Is Our Personal Data Really Safe and Secure: A Review of the Recent Data Attacks.

A Joint Informational Hearing of the Assembly Judiciary and Assembly Banking & Finance Committees

Prepared by staff of Assembly Banking & Finance Committee

2/18/2014

Banking & Finance Data Breach Background

Recent Data Breaches:

The recent retailers affected by the mega data breach are not the first nor will they be the last. The recent data breaches once again made all entities aware that the current payment system has flaws and everyone pays the price, literally. Just to name a few, recently, Target, Neiman Marcus, Michael's all fell victim to hackers. The largest of the three is Target. Between November 27 and December 15, 2013, hackers were able to get access to Target's point of sale system (discussed later), which allowed them to duplicate cards and receive customer's important information. This exposed as many as 40 million U.S. customers to credit-and-debit card fraud. Ultimately, Target reported that an additional 70 million customers had their personal information stolen including names, mailing address, phone numbers, and emails, totaling those affected to 110 million. Target on-line shopping was not affected in the breach and to date, social security numbers were not compromised. The data breach included customer names, credit card numbers, and the card's expiration date. Hackers were even able to retrieve customer's encrypted PIN number from Debit or ATM cards. Both Neiman Marcus and Michael's fell victim to the same type of intrusion but on a smaller scale. These data breaches raise a number of questions such as:

1) As a leader in privacy regulations, what can California do to prevent these from occurring?

2) Would EMV technology prevent data breaches?

3) How can consumers protect their personally identifiable information?

4) Are all entities involved taking the correct steps to ensure the safety and soundness of consumers in the future?

Timeline

Feb. 4: Target CFO John Mulligan testifies to Congress that the company would accelerate its investment in advanced credit card technologies. Mulligan says the company first learned of the breach when notified by the Justice Department. Neiman Marcus and law enforcement representatives also testify.

Feb. 2: White Lodging says it is investigating a breach involving bars and restaurants at 14 hotels it manages, including Marriott (MAR, Fortune 500), Radisson, Renaissance, Sheraton, Westin and Holiday Inn locations. The breach occurred between March 20 and Dec.16, 2013. Independent security researcher Brian Krebs first reports this breach on Jan. 31.

Jan. 30: Target says stolen vendor credentials were used in its massive breach.

Jan. 28: Consumer Bankers' Association, which represents nearly 60 of the nation's largest card-issuing banks, says its members have responded to the Target breach by replacing 15.3 million consumer cards at a cost of $153 million.

Jan. 26: Michaels, the country's largest crafts chain, reports "possible fraudulent activity" on some of its customers' payment cards, suggesting there may have been a breach. CEO Chuck Rubin says the company has not confirmed a breach, but wanted to alert customers.

Jan. 23: Neiman Marcus acknowledged cyber-criminals stole card information for 1.1 million customers who shopped at the retailer between July 16 and Oct. 30, 2013. About 2,400 cards were later used fraudulently, it said.

Jan. 16: Federal investigators warn retailers and other companies that accept card payments about an advanced piece of malicious software that potentially affected a large number of stores. It is widely believed this was the malware that infected Target.

Jan. 14: The nation's largest retail bank, J.P. Morgan Chase (JPM, Fortune 500), says it is replacing 2 million customer cards, prompted by the Target hack.

Jan. 11: Neiman Marcus says a cyber-security firm has found a payment card breach. The company said it is too early to tell how many customers have been impacted.

Jan. 10, 2014: Target says hackers also obtained personal information -- including name, address, phone number and email address -- for up to 70 million customers. It says there may be some overlap with the 40 million impacted by the credit and debit card breach, but it couldn't say how many were counted twice.

Dec. 27: Target says cyber-criminals made off with PIN data, adding that information was "strongly encrypted" and likely remains "safe and secure." It had earlier said PIN numbers were not part of the breach.

Dec. 22: Chase Bank implements strict limits on how much customers can withdraw and spend using debit cards, citing an effort to prevent fraud. Within days, it relaxes those limits.

Dec. 21-22: Target offers customers a 10% discount on many items in its stores.

Dec. 19: Target confirms a breach from Nov. 27 to Dec. 15 involving up to 40 million cards.

Dec. 18: The Secret Service acknowledges it is investigating a reported breach that involved credit and debit cards at Target (TGT, Fortune 500). The news was first reported by Brian Krebs, a security researcher and blogger.

How did it happen?

The latest information provides that the hackers gained access to Target's computer network using the stolen credentials of a refrigeration contractor via "a malware-laced email" sent to the contractor's employees.[1]

---

[1] *Email Attack on Vendor Set Up Breach at Target*, Krebs on Security. February 14, 2014. Available at http://krebsonsecurity.com/

Hackers used a malware program called Citadel to steal passwords from Fazio Mechanical, a suburban Pittsburgh-based company that installed refrigeration systems for Target stores in Ohio and Maryland. Fazio acknowledged that it is part of the investigation into the Target data breach and said its credentials gave its employees access to Target's network "exclusively for electronic billing, contract submission and project management."[2] This access allowed hackers to break into Target's POS systems in order to install malware that enabled the theft of payment card information. Among data security professionals there remains disagreement as to the exact cause of the Target breach, as some believe the breach was the result of multiple attacks over an extended period of time designed to expose weaknesses that could be exploited.[3]

The use of malware in the Target breach appears to be part of the same attacks that affected several other retailers. According to various data security firms and law enforcement sources these attacks demonstrated a high level of sophistication and coordination that had not been witnessed before.[4]

General Data Breach Statistics

Trustwave, a global information security and compliance services and technology company, each year releases a report based on their investigations into data breaches. The following are brief findings from their 2013 report:[5]

- The retail industry was the top target for data breaches in 2012 making up 45% of our investigations. Food & beverage was the second most targeted industry followed by the broader hospitality industry.

---

[2] http://faziomechanical.com/Target-Breach-Statement.pdf
[3] *Disagreement on Target Breach Cause*. Bank Info Security. February 10, 2014. http://www.bankinfosecurity.com/disagreement-on-target-breach-cause-a-6491

[4] *Target Breach May Be Part of Wider Attack*. The Washington Post, January 17, 2014
[5] Executive Summary of Report Available at http://www2.trustwave.com/rs/trustwave/images/Trustwave_GSR_ExecutiveSummary_4page_Final_Digital.pdf

- Cardholder data was the primary data type targeted by attackers.

- Mobile malware increased 400% in 2012. "Malware," which is short for "malicious software" is used to exploit vulnerabilities in computer systems, gather sensitive information, or gain access to private computer systems for a specific purpose—normally cybercrime.

- Out of more than 450 data breaches we investigated, the United States was the top victim location. 73% of victims were located in the U.S.

- In 2012, almost all Point-Of-Sale (POS) breach investigations involved, what's known as, "targeted malware." That's when malware is designed for a specific computer system, business or computer user. SQL (Structured Query Language) injection and remote access made up 73% of the infiltration methods used by criminals. Other commonly used methods were Blackhole exploit kits, malicious PDF files (61% targeted Adobe Reader users) and "memory scraping." Criminals planted malware on users' machines by using all of these infiltration methods.

- It took businesses an average of 210 days to detect a breach. Most victim organizations took more than 90 days to detect the intrusion, while 5% took more than three years to identify criminal activity.

- Only 24% of victim organizations detected the intrusion themselves. Most were informed by law enforcement or another regulatory body.

- Web applications emerged as the most popular attack vector; e-commerce sites being the most targeted asset.

- Users are continuously using weak passwords with "Password1" being the most common password of choice since it meets the bare minimum password requirement typically mandated by policies enforced by IT administrators.

Other Recent Breaches.

Since July 18, 2013, Privacy Rights Clearinghouse has identified over 300 U.S. data breaches in which consumers' personal information was compromised. In addition to the retail breaches previously discussed, several other breaches have been revealed in recent months, including:

- The September 2013 discovery of attacks by an underground criminal identity-theft service, SSNDOB, on major U.S. aggregators of consumer and business data (including LexisNexis, Dun & Bradstreet, and Kroll Background America) as well as on the National White Collar Crime Center;

- The October 2013 discovery of a major hacking attack on computer software company Adobe, in which almost 3 million customers' usernames, encrypted passwords, and encrypted payment information were exposed, with approximately million additional active usernames and encrypted passwords later found to have been compromised as well;

- The October 2013 discovery of the sale of consumers' dates of birth, Social Security numbers, driver's license numbers, and financial information to an underground criminal identity-theft service by Court Ventures, an aggregator of public record information and subsidiary of consumer credit bureau Experian;

- The December 2013 discovery of an attack on JPMorgan Chase that compromised personal information pertaining to prepaid cash cards (Ucards) used for corporate and government payments;

- The December 2013 discovery that 4.6 million Snapchat usernames and phone numbers had been compromised by a group stating its goal was to "raise public awareness on how reckless many internet companies are with user information";

- The January 2014 discovery of two separate breaches involving Yahoo, including one in which malware was served to personal computers via the Yahoo ad network and another in which Yahoo Mail usernames and passwords were found to have been compromised, apparently via a breach on third-party database;

- An apparent breach of guest credit and debit card information held by White Lodging, which owns and manages hotels nationwide under brands including Hilton, Marriott, Sheraton, and Westin.

Existing Payments Ecosystem in the United States:

To properly assess the impact of the latest round of payment system attacks and resulting data breaches it is important to establish some basic information regarding the existing payment structure within the U.S.

The U.S. remains the last developed country reliant on magnetic stripe credit cards (mag stripe), a four-decade old technology. The U.S. is currently on pace to be a full decade behind Europe on the implementation of credit card chip & PIN technology (EMV-Europay, MasterCard, Visa standard). Currently, all face-to-face credit or debit card transactions use a magnetic stripe to read and record account data, and a signature for verification. Under this system, the customer hands their card to the clerk at the point of sale, who "swipes" the card through a magnetic reader. The merchant transmits to the acquiring bank the cardholder's account number and the amount of the transaction. The acquiring bank forwards this information to the card association network requesting authorization for the transaction and the card association forwards the authorization request to the issuing bank. The issuing bank responds with its authorization or denial through the network to the acquiring bank and then to the merchant. Once approved the issuing bank sends the acquiring bank the transaction amount less an interchange fee. This process occurs in a manner of seconds.

This system has proved reasonably effective, but has a number of security flaws, including the ability to get physical access to the card via the mail or via the use of black market card readers that can read and write the magnetic stripe on the cards, allowing cards to be easily cloned and used without the owner's knowledge. The inherit convenience of mag stripe cards is also their inherit weakness.

The data stored on the magnetic stripe is referred to as “Track One” and “Track Two” data. Track One data is personal information associated with the account. Track Two data contains information such as the credit card number and expiration date. In some circumstances, criminals attach a physical device to the POS system to collect card data, which is referred to as “skimming”. In other cases, cyber criminals deliver malware which acquires card data as it passes through a POS system, eventually exfiltrating the desired data back to the criminal. POS systems are connected to computers or devices, and are often enabled to access the Internet and

email services. Malicious links or attachments in emails as well as malicious websites can be accessed and malware may subsequently be downloaded by an end user of a POS system

The terminology and process of a credit card transaction:

Acquirer- A bank that processes and settles a merchant's credit card transactions with the help of a card issuer.

Authorization- The first step in processing a credit card. After a merchant swipes the card, the data is submitted to merchant's bank, called an acquirer, to request authorization for the sale. The acquirer then routes the request to the card-issuing bank, where it is authorized or denied, and the merchant is allowed to process the sale.

Batching- The second step in processing a credit card. At the end of a day, the merchant reviews all the day's sales to ensure they were authorized and signed by the cardholder. It then transmits all the sales at once, called a batch, to the acquirer to receive payment.

Cardholder- The owner of a card that is used to make credit card purchases.

Card network- Visa, MasterCard or other networks that act as an intermediary between an acquirer and an issuer to authorize credit card transactions.

Clearing- The third step in processing a credit card. After the acquirer receives the batch, it sends it through the card network, where each sale is routed to the appropriate issuing bank. The issuing bank then subtracts its interchange fees, which are shared with the card network, and transfers the remaining amount through the network back to the acquirer.

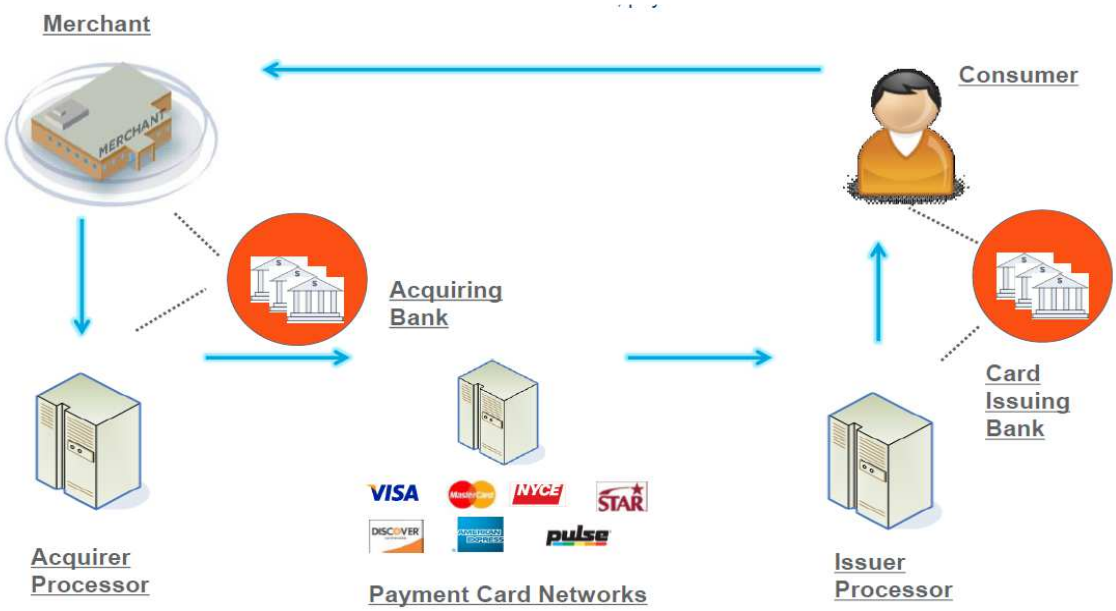
Discount fee- A processing fee paid by merchants to acquirers to cover the cost of processing credit cards.

Funding- The fourth and final step in processing a credit card. After receiving payment from the issuer, minus interchange fees, the acquirer subtracts its discount fee and sends the remainder to the merchant. The merchant is now paid for the transaction, and the cardholder is billed.

Interchange fee- A charge paid by merchants to a credit card issuer and a card network as a fee for accepting credit cards.

Issuer- A financial institution, bank, credit union or company that issues or helps issue cards to cardholders.

Chart: Overview of Typical Credit Card Transaction[6]



The U.S. has over 10 million credit card terminals and 1.2 billion credit cards, with less than 2% of cards having chip technology according the Smart Card Alliance. Annually, credit card fraud equals $11 billion globally, with the U.S. portion amounting to $4.73 billion.[7] The Nilson Report, a credit card industry newsletter, points out that the U.S. accounts for just over a quarter of the global volume of credit card transactions per year, yet accounts for almost 50% of the fraud worldwide.

Mobile Payments:

The Aite group forecasts that U.S. mobile payments will reach $214 billion in gross dollar volume in 2015, a monumental rise from $16 billion in transactions in 2010.

Consumers currently can make three types of payments using a smartphone or tablet computer. The first is a person-to-person transfer initiated by a

[6] Provided by First Data.
[7] Saporito, Bill. "The Little Strip on Your Debit Card is a Massive Achilles's Heel," Time.com. Jan. 23, 2014

mobile device that could include non-commercial payments from one person to another, or commercial payments to a small scale merchant. Second, is for goods or services purchased over the internet on a mobile device. The third option is at point of sale (POS) device initiated from a mobile device at a physical location. These payments can be made using a variety of technologies such as a wallet system that may utilize a smart phone based application to generate barcodes, or a QR Code that allows the user to pay for something from a funding source associated with the mobile wallet. Other options connect a virtual wallet with an email address or username and password. The potential security benefit to a consumer using a mobile payment application is that the consumer's underlying payment data can be shielded from the retailer's payment system. This is one form of the process known as tokenization, which is discussed in detail later in this document.

An April 2013 report from Business Insider, *Why Mobile Payments are Set to Explode*, found the following:

- In-store mobile payments nearly quadrupled last year: eMarketer has estimated in-store mobile payments as adding up to $640 million in transaction volume in the U.S., up from $170 million in 2011. However, this figure does not include swipes on mobile credit card readers like Square and PayPal Here, only consumer-side mobile payments.

- Card readers are building up real scale: Square's mobile payments volume rose to $10 billion in 2012, up from $2 billion in 2011. Starbucks is switching its credit and debit card processing to Square, and as of January 2013 accepts the "Square Wallet" app at 7,000 locations.

- Mobile payments as part of mobile commerce are also exploding**:** PayPal processed some $14 billion in mobile payments last year, evidence of mobile catching on as a transactional platform. PayPal hopes to build a merchant-powered network based on the ubiquity of PayPal as a payment and money transfer platform. PayPal users are already able to pay at thousands of traditional stores by keying in their mobile number and a PayPal PIN selected online (or in their PayPal app).

- Credit card companies are getting in on the action: Credit card companies have responded by making aggressive moves to enter the space. Visa (V.me), and American Express (Serve) have each

introduced digital wallet-like products, MasterCard's PayPass is an NFC-enabled system that is also integrated with the "Google Wallet" app, and Discover has opted to partner with two of the bigger names in the digital payments space ("Google Wallet, and PayPal).

- In the early stages**:** As of year-end 2012, only 7.9 million U.S. consumers (less than 90 percent of the total) had adopted a consumer-facing NFC-compatible system like "Google Wallet," or apps that use QR codes or other methods to generate a payment.

Payment Card Industry Data Security Standard (PCI DSS):

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information.

Defined by the Payment Card Industry Security Standards Council (Council), the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure through 12 requirements. The 12 specific requirements under PCI-DSS are:

Build and Maintain a Secure Network and Systems.

1) Install and maintain a firewall configuration to protect cardholder data.

2) Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3) Protect stored cardholder data

4) Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program.

5) Protect all systems against malware and regularly update anti-virus software or programs.

6) Develop and maintain secure systems and applications.

Implement Strong Access Control Measures.

7) Restrict access to cardholder data by business need to know.

8) Identify and authenticate access to system components.

9) Restrict physical access to cardholder data.

Regularly Monitor and Test Networks.

10) Track and monitor all access to network resources and cardholder data.

11) Regularly test security systems and processes.

Maintain an Information Security Policy.

12) Maintain a policy that addresses information security for all personnel

Although the PCI DSS must be implemented by all entities that process, store or transmit cardholder data, formal validation of PCI DSS compliance is not mandatory for all entities. Currently both Visa and MasterCard require merchants and service Providers to be validated according to the PCI DSS. Smaller merchants and service providers are not required to explicitly validate compliance with each of the controls prescribed by the PCI DSS although these organizations must still implement all controls in order to maintain safe harbor and avoid potential liability in the event of fraud associated with theft of cardholder data. Issuing banks are not required to go through PCI DSS validation although they still have to secure the sensitive data in a PCI DSS compliant manner. Acquiring banks are required to comply with PCI DSS, as well as, to have their compliance validated by means of an audit. A key component of PCI DSS is that organizations do not store sensitive payment cardholder information that is contained in the magnetic strip of the card. If information from the front side of the card is stored in some form, PCI DSS requires that information be protected via encryption.

PCI DSS is an evolving standard and the most recent version (version 3.0) was released November, 2013 and became active January 1, 2014. The new version has been updated to cover topics such as payment terminal security, malware detection, secure software development, use of third party service providers, and ensuring ongoing security rather than point in time compliance.

A report on PCI compliance, *Verizon 2014 PCI Compliance Report*, reported that 56% of U.S. businesses do not meet minimum compliance with overall PCI standards. Delving further into specific areas only 17% complied with security monitoring requirements that require detection and response when data has been breached. Furthermore, 24% were compliance with security testing requirements and 56% met standards for protecting stored sensitive data. Ironically, Europe while leading the way on EMV implementation had only 31% compliance. Limiting access to personal cardholder information is described in the report as one of the "golden rules" of security, but, 71% of the organizations in Verizon's PCI compliance index failed to adequately control access to cardholder data to the level required to be PCI compliant.

EMV: Chip & Pin and Chip & Signature:

Credit card chip technology was established in 1994 by Europay International SA. This chip technology is also called EMV, as it was named after its original developers, Europay, MasterCard® and Visa®.

EMV technology is used today in more than sixty countries outside of the U.S. with worldwide usage at 40% of the total credit cards and 70% of the total terminals based on the EMV standard.[8]

A cardholder's data is more secure on the chip-embedded card than on a mag stripe card. Chip-embedded cards support superior encryption and authentication as opposed to mag stripe card making the data on mag stripe cards easier to obtain via fraudulent means. Chip technology counters the static nature of mag stripe cards by implementing technology that creates dynamic values for each transaction in the form of a different verification code for each transaction. EMV cards can be used both online and in face-to-face transactions, both supporting signature and PIN verification with PIN being the dominant method used in Europe. However, while the EMV cards can complete online transactions, those transactions do not have the same level of security as provided by the chip in the face-to-face transaction. In the online scenario the consumer still enters their card data to complete payment with the addition of a PIN. Currently, several European payment technology companies are working to bring the Chip & PIN protection to online transactions.

---

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

EMV compatible cards come in three forms. A chip embedded card is inserted into the POS terminal and the consumer enters their PIN or uses a signature to complete the transaction. The other way to pay is via contactless cards in which the transaction occurs when the consumer swipes their card within the appropriate distance of the POS terminal that can read the radio frequency identification device (RFID) on the card. The third type of card is a hybrid chip card that allows for both contact and contactless transactions.

As previously mentioned the U.S. is lagging behind in implementation and acceptance of EMV technology. The first U.S. credit card utilizing EMV was issued by United Nations Federal Credit Union (UNFCU) in October of 2010. The primary reason UNFCU issued the card was that many of its members reside outside the U.S. and were in need of a globally accepted card. Outside of the U.S. mag stripe cards are becoming less accepted. Prior to the recent large scale breaches, most large card issuers in the U.S. (Wells Fargo, JPM Chase, and U.S. Bancorp) have begun to migrate some of their portfolios over to EMV cards, but thus far in limited quantities and targeted toward higher income card holders or those that frequently travel to European countries. Subsequent to the recent breaches, several financial institutions replaced cardholder's magstripe cards with EMV cards if they were amongst the millions that had their payment data compromised.

A factor that has contributed to the limited role out of EMV in the U.S. is that currently few merchants accept EMV chip-embedded cards. Most EMV chip cards issued abroad and in the U.S. also contain a mag strip thus allowing acceptance at all U.S. merchants that accept credit cards. Also, up until the recent headline generating data security lapses, most American consumers were unaware of EMV technology or retailers that had EMV capable POS terminals.

On August 9th, 2011 Visa announced an accelerated implementation to EMV technology and established October 1, 2015 as the date when card-present counterfeit fraud liability will shift from issuers to merchant acquirers if fraud occurs in a transaction that could have been prevented with a chip-enabled payment terminal.[9] 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. The announcement specified incentives and deadlines to urge U.S.

[9] Press Release available at http://corporate.visa.com/newsroom/press-releases/press1142.jsp

merchants to accept both contact and contactless chip-enabled cards. One merchant incentive includes the elimination of the requirement for annual card network compliance validation if 75 percent of a merchant's transactions originate from chip-enabled terminals. For the largest merchants, savings from an annual compliance validation would average approximately $225,000 a year. Some industry analysts conclude that only 60% of U.S. point-of-sale terminals will meet the target date.

The history of European adoption of EMV also took a different course and was instigated for varying reasons, many of those different than the current debate in the U.S. American payments model has been very efficient through the verification of transactions from POS over land line phone lines. In Europe, the inefficient telephone system used for verification, created pressure for card networks to create a secure and localized payment transaction system.

The impact of EMV in the United Kingdom was a large reduction in payment card fraud of 40% since 2000, however the U.K. Payments Administration claims that the failure of the U.S. market to adopt EMV has impacted the U.K. market as counterfeit fraud increased because criminals would copy data from stolen U.K. cards and would in turn use the stolen cards in countries with chip and PIN.[10]

Would Existence of EMV Technology Have Prevented the Mega Data Breaches?

Even in Europe where EMV is over a decade ahead of implementation in the U.S. EMV does not protect against all threats. EMV does not exist for card not present transactions such as online transactions or over the phone, and is unable to protect payment data downstream in the payment process once it has left the POS terminal. Statistics for the U.K. and other EMV countries demonstrate that criminals follow the path of least resistance as fraud migrated away from attacking the card present transaction to target transactions such as online banking, online shopping, and mail and phone orders.[11]

EMV is but one step of a multi-layered approach to payment security. Julie Conroy, a senior analysts and fraud expert with Aite Group has stated that

[10] First Data, 7
[11] Ibid, 11

the attacker's malware in the Target breach would have penetrated the payment system regardless of what cards were used by consumers.[12]

EMV would have prevented the ability of fraudsters to make duplicate cards via stealing data at the POS terminal, but it is very unclear whether it would have prevented the Target and Neiman Marcus breaches specifically. However, EMV would make it difficult for criminals to use the information acquired from a breach to make fraudulent cards.

Speed Bumps for EMV Implementation:

According to a First Data report on the implementation of EMV the estimated total costs could be around $8 billion.[13] The costs to financial institutions to issue mag-stripe cards can costs as little as 10 cents each, whereas EMV cards can costs up to $1.30 each.[14] Estimates on the costs vary in terms of production and issuance to the customers, but some estimates find that EMV cards could cost, per card, as much as $10-15 more than existing mag-stripe cards.[15] The Aite Group estimates that the implementation of EMV cards could cut fraud losses in half in the U.S. According to the Nilson Report, U.S. Merchants and banks had 2012 losses of $11.5 billion due to credit card fraud or about 5 cents on every $100 spent and will rise to over $12 billion by 2015. The breakdown of how each entity in the payments chain will absorb the costs is unclear due to ongoing issue relating to the Durbin Amendment, which is discussed later in this document. Thus far, U.S. Financial Institutions have spent nearly $172 million reissuing more than 17.2 million debit and credit cards affected by the Target data breach.[16]

As mentioned previously, some estimates find that only 60% of businesses will meet the 2015 EMV deadline. This means that even during initial phases the marketplace will still have a fair share of mag-stripe cards and EMV capable cards will also still include mag-stripes so that consumers are still able to use their cards at non-EMV compatible merchants. The story of the

---

[12] *Why Target's CEO Changed His Mind About EMV*. American Banker. January 21, 2014
[13] First Data, 13
[14] *The Economics of Credit Card Security*. Washington Post. January 21, 2014.
[15] *Data Breaches Renew Fight Over Credit Card Chip Technology*. USA Today. January 30, 2014.
[16] *Banks spent $172m on Reissuing Credit Cards Affected by Target breach*. Banking Business Review February 2014

Netherlands adoption of EMV is telling as they began their transition to EMV in 2007 with a target completion date of 2010. This allowed magnetic stripe cards to stay in the market longer than most other European countries. During the transition, criminals targeted the remaining magnetic-stripe terminals and in 2011 there were 555 successful skimming attacks on payment terminals, up from 176 in 2010.[17] In a telling example of the potential issues that can occur with a transition to EMV, PayPal President David Marcus reported that on a recent trip to the U.K. his EMV enabled card was compromised.[18]

The European experience demonstrates that fraud shifts to the weakest links in the payment system during a transition to EMV. In what may be a controversial statement on EMV, a report from the Federal Reserve Bank of Kansas City finds:

> *Fraud for card-present transactions on lost or stolen cards may stay the same or even potentially increase. Many countries that use EMV payment cards do not allow cardholder authentication with signatures. Issuers in the United States, however, appear likely to continue to allow signature authorization on EMV debit and credit card transactions (Heun; Punch). As a result, fraud on lost or stolen cards may not decline in the United States. Fraud may even rise as fraudsters, unable to commit fraud on counterfeit cards, begin to target payments with relatively weak security, such as transactions that allow signature authorization. Fraudsters may put more effort into stealing computer-chip payment cards, knowing that they may be able to commit a few fraudulent transactions using a forged signature before issuers cut off use of the card...*
>
> *...The experience of countries that have adopted computer-chip payment cards shows that EMV payment cards offer capabilities for strengthening authentication and preventing fraud. The degree of payoff from adopting the cards only emerges over time, however, because authentication methods tend to evolve and improve during a*

[17] Sullivan, Ricard. The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud.
[18] *PayPal President's Credit Card Hacked for Shopping Spree*. USA Today. February 10, 2014.

transition period. Still, some fraud will migrate to payments with weak authentication capacities, and card issuers will need countermeasures to improve authentication.

Another factor that will take some time is consumer education. Prior to the recent data breaches most U.S. consumers had not heard of EMV technology as these cards were available to a limited number of consumers that met certain guidelines, such as a frequent traveler. The implementation of EMV will require consumers to become comfortable with a new way to make purchases via inserting the card into the terminal and providing a PIN, or tapping the card against the contactless reader. One card network reported that only 5% of the contactless cards on the market today are ever used for contactless payments.[19] The experience of mobile payments implementation may also be telling for the transition to EMV as one of the often cited reasons for the initially slow adoption of mobile payments by consumers is a lack of viewing mobile payments as convenient as traditional payment methods.

Finally, the form of EMV technology may offer additional points of concern and disagreement amongst industry participants. The form of EMV offered will be up to each issuer so that the credit card market in the U.S. will see a mix of Chip & PIN and chip & signature cards. Chip & signature cards offer less protection than those that require a PIN because should someone (other than the cardholder) get physical access to the card the signature is easily forged.

Additional Payments Security:

EMV technology is a vital piece of a larger puzzle in protecting payment information as it does not alleviate the "need for secure passwords, patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees and having clear processes for handling of sensitive payment card data."[20]

---

[19] First Data, 16

[20] Statement of Troy Leach, Chief Technology Officer, Payment Industry Security Standards Council. *Before the Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance United States Senate*. February 3, 2014.

Point-to-point encryption (P2PE) technology helps merchants and acquirers protect payment card data within their systems by encrypting sensitive cardholder information. Because the card data can only be accessed, or unscrambled, with decryption keys held securely by the acquirer, gateway or card network, cardholder information is protected within the payment processing environment.

Point-to-point encryption (P2PE) ensures sensitive credit and debit card data is protected from first card swipe, while in transit, all the way to the payment processor. This technology is also referred to as end to end encryption, or E2EE.

State of the art encrypting devices scan and encrypt cardholder information prior to performing an electronic payment transaction. These sophisticated devices use Triple DES Encryption and DUKPT key management technology to encrypt and transmit cardholder data securely over any network. The encrypted cardholder data being transmitted is NOT equivalent to the original cardholder data in any way. Even if the data were to be intercepted, it would be useless to data thieves.

An additional security measure gaining some media attention is tokenization. Tokenization has advantages for both merchant and service providers. Tokenization is software-based and replaces the cardholder's primary account number (PAN) with a randomly-generated proxy alphanumeric number ("token") that cannot be mathematically reversed and is used for long-term storage or for use as a transaction identifier. From a service provider's perspective, being a software-only technology, it is fairly easy to institute.

For recurring payments from a merchant's standpoint, tokenization is ideal. For these type of payments, the card number is only on the merchant's network "in flight" during the initial transaction which can now be encrypted and protected using P2PE but beyond that, the merchant uses the token that represents the original card for subsequent payments or to track customer transactions for marketing purposes. A myriad of targeted marketing programs can be developed by the merchant using cardholder purchase history data in a tokenized fashion in the merchant's database to, for instance, project what new products may complement those the consumer previously purchased.

One of the major benefits of the tokenization implementation planning process is that it offers the opportunity for merchants to potentially get a head start in compliance with PCI version 3.0, which requires an annual assessment of the locations and flows of cardholder data. Locating all the cardholder data within a merchant's location and identifying who should have access to it could help merchants get ahead of future PCI compliance by re-engineering the logical controls and restrictions to tokenized data.

Tokenization is also a major part of mobile payments security. In the case of mobile payment applications like Square, the consumer's face is the token as because it is shown to the merchant but the actual payment information is secure and never shared.

Dodd-Frank Act: The Durbin Amendment

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) has also created some unintended difficulties ahead for EMV. The Durbin Amendment, entitled "Reasonable Fees and Rules for Payment Card Transaction," added Section 1075 to Dodd-Frank and dealt with the controversial issue of interchange fees. The interchange fee regulation provision is a major point of vitriol between merchants, financial institutions and the card networks. However, a lesser known portion of the Durbin Amendment concerning Debit network competition may have direct impacts on EMV. The Durbin Amendment includes two sets of provisions intended to permit merchants to choose between competing network processing paths for each electronic debit transaction. Issuers and payment card networks are prohibited from (i) restricting the number of payment card networks on which an electronic debit transaction may be processed (network exclusivity restrictions) and (ii) "inhibiting" a merchant (or ATM operator) from directing the routing of an electronic debit transaction through any network that can process that transaction (merchant routing restrictions). The plain meaning of all of this is that debit cards must be able to allow at least two debit networks to process a transaction when the transaction is made. The current EMV standard may not allow for this two network competition and may pose an obstacle for complete integration as debit cards would still rely on mag stripe technology. The Electronic Transactions Association, a global trade group representing companies that offer electronic transaction services has stated that for successful migration to EMV technology the issue regarding dual debit networks needs to be

resolved as the technical features of the current EMV standard do not allow this.[21]

The Durbin Amendment altered interchange transaction fees and rules for debit card transactions. The goal behind Durbin was to transfer wealth from the issuing banks to the merchants with the hope that it would result in lower prices for consumers through lower fees to merchants. The interchange fee is the amount that a merchant has to pay the cardholder's bank (the issuer) through the merchant acquiring bank (acquirer) when a card payment is processed. Currently, only 4 card networks exist: Visa, MasterCard, American Express, and Discover. Visa and MasterCard account for 85% of the U.S. consumer credit card market. In 2011, debit cards were used in 49 billion transactions for a total value of $1.8 trillion, and credit cards were used in 26 billion transactions for a total value of $2.1 trillion**.**

The Federal Reserve Board administered the final rule of the Durbin Amendment which capped the interchange fee at $0.21 cents per transaction to cover the issuers processing costs plus up to an additional 5 basis points of the transaction to cover losses due to fraud and an additional $0.01 for fraud prevention. Additional rules include that the issuers must ensure that each debit card can be processed on at least two unaffiliated networks. Also, the choice of which network a transaction will route to is now decided by the merchant. Merchants can now impose a $10 minimum on credit card transactions (although not in California because state law prohibits merchants from doing this) and are allowed to give discounts to those who pay cash or debit cards.

The final rule only applies to banks with over $10 billion in assets. Banks under the $10 billion threshold are still bound by the merchant routing and network exclusivity rules. In August, 2013, U.S. District Court Judge Richard Leon who sits on the District Court for the District of Columbia overturned the Federal Reserve's ruling of the Durbin Amendment.[22] He

---

[21] Electronic Transactions Association Letter to Congressional Leadership, January 27, 2014. Available at http://www.electran.org/wp-content/uploads/ETA-Card-Security-Hill-Letter.pdf

[22] NACS v. Board, No. 11-02075, Mem. Op. Jul. 31, 2013

concluded the Fed had included costs of debit card issuing in its calculation of the cap which Congress did not intend for in the Durbin Amendment. Judge Leon's decision has been stayed pending a higher court deciding an appeal brought by the Federal Reserve which might not be decide before June, 2014. The appeal will be heard by the U.S. Circuit Court of Appeals for the District of Columbia. The plaintiffs in the case are: the National Retail Federation, NACS (a trade group for convenience stores); the Food Marketing Institute; Miller Oil Co.; Boscov's Department Store LLC; and the National Restaurant Association.

The history of the Durbin Amendment reveals significant disagreements between merchants and the card networks, including financial institutions. Merchants have fought to lower the amount of interchange that they pay and have argued is inherently unfair, while financial institutions argue that interchange revenue is a vital source of anti-fraud revenue. Specifically, community banks and credit unions argue that interchange revenue allows for the quick reissue of customer credit and debit cards when fraud occurs and that the fees cover other fraud losses incurred by financial institutions but that have resulted from problems at the merchant's end of the transaction. While this fight is not always clear in regards to the aftermath of the recent mega data breaches, the way in which entities in the payments market attempt to prevent future events will be influenced heavily by the Durbin amendment debate. The sides of this conflict are best demonstrated through a recent exchange between the National Retail Federal (NRF) and the Independent Community Bankers of America (ICBA). On January 21, 2014 the NRF sent a letter[23] to Congressional leaders that, among other things, stated:

> *For years, banks have continued to issue fraud-prone magnetic stripe cards to U.S. customers, putting sensitive financial information at risk while simultaneously touting the security benefits of next-generation PIN and Chip card technology for customers in Europe and dozens of other markets.*

[23] Letter available at http://www.nrf.com/modules.php?name=Documents&op=showlivedoc&sp_id=7794

On January 22, 2014 ICBA responded with a press release[24] that stated:

> *The NRF should focus its attention on responding to the harm that security breaches at several retailers have done to consumers and their financial institutions rather than hurling false allegations blaming the banking industry for these retail breaches," ICBA President and CEO Camden R. Fine said. "Retailers and their processors—not banks—are responsible for the systems in their stores that process payment cards. ICBA hopes that the massive retail security breaches at Target, Neiman Marcus and others will spur retailers to adopt security solutions going forward." Nearly every retailer security breach in recent memory has revealed some violation of industry security agreements. In some cases, retailers haven't even had technology in place to alert them to the breach intrusion, and third parties, like banks, have had to notify the retailers that their information has been compromised.*

Federal Law Relating to Payment Security

Federal Gramm-Leach Bliley Act

The Gramm-Leach-Bliley Act (GLBA) was enacted in 1999. The law requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. The law does not apply to information collected in business or commercial activities. Whether a financial institution discloses non-public information or not, they must have a policy in place to protect the information from foreseeable threats in security and data integrity. Three main components of the law are the financial privacy rule, the safeguards rule, and the pretext rule.

The financial privacy rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The safeguards rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients'

[24] Press release available at http://www.icba.org/news/newsreleasedetail.cfm?ItemNumber=177385

nonpublic personal information. The privacy notice must be clear, conspicuous, and accurate statement of the company's privacy practices. Customers have to right to opt-out from having their information shared with certain third parties. GLBA does not apply standards of care to merchants or non-financial entities that may hold or transmit consumer payment data and other personal information

The Federal Trade Commission Act: Section 5

Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) prohibits ‘‘unfair or deceptive acts or practices in or affecting commerce.’’ The prohibition applies to all persons engaged in commerce, including banks.

An act or practice is unfair where it:

- Causes or is likely to cause substantial injury to consumers,
- Cannot be reasonably avoided by consumers; and,
- Is not outweighed by countervailing benefits to consumers or to competition.

An act or practice is deceptive where:

- A representation, omission, or practice misleads or is likely to mislead the consumer;
- A consumer’s interpretation of the representation, omission, or practice is considered reasonable under the circumstances; and,
- The misleading representation, omission, or practice is material.

The FTC uses Section 5 as a means to bring action in the world of privacy and data security since the federal government lacks in the area of data security regulation. Although, there is no clear data security regulation, the FTC can bring action under other various regulations such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, including the Disposal rule, the Graham-Leach-Bliley Act, and the Telemarketing and Consumer Fraud and Abuse Act.

In addition, since 2010, the FTC has considered whether to give consumers a "Do Not Track" option that allows them to opt out of websites collecting

information about their online activity, similar to the FTC's Do Not Call Registry, which allows consumers to opt out of most telemarketing calls.

Cardholder Liability Protection

The Truth in Lending Act (TILA) (15 U.S.C. 1601 et seq.) limits consumer liability to $50 if the credit card is lost, stolen, or used without the cardholders authorization, and it prohibits the unsolicited issuance of credit cards.

The Electronic Fund Transfer Act (EFTA) (15 USC 1693 et seq.) specifies that a debit card holder is not liable for any charges, if the loss or theft of the debit card is reported to the customers bank immediately and the card has not been used. If notification to the bank occurs within two business days, the consumer could be liable for up to $50. On day three, liability jumps to $500. After 60 days if the unauthorized use is not reported the customer is 100% liable.

In the case of both credit and debit cards most financial institutions have zero liability policies when card data has been compromised and it is clear that the cardholder is not at fault. However, these are policies and no force of law.

Federal 2014 Legislative Prospects

- Senator Patrick Leahy reintroduced the Personal Data Privacy and Security Act of 2014. This bill was originally introduced in 2005 because "security breaches are a serious threat to consumer confidence, homeland security, national security, e-commerce, and economic stability" and has been reintroduced in each of the last four sessions of Congress. The bill would establish a national standard for data breach notification, and require businesses to safeguard personal information from cyber threats. Under the legislation covered entities are required to provide notice to the Federal Bureau of Investigation or the United States Secret Service of "major" security breaches of "sensitive personally identifiable information."

- Senators Tim Carper and Roy Blunt introduced the Data Security Act, legislation that would require companies that accept credit cards to have information security plans aimed at protecting data and incident response plans to address what steps must be taken in the event a breach occurs. The legislation also contains a notification provision which would require companies to notify affected customers and federal authorities in the

event of a breach and to provide credit monitoring services if over 5,000 customers are affected.

California Law

California enacted a data breach notification law in 2003, the first-in-the nation. (Civil Code sections, 1798.29 and 1798.82.) Since 2003, all but four states have enacted similar security breach notification laws. California's security breach notification statute requires state agencies and businesses to notify residents when the security of their personal information is breached. That notification ensures that residents are aware of the breach and allows them to take appropriate actions to mitigate or prevent potential financial losses due to fraudulent activity, as well as to limit the potential dissemination of personal information.

To be more specific, existing law requires any person or business that conducts business in California, and any state agency, that owns or licenses "computerized data" including personal information to notify any resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a breach of security. The type of personal information that triggers the requirement to notify individuals is unencrypted, computerized information, consisting of an individual's name, plus one of the following: Social Security number; driver's license or California Identification Card number; financial account number, including credit or debit card number (along with any PIN or other access code where required for access to the account); medical information (any information regarding an individual's medical history, condition, or treatment); and health insurance information (policy or subscriber number or other identifier used by a health insurer, information about an individual's application, claims history or appeals), or a user name or email address, in combination with a password or security questions and answer that would permit access to an online account.

Notice must be given to individuals "in the most expedient time possible and without unreasonable delay." Notice to individuals may be delayed if a law enforcement agency determines that notification would impede a criminal investigation or in order to take measures necessary to determine the scope of the breach and restore reasonable integrity to the system. An entity that maintains the data but does not own it must notify the data owner immediately following discovery of a breach.

Privacy as a fundamental right in California

According to section 1, article I of the California Constitution. The Legislature has expressly codified that:

1) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information *and the lack of effective laws and legal remedies*.

2) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

3) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.