PAYMENTS SECURITY AND THE 2013 HOLIDAY SEASON BREACHES:
Analysis and Recommendations

Sponsored By: RS Software, Inc.

How Did It All Start?

On December 19, 2013, the second largest discount retailer in the United States, Target Corporation, confirmed in a news release that unauthorized access to payment card data may have impacted certain guests making credit and debit card purchases in its stores. Initially, Target estimated that approximately 40 million customers might have been impacted between November 27 and December 15 of 2013. That number was later revised upward to include more than 110 million consumers.

As the payments industry was absorbing the news from Target, on January 11, 2014, luxury merchant Neiman Marcus announced on January 11, 2014 that it had been notified in mid-December 2013 that some of its customers' credit and debit cards were possibly used by thieves to make unauthorized purchases in one or more of its 40 upscale stores and clearance operations.

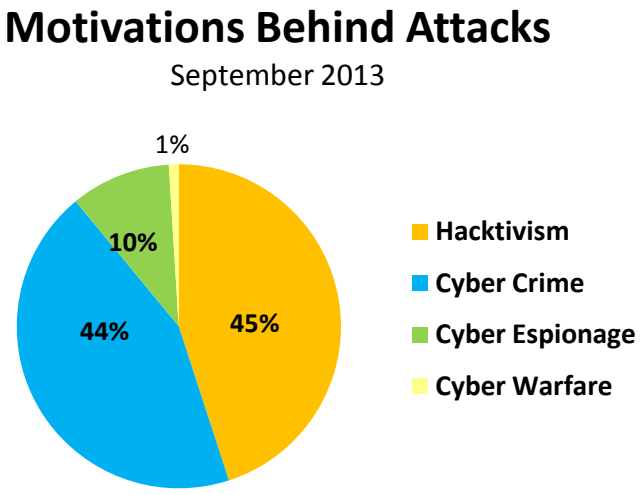
Neiman Marcus didn't say whether the breach was in any way related to the massive data theft at Target, but security experts believe both breaches could be part of the same scam. Whatever the case, the recent security breaches at two major retailers over a holiday shopping season has raised a question about the security of the entire card payments ecosystem and the practices of the companies that participate in it.

The following provides more details on the breaches, an analysis of the reactions by key participants in the industry and a description of the changes the industry faces if it is to win back the confidence of the consumer who uses credit and debit cards.

So What Really Happened?

Before we analyze the impact of the 2013 holiday season breaches, it is useful to look at a few basic facts about what happened.

- **What data was breached?** Initially the indications were that two kinds of information about the cardholder had been compromised. Specifically, card data stored on the magnetic strip on the back of the credit and debit cards had been stolen by the thieves. In addition, in some cases the four-digit personal identification numbers (PINs) of the debit cards were taken. At Target, in addition to PINs, criminals captured personal information – names, physical addresses, email addresses and telephone numbers from approximately 70 million cards.

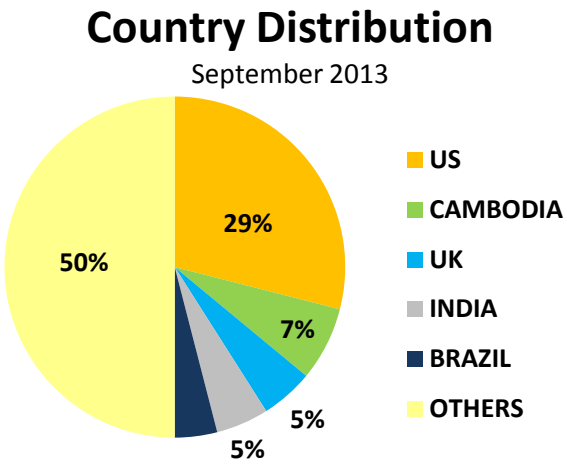


Source: hackmageddon.com September 2013 Cyber Attacks Statistics

- **How did the breach happen?** Forensics on the breaches indicate that the card information was most likely acquired using "malware in the access point." In other words, the point-of-sale (POS) terminals at checkout counters into which customers swipe their cards had been infected with a piece of software designed to capture the customer and card information, then reroute it to the thieves. While spokespersons for the infected organizations insisted that the PINs that were stolen were encrypted and, therefore, relatively useless to the criminals, a Reuters report suggested otherwise. Reuters disclosed that the use of "RAM scraping," a technique that captures data while it is in a computer's working memory before it is encrypted for storage or transmission, could have been used. Some experts initially speculated that the Target breaches were the result of an inside job, but when Neiman Marcus added its name to the list of those operations affected by similar attacks, the consensus became that the attackers had found a common vulnerability in the retailers' systems through which they were able to insert malware.

- **What are the retailers and banks doing to address these breaches?** The retailers targeted by the thieves have identified and are attempting to contact via email and other means the customers affected. Target is offering its affected customers a free credit monitoring service and identity theft protection. The financial institutions that issued the credit and debit cards caught in the breach are independently notifying their customers but their strategies for addressing the breach with their cardholders vary. For example, some banks have elected not to re-issue cards that may have been compromised and instead have notified customers that they should monitor their accounts and report any fraudulent activity. The consumer will not be responsible for reported fraud but will be for any fraud that is not reported within a specified timeframe. Other banks have reissued new cards to their customers and cancelled the cards impacted to minimize the inconvenience to their cardholders.

- **How common is this type of breach?** The Identity Theft Resource Center tracks data-breach incidents and the number of exposed records related to payment cards, customer, university or patient data when known. From 2005 through 2013, the Center tallied 4253 breaches of more than a half a billion records. Many of these breaches involved payment cards and cardholder data; e.g., the March 2007 TJX and January 2009 Heartland Payment Systems breaches. The presence of large credit and debit card databases held by a variety of organizations – such as Apple's database of more than a half billion credit and debit cards – continues to represent a lucrative and tempting opportunity for highly organized, international criminal enterprises.



Source: *hackmageddon.com September 2013 Cyber Attacks Statistics*

THE CHAOS THAT ENSUED

In the past, confessing to a cyber attack, while costly in terms of monetary losses and negative public relations, has seldom led to longer term damage to relations with the general public, the payments industry, investors or other stakeholders. Shares generally would shrug slightly and sales remain mostly steady even when confidential customer data or vital intellectual property was lost, as confused consumers and investors either did not know how to react or believed the lasting effects to be limited. The attacks during the 2013 holiday season were different.

- **Let's start with Target.** When Target admitted that the data from as many as 110 million customers and cards was stolen in a cyber attack, something unusual happened: it damaged business. Target sales declined almost immediately after the breach was made public as the theft scared some customers off.

  This downward trend in sales will not likely be short term. Since the December 2013 announcement of the breach, Target has acknowledged that patrons who shopped at the retailer outside of the November 27 and December 15 period may have also been affected. If this proves to be the case, such news will add to the overall impact of the breach to Target's business as will the more than 40 lawsuits related to the breach filed thus far against the large discount retailer.

  Target has taken steps to try and limit the damage of the data theft to its brand by releasing full-page newspaper advertisements apologizing for the attack. In addition, the company is providing customers with free services designed to protect their credit ratings and identity.

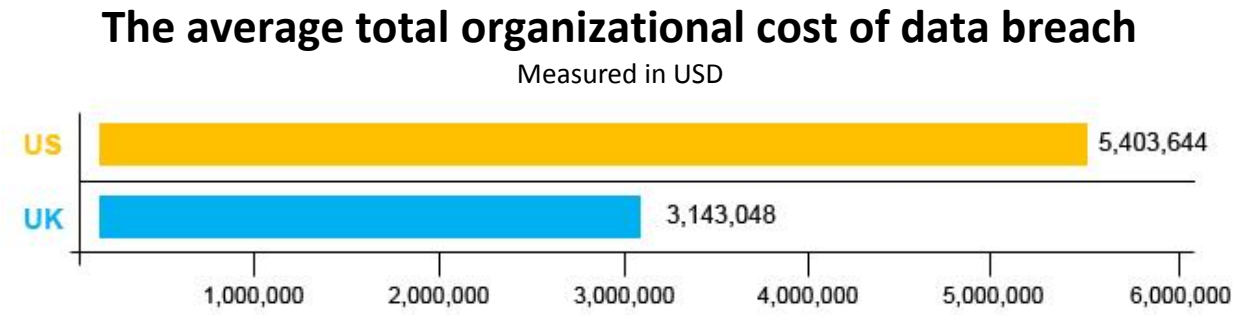
- **What about the merchant community in general?** IntelCrawler, a cyber security firm, has reported that BlackPOS, the point-of-sale (POS)-targeting malware implicated in the Target and Neiman Marcus breaches, has been discovered at six other U.S. retailers. As the news of additional breaches emerges, the impact of them spreads more broadly across the general merchant community. It is likely that one of the results of this impact will be a loss in consumer confidence that could create a downdraft on retail sales in general.

  To address the erosion of consumer confidence, retailers and other industry players will see an increase in their expense related to their technology infrastructure as upgrades designed to limit exposure of card and customer data are done. These additional expenses come on the heels of merchants spending tens of billions of dollars over the past five years to ensure that

the estimated 12.6 million "endpoints" where consumers transact complied with Payment Card Industry (PCI) security standards**.**

Clearly that wasn't enough to prevent the largest security breach in history and these new investments, unlike those for PCI compliance, are reactive rather than proactive which may not satisfy consumer concerns about to paying for goods and services with cards.

Possibly the one good thing that comes out of these damaging criminal acts is the long-awaited push for EMV adoption, something that has become the norm in Europe but has lacked support from merchants in the United States. Roughly a decade ago, Target executives ended an attempt to convert to EMV-chip payment cards to improve security. Since the breach, Target's CEO Gregg Steinhafel has been urging retailers and banks to deploy EMV chip-based cards. Target is not alone in its recent renewed support of EMV. According to Chester Wisniewski, senior security at Sophos, without a massive shift towards EMV, data breaches of this size and scale will continue to plague the retail industry. Additionally, there has been a renewed focus on the utilization of encryption and tokenization to strengthen the payment system further.



Source: Ponemon Institute/Symantec

- **What is the mindset of cardholders?** In the wake of the 2013 holiday season breaches, multiple experts have pointed out that while consumers are not more at risk now than they were before, most are more aware of the danger. Many more cardholders may now understand the difference between the level of inconvenience and exposure they will experience when a debit card versus a credit card is compromised. So, though few commentators are suggesting that consumers will stop using cards to purchase goods and services, what type of card they use – debit or credit – and whose card they use, may change.

  In the long run, the concern created among consumers by the recent breaches may generally heighten their awareness concerning ways they can better protect their cards and identity.

Many more may become proactive in monitoring their card accounts and avoiding the fraud schemes perpetrated on the telephone, email and social media. Also, to protect the consumer further, there is a growing discussion around increasing the government's power for regulating the security practices being used by merchants, financial institutions, networks and processors.

- **Are issuers up to the task?** Issuers have used a combination of tactics to address the recent breaches with the goal of limiting losses in the short term. Some have taken the bulk of the cost and inconvenience on themselves, cancelling the compromised cards and re-issuing new ones. Others have placed the burden on the cardholder to monitor and report fraudulent transactions or incur liability for them. In addition, some issuers set limits on cash withdrawals and purchase amounts in the middle of the holiday season when consumer purchases are highest in volume and value. In some cases, these actions by issuers have stemmed the erosion of the cardholder's trust. In other cases, they have further compromised the consumers' view of issuers as trusted payment providers.

Who are the victims?

Legend

• A plus (+) sign indicates a 10% or greater increase from the previous year's report

• A minus (-) sign indicates a 10% or greater decrease from the previous year's report

Source: Verizon 2013 Data Breach Investigations Report

In addition to supporting the acceleration of the implementation of EMV in the United States, some issuers have begun to advocate technology that would leapfrog existing solutions and provide more comprehensive security measures. During a quarterly earnings conference call in January 2014, U.S. Bancorp CEO Richard Davis expressed concerns that EMV did not go far enough. According to Davis, now is the time to consider options such as tokenization, a

method of obscuring card information by replacing it with a limited-use token, and encrypting data before storing it in the cloud. Both strategies would further secure sensitive information while laying the foundation for growth in the adoption of payments made with mobile devices.

- **Networks:** Of all the players in the payments ecosystems, networks have a track record for being most actively engaged in educating retailers about security threats and advising about the measures that should be taken to address the related risks. In April 2013, Visa published a bulletin to its retailers describing mitigation strategies to address the malware used to attack Target. The bulletin entitled *"Retail Merchants Targeted by Memory-Parsing Malware"* was updated in August 2013 describing specifics actions Visa retailers should take to prevent or limit intrusions in their networks and POS systems.

  After disclosure of the breach, the networks were key in helping their issuers identify the exact impact of the breach and in defining what options were available to the retailers for addressing the damage done. Networks also have been aggressive in addressing the cardholders' concerns by publicising their zero-liability offerings and offering counselling and assistance to identify theft victims. Longer term, networks will assess the fraud and risk measures adopted by issuers and acquirers using the results of that assessment to establish future interchange rates.

WHY THE INDUSTRY SHOULD BE CONCERNED ABOUT THE FUTURE

Data theft is lucrative: Stolen data can be worth as much as $80 per card making the Target breach alone a several billion-dollar payday for those involved. This type of opportunity is attracting international, organized crime rings willing to make substantial investments in the tools required to compromise databases around the world. In addition, the extent of thefts by these groups are broader and deeper than the general public is aware since financial institutions and payment networks are forbidden by law from naming merchants that have been breached, unless the merchants themselves disclose their exposure. Whatever the actual numbers are, experts agree that attacks targeting card information will not only continue but also increase.

Data theft impacts consumers broadly: Though the cardholders' liability for unauthorized transactions is limited under federal law, the impact to consumers whose debit and credit cards are compromised reaches beyond the monetary. Repeatedly having to review transactions across multiple accounts, reporting fraud and waiting for a credit card to be re-issued or re-activated is a

time-consuming experience one out of 10 Americans go through annually. With debit cards, the impact on a cardholder's life is worse. Monetary exposure can be as high as $500 depending on when the cardholder reports the fraud. If a report is filed beyond 60 days, all losses fall to the cardholder. In addition, studies have shown that a breach involving an ATM/debit card can require more than 300 hours of effort from the cardholder to address. Such inconveniences directly impact cardholder loyalty and use levels as well as the profitability of the payments industry.

Data theft can be a catalyst for the next wave of innovation: The breaches announced in late 2013 should create a greater sense of urgency around the adoption of technologies designed to limit the vulnerability of payments systems. This includes near term, generally available technologies such as those used in the EMV standard. It also should encourage investigation into the viability of options such as tokenization, encryption and similar strategies that rely on credentials that are never "in the clear."

Studies focused on the obstacles that have slowed the adoption of payments made with digital devices (e.g., Smartphones, tablets, laptops) online and in-store have shown consistently that the greatest areas of concern for consumers exist around security. Innovations that address data breaches and work within the growing ecosystem of devices used by the consumer could limit the success of the criminal participants in the industry and unlock a potentially lucrative digital payments segment for the legitimate players in the payments space.

A Word About The Sponsor Of This Paper

RS Software understands today's payment environment because it has participated in its evolution through two decades of working with industry leaders. We have helped our clients address the convergence of payment types, the proliferation of mobile devices, the move to cloud computing and the introduction of new strategies, such as behavioral targeting. We have built solutions to support the introduction of new standards such as EMV, encryption, and tokenization and of new technologies such as mobile and contactless payments, while mitigating the pain and cost associated with the legacy systems supporting them.

Our largest client is the world's biggest payments network. We have worked with this client for more than 20 years investing over 6000 person years across 150 payment applications within their organization. After the breaches reported in December 2013, we worked with them to deliver

proactive risk management and help minimize the risk exposure to issuers. Our areas of focus included:

- Automation of the analysis process using a combination of technology (ETL, Hadoop) and domain expertise (what-if analysis, drill-down / drill across) to define the overall objectives of the analysis
- Prioritization of communications to issuers, based on the size of the portfolio and the risk exposure, to tackle the problem of a huge amount of data
- Qualification and pre-screening of the data for compromised merchant locations for reported duration using geo-location, photonic / pneumonic searches to identify the affected issuers
- Creation of rule-based strategies that match activity against conditions that help to accurately derive lists of compromised card numbers and the number and value of transactions performed on cards during the period
- Development of a risk based, anti-fraud detection tool to establish intricate identity linkage across transactions that establishes scores and attributes that readily expose fraudulent activity within affected cards (establish and establishes in same sentence?)

These activities resulted in the following benefits for our client:

- Enhanced accuracy and reduced false positives
- Improved detection and reduced need for manual intervention
- Minimized cardholder and issuer impact
- Improved operational efficiency and data reporting
- Lower overall operational costs