issues do not cause a delay.

Impact of EMV Signature Verification on Fraud Reduction

Data on the impact of EMV signature verification on fraud reduction does not exist because signature verification was not adopted in other countries (they chose to adopt PIN verification). So, while the primary driver of the transition is fraud reduction, it remains to be seen if signature verification will produce the same level of fraud reduction in the United States as PIN verification has produced in other countries.

Potential Debit Card Transition Lag

The delay reaching agreement over debit card programming could cause the EMV debit card transition to lag behind the EMV credit card transition. One study found that fraud reduction in POS transactions was achieved more quickly by migrating all card products at or near the same time. The payments industry will need to stay on track to achieve the simultaneous transition, which could have an impact on overall fraud reduction, and the relative level of fraud between credit cards and debit cards.

Data Breach Issues

Given the broad interest in reducing data breaches and fraud, and the approaching October 1, 2015, transition deadline, the 114th Congress might wish to examine the effectiveness of the transition to determine whether legislative action may be needed, especially if major breaches continue to occur. Many questions were raised in hearings during the 113th Congress, including:

Are companies implementing the additional security safeguards recommended to decrease card-not-present fraud? CNP fraud decreased significantly in countries where both card issuers and merchants implemented additional safeguards on such transactions. Card issuers here have implemented various methods to offer those safeguards, but success will be largely dependent on widespread use by merchants.

Are companies taking adequate steps to prepare for a data breach? Data breaches will likely continue, but there are steps that companies can take to prepare for them and mitigate their damage. For example, Experian has published a preparation guide[75] for companies that could make post-breach activity easier and more conducive to assisting law enforcement.

[75] Data Breach Response Guide, Experian, http://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

Are existing post-breach consumer notification procedures adequate and consistent? Consumers might reasonably expect to receive all the information needed, in a timely manner, to protect themselves after a data breach. Additionally, they might expect to receive the same information after every breach, regardless of the company who had been breached or where they are located.

Are existing legal and regulatory post-breach thresholds that trigger mandatory reporting to law enforcement adequate and consistent? Law enforcement is unable to begin investigating breaches until they have been notified that a breach has occurred by the affected company. In addition, nearly all states[76] have their own laws requiring notification; there are no federal laws or guidelines. Of the states that have laws, the circumstances that "trigger" reporting differ.[77] For example, some states define "personal information" narrowly, while others have adopted more expansive definitions. So, in effect, a company might be required to report in some states, but not all, when their data has been breached, as well as report different information in each state. These differing requirements can present a challenge to companies with a presence in more than one state. This is one reason that some in the federal government, including some in Congress and the Federal Trade Commission, have advocated a single federal law to address all aspects of data breach reporting nationwide. Many states with existing, and in many cases long-standing laws, though, have expressed concerns about enacting a federal law. They believe such a law, which would likely supersede state laws, might offer consumers less protection.[78] One compromise that policymakers have discussed would be to allow existing state laws with more stringent protections to take precedence over a federal law.

Author Contact Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov, 7-2508

[76] Forty-seven states have data breach notification laws. Only Alabama, South Dakota, and New Mexico do not.

[77] See "Here's Why the Government Wants a National Data Breach Law," *Washington Post*, February 24, 2014, http://www.washingtonpost.com/blogs/wonkblog/wp/2014/02/24/heres-why-the-government-wants-a-national-data-breach-law/.

[78] "Step aside, States?," Slate.com, January 22, 2015, http://www.slate.com/articles/technology/future_tense/2015/01/obama_data_breach_legislation_federal_laws_shouldn_t_pre_empt_state_laws.html.