12-2014

Cyber Attacked: Could You Be Next?

Sarah DesJardins
University at Albany, State University of New York

Cyber Attacked: Could You Be Next?

Sarah DesJardins

Research Advisor:

Raymond K. Van Ness, Ph.D.

An honors thesis presented to the Department of the School of Business, University at Albany, State University Of New York in partial fulfillment of the requirements for graduation from The Honors College.

Fall 2014

Abstract

In today's modern world, companies store the majority of their business information on computer systems. If not properly protected, private data such as customer financial records, trade secrets, and company financials, can be easily compromised. Major data breaches are becoming more frequent, as hackers are becoming more sophisticated. Cyber-attacks have a negative impact on customers, shareholders, employees, and of course the company itself. This paper examines several recent cyber-attacks and explores the reaction to these by the corporations. It examines the potential and verifiable consequences of these attacks and identifies a range of shareholders who can be injured by the attacks. It examines the adoption of chip and PIN cards as a proposed solution to what appears to be an accelerating and almost unstoppable attempt by criminals to steal personal and financial information.

Introduction

Every day, millions of people use debit and credit cards as a form of payment. Each time a card is swiped or used on-line, the opportunity exists for hackers to breach security barriers and steal personal and financial information. This information is then sold on the black market and used for fraudulent activity, (unauthorized transactions). With recent large data breaches making headlines, companies are facing increasing scrutiny of their anti-fraud policies and practices. As stated in Time Magazine, "Cyber war isn't the future; it's already here (Grossman)."

The number of card-based transactions has steadily increased during the last decade from 43% to 67% of all noncash transactions (Federal Reserve System). In the past three years alone, the number of transactions has increased 7% (Federal Reserve System). At the same time, hackers have become more sophisticated in breaching card security systems. Of the 31.1 million unauthorized transactions from 2012, 92% were made using credit and debit cards (Federal Reserve System). These two elements, the increase in total card-based transactions coupled with more motivated and sophisticated attacks, have put society at greater risk of cyber-attack than ever before. Up until recently, U.S. financial institutions and companies have considered unauthorized transactions "par for the course" and simply a cost of doing business. However, as the number of breaches increases along with the potential for public relations disasters, U.S. business is starting to reconsider this position.

This paper provides an assessment of the impact of data breaches on U.S. business and the risk to shareholders, customers, employees, and the company itself. The first section defines a data breach and uses case studies on Target Corporation and Adobe to consider the initial impact on customers. Part 2 takes an in-depth look at the long-term effects on the shareholders,

customers, employees, and the company itself. Finally, in Part 3, the paper recommends the use of chip-based technology to provide a higher degree of security at the point of transaction to mitigate unauthorized transactions. This recommendation is supported with statistics from the European economy where chip-based card solutions have reduced unauthorized transactions by 58% from 2004 to 2009 (EMV FAQ).

Part 1: Cyber-Attacked

Industry journal *PC Magazine* defines a data breach as "an unauthorized dissemination of information (PC Mag)." This information can include, but is not limited to, names, phone numbers, addresses, email addresses, passwords, and credit and debit card information. Obtaining this information often involves hacking into a system undetected, installing malware to gather the information, and then transferring this information to a server. As hackers become more sophisticated, major data breaches occur more frequently. What does this mean for companies and consumers? When a breach occurs, companies lose time and money and risk their reputation with customers, investors, insurers, and regulators. This can lead to a reduction in the affected company's customer base, resulting in a loss of profits.

"According to various estimates, at least 80 million insider attacks occur in the United States each year (Upton)." A large data breach can have serious consequences for both the company and the individual. The ways in which a company is affected by a data breach can vary depending on a variety of factors. Some of these factors include how the company responds to the crisis and how they handle the customer relations regarding the information breach. A company that manages the crisis well may experience little to no effect on their stock price or sales. However, a company that has poor communication with their customers will lose trust and

loyalty, resulting in a loss of sales and perhaps a drop in stock price. Poor responses to a data breach can also result in the loss of customer trust and loyalty. Just because a company is quickly responding to a breach does not mean that they are responding in a manner that will satisfy the customers. It is also important to explain the breach in a way that customers can understand, while ensuring that the customers do not become alarmed. With more and more businesses storing information on computer systems, it is becoming increasingly important that the information is properly protected. This important concept is demonstrated by the Target data breach of 2013.

Case Study: Target Corporation, December 2013 Data Breach

Target Corporation is the second largest discount retailer in the United States. Founded in 1902, Target Corporation has had many years of successful operations. They pride themselves on "delivering outstanding value, continuous innovation, and exceptional guest experiences (Target)." With over $72 billion in 2013 sales revenues, Target is responsible for storing financial information for millions of customers every year. A company as large as Target should have many security measures in place in order to protect this vast amount of information. However, in December 2013, Target was hacked, resulting in the loss of customer financial information. Although Target did have sufficient security software, it was still being tested and they chose to ignore the warnings that the software had automatically issued about the potential breach. As a result, in December 2013, Target Corporation informed their customers of a major security breach that affected over 110 million customers.

On December 2nd, 2013, hackers began downloading data from Target's point-of-sale terminals. Point-of-sale terminals are used during the checkout process of a sale. They transmit

the financial data from the credit or debit card into the computer system. Once the information is read from the card, the system encrypts the data, or alters it using a code so that it will appear to be unrecognizable to hackers. Unfortunately, the hackers who were collecting data from Target were able to obtain the data right before it became encrypted through a process known as "scraping," which searches for strings of text that include payment data and then sends that data to the hackers' servers (National Public Radio). More specifically, the hackers used a process called "RAM scraping," which stands for Random Access Memory scraping. The RAM is the form of computer data storage that is used by the point-of-sale systems. Thus, the hackers were able to successfully collect and download information that would be sold on the internet through hacker or carder websites. Once purchased, this information could be made into physical cards that could be then sold on the black market (National Public Radio).

The seemingly simple process of gathering data before encryption may lead one to question the security measures that Target had in place at the time. Surely Target could have seen this loophole in their plan. In fact, prior to this breach, Target had invested $1.6 million in software known as FireEye. It was designed to locate unusual or suspicious activity and to alert security personnel of potential issues. This software was capable of discovering the hack and automatically stopping it. However, the security team was still adjusting to the new software and set it up to alert them if a problem was found, but not to do anything without authorization. During the course of the breach, the system sent out multiple warnings, only to be ignored by the security team(Smith). It was not until December 12th, 2013 that Target Corporation realized there was a problem when Federal Law Enforcement officials contacted them to inform them of the major breach that had occurred (Riley). By this point, the hackers had already collected over eleven gigabytes of data from the Target computer systems (Kosner). In less than two weeks,

they had collected information for over 40 million debit and credit cards. With this information, the hackers were able to produce copies of the cards which were then sold on the internet to people all over the world.

Target was most likely alerted of the breach by the FBI. One of the roles of the Federal Bureau of Investigation is "to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud (Cyber Crime)." Their Cyber Division includes the Cyber Action Teams which are "small, highly trained teams of FBI agents, analysts, and computer forensics and malicious code experts who travel around the world on a moment's notice to respond to cyber intrusions (FBI Cyber Action Teams)." In 2006 when Turkish and Moroccan hackers began stealing thousands of credit and debit card numbers from computers around the world, a Cyber Action Team was sent to Turkey and Morocco to discover the hackers and alert Turkish and Moroccan authorities so that the hackers could be arrested (FBI Cyber Action Teams). It is through efforts such as this that alerted Target officials of the data breach.

Case Study: Adobe Systems Inc., October 2013 Data Breach

Adobe Systems Inc. is a multinational computer software company founded in 1982 by Charles Geschke and John Warnock. Originally focused on designing and selling postscript page description language, Adobe has evolved into a company that specializes in developing internet application software, including popular programs such as Photoshop, Acrobat, and Reader. With nearly 12,000 employees, and offices in nearly twenty countries, Adobe generated $4 million in revenues in 2013.

Adobe's heavy focus on technology development may lead one to believe that they would have an affinity for strongly protected systems and software. However, Adobe has a

history of security vulnerabilities. Over the years, various vulnerabilities in their software products have allowed hackers to access files on personal computers through Adobe Reader, publish counterfeit Flash Player updates to download malicious software, enter people's computers through open back doors to steal information, create malicious PDF attachments, and tap into internal servers to gain access to Adobe's security verification system (Pagliery). Each time that vulnerabilities are discovered, Adobe issues various updates to address the issues. Unfortunately, hackers eventually succeeded in breaching Adobe's internal network. On October 3rd, 2013, Adobe announced that there had been a data breach that would affect 3 million people (King). What this meant for employees, customers, and shareholders was unknown at the time, but would slowly be revealed in the weeks and months to follow.

Within one week of the announcement, the number of affected accounts had grown from 3 million to 150 million. Credit and debit card information for roughly 3 million customers was exposed, as well as the user names, passwords, and email addresses for more than 150 million people when hackers entered the network (Krebs on Security). However, this number is not nearly as alarming as it sounds. The database that was hacked was an older database that was a backup system designated to be decommissioned (Ragan). Many of the accounts were inactive. Company spokeswoman Heather Edell said that "the records include some 25 million records containing invalid email addresses, 18 million with invalid passwords (Finkle)." The problem arises when the customers of the active accounts reuse those passwords across multiple websites, including those containing banking information. Adobe stated that the information exposed through the data breach was encrypted. This means that the information had been run through an encryption algorithm that would disguise it in a way that hackers would not be able to view it

directly. If they could figure out the decryption key, they would gain access to all of the accounts in that database. This would be very difficult to do, but also quite possible.

The other option would be to look for patterns in the ciphertext (the encrypted phrases) that would signify important details. For example, if a particular piece of ciphertext is repeated many times, one may conclude that it is a popular password. Since the same algorithm is used to encrypt all passwords, identical phrases would look identical. The next step would be to look up popular passwords discovered as a result of other data breaches and run them through the system until the passwords are revealed. Additionally, the password hints that the customers provided were not encrypted in any way. Password hints such as "the password is password" and "1-8" made it very easy to guess the passwords which, in this example were "password" and "12345678," respectively (Anatomy of a Password). In fact, by using the password hints and various patterns, it was found that 1.9 million of the breached accounts had used "123456" as their password and over 345,000 had used the word "password." Also included in this data was that 211,000 accounts had used the word "adobe123" as the password(Stricture Group). What does all this mean? While it is the company's responsibility to keep their customer information secure, there is also some responsibility on the customer to create unique passwords. In cases such as the adobe breach, having a strong password could deter hackers from attempting to get into specific accounts. Rather, they will hack into those accounts protected with simple, easy-to-crack passwords.

Encrypting passwords is becoming less and less popular as new, more secure techniques become available. For example, hashing and salting passwords is one of the most secure ways to store customer password information. According to the Microsoft Developer Network, "hashing passwords is a way of taking a variable-length password and creating a cryptic, fixed-length

password from it. You do this by generating and using a salt value. A salt value is a random value that you use to generate the hashed password(Microsoft).” Hashing alone does not result in optimal security. Adding salt, a random series of letters and numbers, results in truly unique phrases that are much more difficult to decipher (Adobe Customer Data Breached). While this method will not prevent hackers from obtaining the information, it will most likely prevent them from decrypting it. Unlike encrypted passwords, those that are hashed and salted leave no resemblance to their prior form. Hashing and salting results in completely random phrases of numbers and letters even when applied to identical passwords, thus, instead of discovering the master key that decodes all the passwords at once, hackers would need to separately decode every single password, making it much more difficult and time-consuming.

Responses

The way in which a company responds to a breach can significantly affect their business and reputation. As soon as a data breach occurs, the company must begin the difficult task of deciding when to announce to the public that their personal information has been exposed. If the company announces it too soon, they may not have enough information about the breach to satisfy the outraged customer response. Releasing information that may be inaccurate can cause unnecessary alarm for the customers. On the other hand, waiting to announce it until they have more information may be detrimental to their reputation, as customers may become angered if the breach was unofficially announced, but the company is not responding in a timely manner. This decision is a balance between the amount of information you have available and the amount of time that has passed since the breach was discovered. Perhaps the best way to handle it would be to inform customers of information as it becomes available, with the stipulation that they are still under investigation and suggestions of how customers should move forward.

After Target was informed that their company had been breached, it took almost a week before they informed their customers that their credit and debit card information was stolen. In the case of Adobe, the company knew about the breach on September 17th, 2013, yet did not make the official announcement until October 3rd, 2013, more than two weeks after they had learned of the incident. This gap between the time that both companies knew of the breach and the time that they officially announced it is different for each data breach. It takes time to figure out the best way to approach the announcement. Companies must wait for the investigation to come up with enough information before they release anything. For both Adobe and Target, the breach had already been unofficially announced by security blogger Brian Krebs, thereby forcing each company's hand. Ideally, Target and Adobe should have been the first source to announce their breaches to the public. As stated by Jason Maloni, of Levick Strategic Communications, "anytime you are not controlling the release of information, you lose the opportunity to cast yourself in the role of the hero rather than the villain (Burg)." Although they may have been waiting until they collected further information, customers should have been made aware of the breaches as soon as possible. Instead, customers were left to wonder whether or not the breach actually occurred and how or if they would be affected. This situation is fairly unavoidable due to the fact that the investigation did not yet have enough information to release. It seemed as though both companies handled this to the best of their abilities.

One of the problems that comes with releasing information quickly is that the situation can change as the investigation continues. On December 19th, 2013, Target announced the breach to the public, admitting that nearly 40 million people could have been affected. On January 10th, 2014, they raised this number to 70 million. By January 13th, the number of customers affected reached 110 million (Acohido). Adobe had a similar path, first releasing that only the financial

information of 3 million customers was exposed, later following up with the loss of personal information of 150 million. Although people were annoyed and confused by the fact that Target and Adobe continued to raise the number of people affected with each announcement, this was simply the most accurate information they had available at the time. Customers can be very understanding and they realize that the company does not immediately have all of the answers. When releasing information, it may be helpful to use language such as 'this information is subject to change as the investigation continues', or 'the situation is still evolving,' which can remind customers that there may be updates to this information in the coming weeks or months. Releasing honest and timely information with thorough explanations can ensure that companies retain their customers during a data breach. Also, having a strong plan in place that details the steps to be taken if a breach occurs can help a company to keep their reputation strong.

Part 2: Long-Term Effects

As data breaches are occurring more frequently among large well-known companies, customers are becoming immune to the effects. Although initial customer reactions are still strong, the long-term effects on the company seem to be almost nonexistent. The Target breach supports this observation. Is it because Target and Adobe were very strong financially and well-respected for their products and services prior to the breaches? Perhaps weaker companies would not survive such crises?

Customers

Although the initial announcements by Target were handled well, inadequate communication systems prevented customers from getting their questions answered and their concerns mitigated. Directly following the announcement, the phone lines were completely grid-

locked, making it nearly impossible for concerned customers to gather further information. During a breach, it is extremely important that a company maintains a healthy relationship with their customers. This will ensure that customers will stay loyal to the company and continue to trust and support them. "A security crisis can very quickly turn into a crisis of trust and loyalty if swift communications and responsive customer service aren't employed (Burg)." If customers cannot contact a representative from the company to discuss their concerns, they may become frustrated and refuse to do business with the company in the future. They may also turn to social media to express their frustration which can be detrimental to the reputation of the company. Following the Target breach, customers were angered over the difficulty with communicating with Target directly. Many customers turned to social media networks to express their concern with the company, stating that they would never be shopping at Target again. Other people were more understanding, stating that "I still love Target. It does great work in the community…every retail operation has to fear data hacking…there is no way to keep data 100% secure (Facebook: Target)."

One way that Target tried to encourage business during the data breach was by implementing a ten percent discount on all items in their stores in the days leading up to the holiday season (Jonsson). Both Target and Adobe offered all affected customers free credit monitoring for a year (Malcolm)(Arkin). This is important to maintain the trust and loyalty of customers. It allows customers to feel more comfortable purchasing from the company without having to worry about having their information being compromised. While credit monitoring does not stop hackers from obtaining information, it will ensure that no further damages are done, thus giving customers piece of mind.

When financial information is exposed, customers may be advised to change their debit and credit card numbers to prevent fraudulent charges. This was one of the major inconveniences that resulted from the Target and Adobe breaches. Customers had to take it upon themselves to contact their debit or credit card companies and request that their cards be reissued. Some companies may charge a small fee to cover the cost of replacing the card. Other companies may cover the cost in the short-term, but may sue the breached company for the fees if they had many affected customers. Changing credit and debit card numbers may result in issues with companies for which the customer has enabled automatic payments. If not resolved immediately, this can result in late payment fees and temporary service interruptions in the case of cable or electric companies. Therefore, the customer must spend additional time ensuring that all of the companies they pay are updated with their new card information.

Since the passwords of many Adobe customers were exposed, Adobe required that affected customers change their passwords to ensure optimal security. Adobe also suggested that customers change their passwords to other sites for which they may have used the same or similar passwords. This involves time on behalf of the customers and may even come as an annoyance, despite Adobe's best intentions.

Employees

When a company goes through an experience as destructive and stressful as a data breach, one can expect that there will be effects on employees. This is a topic that is not often highlighted by the media, which tends to focus more on the effects of the customers. However, it is also important to consider the effects on the employees. In the Adobe breach, there was actually another file stolen that contained the information for 64,000 past and present employees

(Horowitz). This file included information such as their names, job titles, and company affiliation, as well as personal information including phone numbers and email addresses (Perlroth). On top of the direct effects such as having their information at risk as well, there are some effects that often are not seen until months later. These can come in the form of lay-offs, reorganizations of the company, and mandatory training sessions that involve security practices and policies. We saw more of these effects in the Target breach.

In the case of Target, Beth M. Jacob, the chief information officer and executive vice president decided to voluntarily step-down from her position as a result of the breach. Target also centralized and unified their security team by creating a "high-level position to focus on web security (Harris)." Breaches are often viewed as the opportunity to reorganize the company and to improve on security policies and practices. A few months following the breach, president and CEO Gregg Steinhafel stepped down from his position, stating that he held himself "personally accountable" for the breach (Alter). This was a major step in the business reorganization. Target also plans to bring in new members to replace some members of those on the board of directors. The breach occurred in part due to a lack of strong and unified leadership. Perhaps the breach was an indication that changes in leadership were necessary for the healthy continuation of the company.

In addition, Target laid off 475 "employees at its headquarters in Minneapolis and worldwide left 700 positions unfilled (Clark). It is important that a company takes into account the effects that a breach can have on their employees. They need to assure employees that their jobs are secure if indeed they are, as breaches can result in worried employees.

Shareholders

The Target breach was considered to be "one of the largest data breaches in retail history (Malcolm)." How does a breach of this magnitude affect the performance of the stock? In researching Targets' stock price in the time surrounding the breach, it appears as if it was relatively unaffected by the release of information. In fact, on December 19th, 2013, the day that Target announced the breach, the stock price closed at $62.15. The following day, the adjusted close was $61.56. In the few weeks prior to the breach, the stock price was between $61.70 and $62.44. After the data breach was discovered and announced to the public, the stock price stayed at this level until the middle of January 2014, where it began to drop off to as low as $54.25. By the end of February 2014, the stock price returned to the pre-breach average of $62. Based on these observations, I do not believe that the data breach affected the stock price negatively. The lower stock price could be explained by other events such as the struggling Canadian expansion that was occurring in the same time frame. Even if the lower prices observed from January through February were related to the data breach, the effects were minimal (Yahoo Finance).

It appears that the same holds true for the Adobe breach. On October 3rd, 2013 when Adobe announced the breach, the shares closed at $50.88. The following day, the stock price closed at $51.57. The stock price actually increased by $0.69 following the data breach. In the weeks surrounding the data breach, the stock price ranged from roughly $49 to $52. Based on these results, I do not think that the breach affected Adobe stock prices negatively. They may have even had a positive effect on them. This effect seems to be occurring more and more frequently when a company is breached. Is it possible that shareholders simply don't care that their company is breached? Do they not realize the implications that this could have on sales revenues or reputations? Perhaps they recognize that data breaches are going to happen and the

fact that a company is hacked does not necessarily reflect on their ability to perform well financially. While it may hurt the company in the short-term, the effects do not seem to carry too far into the future. “It's simply not a big issue with consumers,” said Craig Johnson, president of retail consultancy Customer Growth Partners, noting that shoppers seem to be almost immune to the breaches now. “Everybody knows that this is not people's first rodeo (The Associated Press).”

Company

As Jim Jaeger states, “Companies typically underestimate the confusion of the first few days or first week or two of a breach (Prince).” Data breaches may lead to a decrease in profits, expensive lawsuits with credit card companies and banks, a loss of reputation, and increased expenses related to the investigation. They may also suffer from a loss of loyal customers that made up the majority of their purchases.

Although it does not appear that the stock price was affected, Targets’ sales were affected, especially since this breach occurred during the holiday season which is typically a busy time for retail stores. As Target reported in their 2013 annual report, “Prior to our December 19, 2013 announcement of the Data Breach, our U.S. Segment fourth quarter comparable sales were positive, followed by meaningfully negative comparable sales results following the announcement. Comparable sales began to recover in January 2014 (Target Corporation).” They also referenced the loss of reputation in the 2013 annual report when they said, “We know our guests' confidence in Target and the broader U.S. payment system has been shaken. We are committed to, and actively engaged in, activities to restore their confidence (Target Corporation).” Target said that its fourth-quarter profit was down 46 percent from the

same period the year before, partly because of a steep drop in sales and traffic after the breach became public (Harris). The company also spent $61 million on expenses related to the breach during the fourth quarter, and said it expected to receive $44 million in insurance payments (Harris). As for Adobe, they still achieved their fourth quarter revenue of $1.04 billion (Adobe).

Retaining customers during a data breach can prove to be very important, especially for a company like Target which has multiple competitors. Customers may find it simpler to switch to Wal-Mart, for example, which carries very similar products for similar prices, than to deal with the worries of having their information stolen again. This is where is pays to have a strong company that has unique aspects that it focuses on such as customer service, low prices, or quality products.

When a company is breached, it is important that they consider the long-term effects on their shareholders, customers, and employees. Any efforts to mitigate these effects will help to lessen the impact of the breach on the company. Communication between the company and customers is extremely important to maintain a strong relationship with their customers. Properly handling a breach can result in minimal effects on stock-price both initially, and in the future.

Part 3: Chip and PIN cards

Based on the information preceding this section, it is clear that data breaches are becoming a major problem in the United States. When Target was breached, the financial information for over forty million people was exposed. As a result of the Adobe breach, three million people lost their financial information. Both companies and customers can better protect their information through stronger, more unique passwords, and better, more advanced systems. A major way to lessen the exposure of financial information is by adopting chip and PIN credit

and debit cards, or EMV cards. EMV stands for Europay, Mastercard, and Visa. These are the three organizations that established the original EMV specifications in 1994 (About EMV). The adoption of chip and PIN cards involves the cooperation of banks, customers, and retailers. Currently, over 130 countries, including Canada, Mexico, the United Kingdom, France, and China, have already adopted chip and PIN cards and have seen drastic decreases in the amount of fraudulent credit and debit card transactions since doing so. Perhaps this is due to the fact that chip and PIN cards are much harder to duplicate. Also, the transaction must be authorized by the user with a four-digit PIN, as opposed to the simple signature required by traditional magnetic stripe cards. The adoption of the chip and PIN cards will result in less data breaches because the information contained on the cards is less valuable since it does not contain the PIN needed to make a transaction.

Magnetic stripe cards contain the card holder's name, the account number of the card, the expiration date, and the security code. When the card is swiped through a card reader, the information is read by the magnetic read head. This is similar to the way that cassette tapes work (HowStuffWorks). Chip and PIN cards, or EMV smart cards, are different from the magnetic stripe cards in that they are embedded with a small computer chip that contains the financial information that would be traditionally found in the stripe. These cards "contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards (EMV FAQ)." Protected with cryptography, the computer chip provides much more security to the information. This makes it harder to obtain since the code is needed in order to access the information. When an EMV card is inserted into the card terminal, "the contact plate allows the chip to connect to a reader. This connection enables the chip to get power from and exchange data with the terminal (About

EMV).” The information stored on a chip and PIN card is the same as that stored on a magnetic stripe card, although the computer chip better protects the information.

Aside from inserting the card into a terminal, entering the PIN number, and then removing the card, there is another way to engage in a transaction. Contactless payments are becoming more and more popular with the recent introduction of Apple Pay. A contactless payment involves holding the card within two to four inches of the terminal while the “payment account information is communicated wirelessly (Contactless Payments).” With each transaction, a unique code is created that ensures that the transaction is secure. If a hacker were to get ahold of the information, they would have to use the same code that had already been used in a prior transaction. The system would not allow this transaction to go through with a code that had already been used, thus the information would be useless to hackers. Apple Pay is essentially the same thing as using a physical card, but the information would be stored in the users phone rather than on their card. With Apple Pay, a user can choose from multiple credit and debit cards that are all located on a single device (Apple Inc.).

One of the major reasons that chip and PIN cards are more secure is the fact that they require the user to enter the four-digit PIN for every transaction. With a magnetic stripe card, only a signature was required that could easily be forged. The user relies on the store clerks to match the signature on the back of the card with the signature provided at the time of transaction. It is impractical to expect the store clerk to determine whether or not the signature is fraudulent. The PIN erases the need for the store clerk to judge signatures and instead places the liability on the card owner. Since the PIN is not actually stored on the card, if an unauthorized transaction occurs, it is most likely due to the fact that the owner did not properly protect their PIN. This is

an efficient way to protect users from fraudulent transactions due to lost or stolen cards. Furthermore, the chips are encrypted and therefore difficult to replicate.

Many countries have already adopted chip and PIN technology including the United Kingdom and France. Both of these countries have seen dramatic decreases in fraudulent activity relating to point-of-sale systems. "In the U.K., for example, payment card fraud losses reached a 10-year low in 2011, and experts credit this achievement largely to the use of "Chip and PIN," a form of EMV-enabled card authentication (First Data Corporation)." In 2004, the year of implementation, the fraud rate was 0.14% per transaction for point-of-sale transactions. By 2010, this number decreased to 0.07% (BITS). "Fraud on lost and stolen cards is now at its lowest level for two decades and counterfeit card fraud losses have also fallen and are at their lowest level since 1999. Losses at U.K. retailers have fallen by 67 per cent since 2004; lost and stolen card fraud fell by 58 per cent between 2004 and 2009; and mail non-receipt fraud has fallen by 91 per cent since 2004 (Contactless Payments)." Clearly, chip and PIN cards have been able to dramatically reduce fraudulent activity across the United Kingdom.

In France, chip-embedded cards were first implemented in 1986 (BITS). The fraud rate in 1987 was 0.27% per transaction (BITS). By 1995, this number was reduced to just 0.03% (BITS). This dramatic reduction took place before official EMV cards were introduced. Once these were introduced, the fraud rate briefly rose, before continuing the decreasing trend. However, France is noticing a significant increase in the fraud rates related to card-not-present (CNP) transactions. They currently represent 54% of all card fraud, up from 25% in 2006 (BITS). Similarly, the United Kingdom is noticing that many more fraudulent transactions are occurring in CNP transactions, especially those transactions made on-line (BITS).

Major companies including American Express, Discover, MasterCard, and Visa are currently planning the adoption of EMV technology for their customers (Contactless Payments). Effective October 1st, 2015, there will be a liability shift between the retailers and MasterCard that will result in the retailers being responsible for any data breach costs that would have previously been paid by the banks if the retailers do not switch over their point-of-sale operating systems to accept chip and PIN payment cards. This will encourage companies to adopt this technology, resulting in further security for customers, banks, and retailers. Furthermore, if a customer is found liable for a transaction in which the PIN could only have been available to hackers due to their carelessness, they may be found responsible for paying the fines and covering the costs of the fraudulent transaction (Miller). The liability shift relating to Visa will be effective October 1st, 2015 as well.

Implementing EMV cards in the US proves to be very costly. As stated by Total Systems Services, "replacing cards is pegged at nearly $3 billion, and replacing payment terminals will cost merchants more than $2.5 billion collectively (Total System Services)." Retailers are comparing the costs of a data breach with the costs of implementing the EMV system. Although some companies would rather risk a data breach than front the costs of adopting EMV technology, the upcoming liability shifts effectively force major retailers to purchase EMV enabled point-of-sale systems, or risk covering the full costs of a breach. Had the Target and Adobe breaches occurred after the adoption of EMV cards was complete, it would be highly unlikely that they would have experienced such large numbers of lost financial records. The hackers would not have found this information to be very useful due to the computer chips that are difficult to replicate, the fact that the PIN is not actually stored with the information, and the fact that the CVC is unique to each transaction. The combination of these three things may have

actually prevented the breach from occurring, as the hackers may not have been as motivated. With the upcoming adoption of EMV technology, retailers should see a significant drop in the amount of fraudulent transactions that occur in-store.

It is clear that EMV adoption has dramatic results in reducing fraud rates in other countries. Despite the high implementation costs for banks and retailers, customers should receive the benefits of stronger security, while banks and retailers should see lower costs due to data breaches in the future. The magnetic stripe technology was very vulnerable to attackers, as they simply swiped the card and forged a signature. Adding the required PIN to the transaction will prevent people from stealing cards and using them right away. They would need to invest a lot of time and energy into a single card in order to potentially gain access to the funds. Not only should the adoption of EMV technology reduce the number of records breached during a data breach, but perhaps less data breaches will occur overall. The U.S. will need to monitor CNP transactions in the future, as it has been demonstrated in other countries that the fraudulent transactions switch from point-of-sale systems to on-line transactions with the implementation of EMV. "Such technology wouldn't prevent a breach, but it would make the card data essentially useless for thieves, who typically take the information and produce counterfeit cards (Sidel)."Overall, the implementation should decrease the fraudulent transactions in the U.S.

Conclusion

As data breaches are occurring more and more frequently, it is important that companies are properly protecting their information. Although it is nearly impossible to prevent all data breaches, the implementation of chip and PIN cards in the United States can help to reduce the number of data breaches, as well as the amount of financial information stolen when a data

breach does occur. This has been demonstrated in many countries that have already adopted chip and PIN cards. Although this implementation is expected to reduce the risk of exposed financial information, it is important that the customer does their part as well to insure that their information is protected.

REFERENCES

Acohido, Byron. "Timeline: Target, Neiman Marcus disclosures." *USA Today.* 6 Feb. 2014. Web. 4 Apr. 2014. <http://www.usatoday.com/story/cybertruth/2014/01/23/timeline-target-neiman-marcus-disclosures/4799153/>.

Adobe. "Adobe's Cloud Innovations Drive Strong Q4 and FY2013 Financial Results." *Adobe.* 12 Dec. 2013. Web. 14 Jun. 2014. <http://www.adobe.com/aboutadobe/pressroom/pressreleases/pdfs/201312/Q413Earnings.pdf>.

Alter, Charlotte. "Target CEO Resigns Amid Fallout From Data Breach." *TIME.* 5 May 2014. Web. 14 May. 2014. <http://time.com/87638/target-gregg-steinhafel/>.

Apple Inc. "ApplePay." Web. 14 Sep. 2014. <http://www.apple.com/apple-pay/?cid=wwa-us-kwg-features-com>.

Arkin, Brad. "Important Customer Security Announcement." *Adobe.* 3 Oct. 2013. Web. 10 Jun. 2014. <http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html>.

BITS Financial Services. "Factors Influencing EMV Adoption in the United States." *The Inovator.* Mar. 2014. Web. 22 Sep. 2014. <http://www.bits.org/publications/Innovator/InnovatorMarch2012EMV.pdf>.

Burg, Natalie. "Five Lessons For Every Business From Target's Data Breach." *Forbes.* 17 Jan. 2014. Web. 20 Jun. 2014. <http://www.forbes.com/sites/sungardas/2014/01/17/five-lessons-for-every-business-from-targets-data-breach/>.

Clark, Megan. "Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer." *International Business Times.* 5 May 2014. Web. 17 Aug. 2014. <http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056>.

Ducklin, Paul. "Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder." *Nakedsecurity.* 4 Nov. 2013. Web. 2 Sep. 2014. <http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/>.

Ducklin, Paul. "Adobe Customer Data Breached - login and credit card data probably stolen, all passwords reset." *Nakedsecurity.*4 Oct. 2013. Web. 15 Jul. 2014. <http://nakedsecurity.sophos.com/2013/10/04/adobe-owns-up-to-getting-pwned-login-and-credit-card-data-probably-stolen-all-passwords-reset/>.

Facebook. "Target." *Facebook.* 19 Dec. 2013. Web. 11 Apr. 2014. <https://www.facebook.com/target>.

Federal Bureau of Investigation. “Cyber Crime.” *FBI.* Web. 12 Sep. 2014. <http://www.fbi.gov/about-us/investigate/cyber>.

Federal Bureau of Investigation. “FBI Cyber Action Teams.” *FBI.* 6 Mar. 2014. Web. 14 May. 2014. <http://www.fbi.gov/news/stories/2006/march/cats030606>.

Federal Reserve System “Summary of Findings.” The 2013 Federal Reserve Payments Study (2013): 6, 8, 12.

Finkle, Jim. “Trove of Adobe user data found on Web after breach: security firm.” *Reuters.* 7 Nov. 2013. Web. 1 Jul. 2014. <http://www.reuters.com/article/2013/11/07/us-adobe-cyberattack-idUSBRE9A61D220131107>.

First Data Corporation. “EMV and Encryption + Tokenization: A Layered Approach Security.” *First Data Corporation.* Web. 16 Aug. 2014. < http://www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF>.

Grossman, Lee. “The Code War.” *Time: World War Zero.* 21 Jul. 2014. Print.

Harris, Elizabeth A. “Target Executive Resigns After Breach.” *New York Times.* 5 Mar. 2014. Web. 6 Jun. 2014. <http://www.nytimes.com/2014/03/06/business/a-top-target-executive-resigns.html?_r=0>.

Horowitz, Brian T. “Adobe Breach Hits 38 Million Customers.” *Cruxial CIO*. 30 Oct. 2013. Web. 8 Jul. 2014. <http://www.cruxialcio.com/adobe-data-breach-hits-38-million-customers-2502>.

HowStuffWorks. "How does a magnetic stripe on the back of a credit card work?" *HowStuffWorks.com.* 14 April 2008. Web. 9 Aug. 2014. <http://money.howstuffworks.com/personal-finance/debt-management/magnetic-stripe-credit-card.htm>.

Jonsson, Patrik. “Target Corp. feels customers' fury over response to card-data breach.” *The Christian Science Monitor*. 21 Dec. 2013. Web. 17 May. 2014. <http://www.csmonitor.com/USA/2013/1221/Target-Corp.-feels-customers-fury-over-response-to-card-data-breach-video>.

King, Rachel. “Adobe Hacked, 3 Million Accounts Compromised.” *CNET*. 3 Oct. 2013. Web. 13 Jun. 2014. <http://www.cnet.com/news/adobe-hacked-3-million-accounts-compromised/>.

Kosner, Anthony Wing. “Researchers Report Exact Timeline Of Massive Target Data Breach.” *Forbes.*17 Jan. 2014. Web. 1 Jun. 2014. <http://www.forbes.com/sites/anthonykosner/2014/01/17/researchers-report-exact-timeline-of-massive-target-data-breach/>.

Krebs on Security. “Adobe Breach Impacted At Least 38 Million Users.” *KrebsonSecurity.* 29 Oct. 2013. Web. 21 Jun. 2014. <http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/>.

Malcolm, Hadley. “Target Sees Drop In Customer Visits After Breach.” *USA Today.* 11 Mar. 2014. Web. 16 Apr. 2014. <http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/>.

Microsoft. “How to Hash Passwords.” Web. 11 Jun. 2014. <http://msdn.microsoft.com/en-us/library/aa545602(v=cs.70).aspx>.

Miller, Phillip; Berg, Guy; Stroud, Jeff; Paese, Steven. “EMV Fror U.S. Acquirers: Seven Guiding Principles for EMV Readiness.” *Master Card Advisors.* Jul. 2012. Web. 13 Sept. 2014. <http://www.mastercardadvisors.com/_assets/pdf/emv_us_aquirers.pdf>.

National Public Radio. “How The Hackers Did It: A Discussion About Target’s Data Breach.” *NPR.* 13 Jan. 2014. Web. 10 Aug. 2014. <http://www.npr.org/2014/01/13/262185937/how-the-hackers-did-it-a-dicussion-about-targets-data-breach>.

Pagliery, Jose. “Adobe has an epically abysmal security record.” *CNN Money.* 8 Oct. 2013. Web. 16 Jul. 2014. <http://money.cnn.com/2013/10/08/technology/security/adobe-security/>.

PC Mag. “Encyclopedia.” *PCMag*. Web. 14 Aug. 2014. <http://www.pcmag.com/encyclopedia/term/61571/data-breach>.

Perlroth, Nicole. “Hacker Claims to Have Breached Adobe.” *New York Times.* 14 Nov. 2012. Web. 14 Jul. 2014. <http://bits.blogs.nytimes.com/2012/11/14/hacker-claims-to-have-breached-adobe/>.

Prince, Brian. “Cybersecurity: Confronting the Threat of Shadow IT.” *Forbes.* 20 Oct. 2014. Print.

Ragan, Steve. “Adobe confirms stolen passwords were encrypted, not hashed.” *CSO Online.* 4 Nov. 2013. Web. 14 Jul. 2014. <http://www.csoonline.com/article/2134124/network-security/adobe-confirms-stolen-passwords-were-encrypted-not-hashed.html>.

Riley, Michael; Elgin, Ben; Lawrence, Dune; Matlack, Carol. “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It.” *Bloomberg Businessweek Technology.* 13 Mar. 2014. Web. 10 Aug. 2014. <http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p3>.

Sidel, Robin; Yadron, Danny; Gasparro, Annie. “Data Breach Puts Focus on Beefed-Up Card

Security." *The Wall Street Journal.* 15 Aug. 2014. Web. 20 Oct. 2014. <http://online.wsj.com/articles/data-breach-puts-focus-on-beefed-up-card-security-1408144918>.

Smart Card Alliance. "EMV FAQ." EMV Connection. *The Smart Card Alliance.* Web. 19 Sept. 2014. <http://www.emv-connection.com/emv-faq/#q12>.

Smart Card Alliance. "Contactless payments: Frequently Asked Questions." *EMVCo.* Web. 4 Sep. 2014. <http://www.smartcardalliance.org/publications-contactless-payments-faq/>.

Smart Card Alliance. "About EMV." *EMVCo.* Web. 4 Sep. 2014. <http://www.emvco.com/about_emv.aspx>.

Smith, Chris. "It turns out Target could have easily prevented its massive security breach." *BGR.* 13 Mar. 2014. Web. 10 Aug. 2014. <http://bgr.com/2014/03/13/target-data-hack-how-it-happened >.

Sticture Group. "Top 100 Adobe Passwords With Count." Web. 5 Aug. 2014. <http://stricture-group.com/files/adobe-top100.txt>.

Target. "Mission & Values" *Target*. Web. 10 Jul. 2014. <https://corporate.target.com/about/mission-values>.

Target Corporation. "2013 Annual Report." *Target.* Web. 14 Aug. 2014. <https://corporate.target.com/annual-reports/pdf-viewer-2013?cover=6725&parts=6724-6726-6727-6730-6728>.

The Associated Press. "Home Depot's breach damage likely mitigated." *Trib Total Media.* 12 Sep. 2014. Web. 28 Sep. 2014. <http://triblive.com/business/headlines/6779292-74/depot-breach-target#axzz3D78mzOpk.>

Total System Services, Inc. "U.S. EMV Adoption: Lessons Learned From Canadian-Based Value Added Resource (VAR)." *Total System Services, Inc.* Web. 23 Sep. 2014. <http://www.tsys.com/acquiring/engage/white-papers/United-States-EMV-Adoption.cfm>.

Upton, David M; Creese, Sadie. "The Danger From Within: The biggest threat to your cybersecurity may be an employee or a vendor." *Harvard Business Review.* Sep. 2014. Print.

Yahoo Finance. "Target Corp. Historical Prices." *Yahoo Finance.* Web. 23 Jul. 2014. <http://finance.yahoo.com/q/hp?s=TGT&a=11&b=19&c=2013&d=03&e=28&f=2014&g=d&z=66&y=66>.