Institution Solutions

Target Corporation Data Breach: Repercussions for Credit Unions

HELPING MEMBERS WITH ISSUES OF FRAUD

BY

PAUL CLAMPITT

WHITE PAPER

JANUARY 2014

Target and the Credit Union Paradigm

Executive Summary

Forty million Target Corporation in-store shoppers were victimized by a major data breach that spanned November 27 through December 15, 2013. Hackers hijacked sensitive information — including PIN numbers — residing on the magnetic strip of both debit and credit cards. The breach occurred as a result of malware installed on Target's point-of-sale terminals in each of its 1,797 store locations. Compromised accounts include Target's proprietary cards and those of other issuing banks, constituting every major card brand. Illicit websites immediately began selling the compromised information "dumps" to international card counterfeiters and fraudsters, and back to issuing banks trying to mitigate their risk. Confirmed fraud involving the compromised card information was detected by multiple card processing companies on or before December 18, 2013, when the breach was first reported.

Subsequent forensics revealed an additional 70 million identities were taken during the same intrusion; this information includes names, mailing addresses, and phone numbers or email addresses. Whether the 70 million identities includes online Target shoppers has not been clarified, but suspicions are rising. The second component of the data breach was disclosed on January 10, 2014, making the Black Friday Target breach the most extensive in history. There was a second announcement made the same day — late that afternoon, high-end retailer Neiman Marcus disclosed that the company experienced a similar breach during the Black Friday shopping window. Although precise circumstances of the Neiman Marcus breach have not been disclosed, the gravity of a sophisticated and coordinated attack against multiple retailers is frightening.

From a damage perspective, the Target breach is probably the worst in history. Certainly, the fraudulent use of the stolen information is pervasive and disturbingly audacious. There is no question, people and companies are being victimized by fraud made possible because of the compromised Target information.

The Credit Union Challenge

Quite often, folks turn to a financial institution for guidance and protection from the threat of a major breach — for many families their trusted source is a local credit union. And why not? The lifeline for any credit union is a secure base of satisfied members. Few acts are more endearing than a credit union standing shoulder-to-shoulder, brothers-in-arms with its member to defend their financial well-being against international criminals. After all, no one wants to be intimidated or threatened by "Boris and Natasha" stamping out bogus credit cards in Kaunas, Lithuania.

How extensive is the problem and what is the likely impact on a credit union's membership? To begin, the breach occurred at every Target store scattered throughout the country — no region or area was spared. One major card issuer, J.P. Morgan Chase, contacted 2 million of its affected debit cardholders. Chase estimates the compromised cardholders to be nearly 10 percent of its customer base. Extrapolating 40 million card thefts from total debit and credit cards issued in the U.S. yields a similar victimization rate of 8.4 percent. As always, the family victimization rate is higher, probably around 15 percent when duplications are eliminated. Senator Edward J. Markey (D-Mass.) summed the situation succinctly, "*When a number equal to nearly one-fourth of America's population is affected by a data breach, it is a serious concern that must be addressed.*"

Additionally, many credit union commercial accounts, particularly retailers and merchants, will be affected by subsequent fraud in weeks and months to come. Finally, for those credit unions that have issued credit and debit cards, their problems are further compounded by expenses associated with reissuing new cards and PIN numbers.

Yes, the Target data breach is very serious for credit unions and their members. Find out why we call the breach

The Nightmare Before Christmas!

Target Corporation Data Breach: Repercussions for Credit Unions

HELPING MEMBERS WITH ISSUES OF FRAUD

First public disclosure; An admission by Target

On December 19, 2013, Target Corp. confirmed a report issued the previous day that hackers hijacked sensitive data from 40 million payment cards. The affected data included customer names and credit or debit card numbers. The expiration dates associated with those cards were also compromised, giving thieves the data required to make purchases at some merchant web sites. The cyber criminals also made off with the CVV, or Card Verification Value code, which resides on the magnetic stripe of payment cards.[2] Apparently, they did not access the CVV2 code, the 3- or 4-digit code used by many online retailers to verify that a consumer making a purchase has the card in their hand. However, not all retailers ask for the CVV2 code and are, as a consequence, at risk.

No bargains on “Black Friday” at Target

The cards were used by shoppers who visited Target stores from November 27 through December 15. Apparently the breach occurred during the period when Americans kick off their holiday shopping and store traffic is normally at its highest during the year. Retailers try to lure shoppers to stores on Black Friday with "door buster" deals and overnight hours that often draw big crowds.

Target cards and those of every major brand

Affected payment cards include Target's REDcard private label debit and credit cards as well as other bank cards, Target spokeswoman Molly Snyder told Reuters.[1] KrebsOnSecurity, a closely watched security blog that broke the news on December 18, said the breach involved nearly all of Target's 1,797 stores in the United States. Target said its online business had not been impacted.

Merry Christmas from Target

Target notified law enforcement and the financial institutions that issue the credit and debit cards. The retail chain also posted a note on Target.com notifying consumers of the data breach: *“You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports.”*

Potentially horrendous consequences

Reuters reported that Target, itself, did not detect the intrusion but was alerted by credit card processors who detected a surge in fraudulent transactions involving cards used at Target. This information could have far reaching consequences but it was disclosed by a source familiar with the investigation who was not authorized to discuss the matter.[1] The *New York Times* reports that as early as December 11, fraud analysts *detected "a ten to twentyfold increase in the number of high-value stolen cards on black market websites, from nearly every bank and credit union."*[19]

The incident is the most extensive breach reported by a U.S. retailer. The second-largest breach against a U.S. retailer, uncovered in 2007 at TJX Cos Inc, led to the theft of data from more than 90 million credit cards over 18 months.

The timing of the breach could not have been worse for Target, rearing its head during the busiest shopping window of the year after what had already been a dismal holiday season. Weeks prior to the data breach, Target lowered its annual profit forecast after disappointing third quarter sales. The breach also comes at a time that Target is trying to build its online business, which only constitutes about 2 percent of sales. Compounding these woes is the fact that Target used its store-branded credit and debit cards as a marketing incentive to attract shoppers with a 5 percent discount. In fact, one-in-five store-customers carry the Target-branded card. Target has also found that households activating Target cards increase their store spending by 50 percent on average.[13] Consequently, loss of confidence in the Target card mechanism could have a deleterious impact on the company's profitability.

Complaints from customers erupted on social media as cardholders learned of the data breach. Customers clogged Target's phone lines, jammed its credit card website, and left angry posts on the corporate Facebook page. Ms. Snyder said Target was experiencing "extremely high" call volume and was adding employees to its call centers to answer questions concerning the security breach.

"An attack against a major retailer during the peak of the Christmas season undermines confidence," said Mark Rasch, former prosecutor of cyber crimes.[1]

Target, the third-largest U.S. retailer, is working with the Secret Service and Dept. of Justice[10] and outside experts (Verizon Communications) to prevent future attacks. Initially, the company did not disclose how its systems were compromised. However, the *Wall Street Journal* reported:

> *"In this case, malicious software, or malware, made its way onto Target's point-of-sale terminals—the red credit-card swiping machines in checkout aisles, according to people familiar with the breach investigation."*[3]

Problems mount as reality sets in

Bank fraud departments throughout the U.S. reacted quickly and decisively to limit their losses. Typically, banks are responsible for financial losses tied to fraudulent transactions, though in some significant cases, that responsibility may be passed on to the merchant. J.P. Morgan Chase placed daily limits on use by debit card holders who shopped at Target Corp. The limitations were intended only during the period required to reissue cards. Daily cash withdrawals were limited to $100 with a $300 daily limit on purchases.[8] Holiday shoppers were furious and vocal, taking their complaints to social media.

Problems mount as reality sets in (Continued)

Two days later, on December 23, J.P. Morgan Chase eased back on the limitations. The big New York bank issued emails to customers and posted a notice on its website, saying that most customers whose card information had been compromised at Target now would be permitted to withdraw $250 from ATMs and make $1,000 in daily debit card purchases. The new limits were still below the typical caps set for many cardholders. Customers traveling overseas were not allowed to use their debit cards at ATMs or to make purchases.[9]

An egregious loss of credibility

Although Target initially contended that the card PIN data had not been compromised, the company recanted this assessment on December 27. Target admitted that PIN data was lifted during its massive data breach, but was *"confident that PIN numbers are safe and secure."* But through *"additional forensics work"* the company confirmed *"that strongly encrypted PIN data was removed." "The PIN information was fully encrypted at the keypad, remained encrypted within our system, and remained encrypted when it was removed from our systems,"* Target said.[16] This admission ignited another firestorm of furious cardholder criticism which often questioned Target's credibility and sincerity with its customers when dealing with the breach — nightmare complete!

Another card complication; further loss of confidence

In the midst of Target's struggle to retain customer loyalty and restore brand confidence in its branded cards, a story broke claiming that some customers have been unable to use their Target gift cards because they were not fully activated.

"We are aware that some Target gift cards were not fully activated and apologize for the inconvenience," said Target spokeswoman Molly Snyder in an e-mail. *"The company will honor the affected cards."*[15]

Enter the politicians and litigators

Senator Richard Blumenthal (D-Conn.) sent a scathing letter to the Federal Trade Commission, urging the agency to investigate Target's responsibility in the massive breach. He said that the scope and duration of the intrusion suggests that the retailer may have relied on a lax security program that *"does not live up to a reasonable standard."* Target's conduct would be *"unfair and deceptive,"* Blumenthal wrote.[12] Blumenthal's comments seemed to echo the complaints filed in more than a dozen class action lawsuits against Target in response to the breach.

Behind a very dark curtain

KrebsOnSecurity reports that credit and debit card accounts stolen in the Target data breach are flooding underground black markets, selling in batches of one million cards and priced from $20 to more than $100 per card. Banks are buying huge chunks of their own card accounts from illicit online "card shops."[18]

One card store is well-known for selling quality "dumps," data stolen from the magnetic stripe on the backs of credit and debit cards. This information allows thieves to clone the cards for use in stores. If the dumps are from debit cards and the thieves also have access to the PIN number, they can use the cloned cards at ATMs to pull cash from the victim's bank account. Indeed, shortly after the Target breach began, the proprietor of this card shop — a miscreant nicknamed *"Rescator"* and a key figure on a Russian-language cybercrime forum known as *"Lampeduza"* — began advertising a new base of one million cards, called Tortuga.[17]

KrebsOnSecurity was asked by a small, issuing bank to help recover (through online purchase) the bank's credit card accounts compromised through Target. The first step was to determine if the bank's cards were, in fact, being offered for sale via the illicit card shop's website – described as *"remarkably efficient and customer friendly."* Like other card shops, this store allows customers to search for available cards using a number of qualifications, including BIN (a bank's unique number which is merely the first six digits of a debit or credit card); dozens of card types (MasterCard, Visa, et. al.); expiration date; track type; country; and the name of the financial institution that issued the card.

Cards were, in fact, identified as a mix of MasterCard dumps ranging in price from $26.60 to $44.80 apiece. Purchases are settled on these illicit websites with irreversible payment mechanisms, including virtual currencies like Bitcoin, Litecoin, WebMoney and PerfectMoney, as well as the more traditional wire transfers via Western Union and MoneyGram.[17]

Another fascinating feature of this card shop is that it appears to include the ZIP code and city of the store from which the cards were stolen. Apparently, this information is included to help fraudsters purchasing the dumps to make same-state purchases, thus avoiding any knee-jerk fraud defenses the financial institution might use to block out-of-state transactions from a known compromised card.

The bank quickly ran fraud and common point-of-purchase analyses on each of the dumps purchased. The bank's database showed that all had been used by customers to make purchases at Target stores between November 29 and December 15. Some cards had already been tagged "confirmed fraud," while others were just issued and had only been used at Target. KebsOnSecurity and the bank also discovered that a number of the cards were flagged for fraud following the compromise after they were used to make unauthorized purchases at big box retailers, *"including – wait for it – Target."*[17]

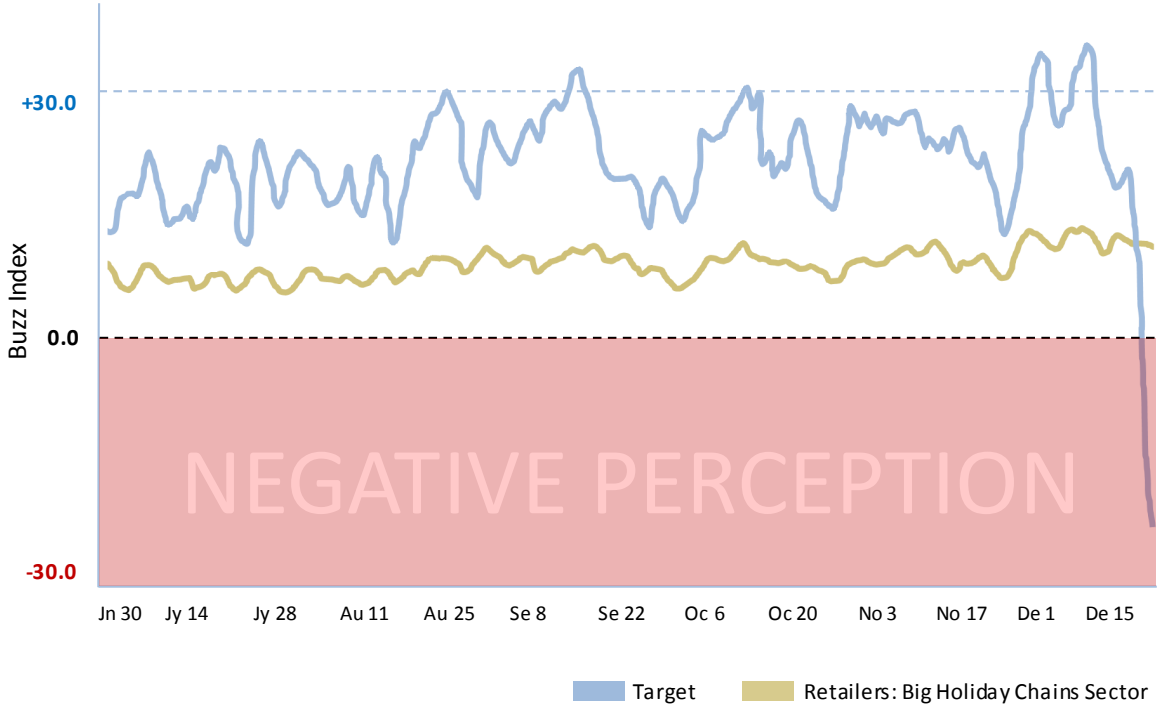
Fraud specialists explained that criminals often use stolen dumps to purchase high-priced items such as Xbox consoles and high-dollar amount gift cards that can be fenced, auctioned or offloaded quickly and easily for cash.

Circumstances have crushed consumer perception of Target

Consumer perception about the Target brand has dropped steeply since news of the data breach first surfaced. Perception is empirically measured by *You Gov BrandIndex*, which surveys 4,300 people daily. The index ranges from positive 100 to negative 100 and is compiled by subtracting negative customer feedback from positive customer feedback. Prior to the breach, Target's index was plus 26, higher than the rating of 12 of its peer group of retailers including Wal-Mart. Target's current index is negative 19, the first time in six years that negative perception of Target has outweighed positive feelings about the brand.[14]

Target's drop in consumer perception is more severe than brands damaged by similar large-scale security breaches, such as Sony Online Entertainment and Citibank. The lower perception may also indicate that Target Chief Executive Gregg Steinhafel failed in his effort to soothe patrons with store discounts and promises of free credit monitoring for shoppers affected by the breach.[12]

Vaporizing Target's Customer Goodwill



Target discloses 70 million more breached identities

On January 10, 2014, Target Corp. said that up to 70 million individuals had their personal information stolen as part of the recent data breach. The company said those 70 million people were separate from the approximately 40 million credit and debit card accounts previously reported as compromised, though there was some overlap. Nevertheless, the Black Friday Target breach is now the largest ever perpetrated against a U.S. retailer!

Target said the stolen personal information included names, mailing addresses, phone numbers or email addresses. Still, the retailer noted that the theft isn't a new breach but was uncovered as part of its continuing investigation.

Neiman Marcus victimized by Target-like intrusion

Neiman Marcus Group Ltd. reported on January 10, 2014, that customer payment card information was stolen and that unauthorized (fraudulent) charges were made during the holiday season.[20] While a direct connection has yet to be disclosed, cyber-security experts are speculating that the Target and Neiman Marcus data breaches are related or connected.[21]

The company confirmed that its customers are at risk after hackers breached its servers and accessed payment information of those who visited its bricks-and-mortar stores. Neiman Marcus operates 79 retail locations. Neiman Marcus spokesperson Ginger Reeder said, *". . . There is no evidence that shoppers who purchased from the company's online stores were affected by this breach."* [22]

KrebsOnSecurity previously reported a spike in fraudulent credit and debit card charges on cards that had been used at Neiman Marcus stores. Neiman Marcus said it was informed of the breach in mid-December by its credit card processor and that the company subsequently informed law enforcement officials, including the Secret Service.

> *"According to people familiar with details of the incident, fewer than one million cards belonging to people who shopped at the luxury retailer may have been compromised. The would make the Neiman Marcus incident much smaller than the massive attack at Target Corp. Regardless of size, the Neiman Marcus breach is bad news for the retail industry, undercutting confidence in credit-card security."*[20]

More undisclosed breaches in the shadows

A report released by Reuters on January 12, said that Target Corp. and Neiman Marcus are not the only retailers to experience security breaches over the holiday shopping season. Sources familiar with attacks on other merchants said that smaller breaches were perpetrated against at least three other well-known U.S. retailers that have yet to be publicly disclosed. According to Reuters, the companies are retailers with outlets in malls. Reuters also reports that sources believe the perpetrators may be the same who launched the Target attack, but at this point they are still trying to find the culprits behind all of the security breaches. Law enforcement sources said they suspect the ring leaders are from Eastern Europe, which is where most big cyber crime cases have been launched over the past decade.[22]

Retailers forced to accept EMV technology; focus on mobile devices

The Target data breach has focused a spotlight on America's woefully outdated credit card technology. No country other than the U.S. uses "swipe and sign" credit cards. Europe, Latin America, Asia, Africa, and the Middle East rely on EMV technology: Credit and debit cards with embedded chips that are protected by a personal identification number that generates a unique verification code every time a transaction is completed. EMV technology makes it difficult to counterfeit cards with stolen data.[7] As thieves found themselves thwarted by EMV technology, they feasted on the world's easiest target – the United States.

EMV cards are inserted into credit terminals instead of swiped. The chip sends a signal with a unique security code through the network, where the transaction is verified and authorized. Instead of signing for a purchase, consumers enter a PIN, which adds an extra layer of security protection. Without that PIN, a stolen card cannot be used for purchases in stores or to withdraw money from ATMs.

The U.S. is not scheduled for EMV technology until 2015. Why the delay? There are 8 million U.S. merchants who will need to upgrade their point-of-sale structure. More than 1 billion credit and debit cards will need to be reissued. Every gas station fuel pump and ATM in the country will have to be modified. And there are countless nagging technical issues to coordinate among the country's 7,000 financial institutions. The change will require billions of dollars.

A significant consequence of the conversion to EMV will be a shift in who swallows the losses associated with fraud. Banks could argue, as they have done overseas, that consumers are responsible when cards are compromised, accusing them of sharing PIN information. And retailers who fail to convert to EMV after October 2015 will be held liable for fraudulent purchases instead of the issuing bank.

U.S. retailers, for the most part, view EMV as a burdensome expense, with little upside beyond improved data security. Mobile device technology, on the other hand, promises more in terms of future marketing capability and customer loyalty.[11] Many retailers are convinced that mobile offers more pluses than minuses as the American consumer adopts that technology.

Considerations for merchants responding to the Target breach

The enormity and severity of the Target breach has serious implications for any U.S. merchant/retailer accepting debit or credit cards as a mechanism for transaction payment. Generally speaking, merchants should be extremely proactive when detecting and dealing with any suspicious activity.

Web retailers should verify that the billing address a consumer enters matches the address on record for the card being used. It would appear that the fraudsters do not have access to the address; therefore, a retailer who verifies the address and requires a match lessens the risk of being defrauded.

When a merchant identifies a fraudulent order, the merchant should note all order details, such as shipping address and e-mail address. *"It is more likely that fraud details will be used repeatedly during a data breach and this will help prevent repeat criminal attacks if it is the same organized crime group,"* recommends Julie Fergerson, vice president of emerging technologies at Ethoca Ltd.

"Be vigilant," Fergerson advises. *"Educate your fraud team to look for patterns that seem unusual or out of the ordinary. Often there are signs that in isolation don't seem like a warning, but in the context of a data breach they can help to more quickly identify and shore up any holes the criminals may be attempting to exploit."*

- Note any increase in orders being routed for manual review, as that could be an indication that the criminals responsible for this attack are using the card numbers to commit fraud at e-retail sites.
- Review chargeback complaints from legitimate cardholders. Although there is typically a delay of four to six weeks between the fraud and the cardholder complaining, *"chargebacks may be the first indication that the merchant is a victim of increased fraud volumes due to the data compromise,"* Fergerson says.

Incidents like these underscore the importance of retailers paying close attention to protecting payment card data, says John Kindervag, a vice president and principal analyst at Forrester Research Inc. He says a breach in 2007 at TJX Cos., operator of such retail chains as TJ Maxx and Marshalls, likely cost the company between $100 million and $250 million.

"Usually in credit card security, people are very penny-wise and pound-foolish," Kindervag says. *"This is a business of 'pay me now or pay me a lot later.'"*

Suggestions for credit union members

Michael Blanco, a fraud specialist with Global Institutional Solutions (GIS) says that his company is experiencing a dramatic increase in proactive calls from customers concerned about the Target breach. GIS provides identity theft resolution services for insurance company policyholders and members of credit unions. The company also assists individuals in protecting themselves from future fraud. *"Target isn't like many large-scale breaches,"* Blanco said. *"Some compromised accounts are definitely experiencing confirmed fraud."*

Suggestions for credit union members (Continued)

"It is important for consumers to realize that just because they shopped at a Target store before Christmas, they are not necessarily a victim of fraud. But many shoppers are worried – in fact, they're very worried!" Mr. Blanco offered the following suggestions for concerned cardholders trying to confront the issue without professional assistance.

1) Monitor your accounts daily from a secured internet connection. Daily, log into your accounts and review your balances and account activity. If there are errors or suspicious transactions, immediately contact your bank or credit card issuer.

2) Change your passwords for online financial accounts. Use a password that is not easily guessed or is based on your children's names, mother's maiden name, or family birthdates.

3) Cancel and replace your credit and/or debit cards. Ask your bank or credit card issuer to cancel any card used at Target and to issue a new card. If you used a debit card at Target, change the PIN number on your card.

4) Talk with your financial institutions about setting transaction dollar limits on your cards. Ask that an alert be issued to you if a transaction exceeds the dollar limit. Review the alerts.

5) Consider placing a security freeze on your credit files. A credit file security freeze will keep the credit bureaus from issuing your credit report without your express consent. This will prohibit a cybercriminal from opening a new credit account using the information obtained from the Target breach, but only if the new account provider checks the credit file.

6) Be vigilant in monitoring e-mails. Don't respond to an email that appears to be from your financial institution without first contacting your financial institution. Phishing e-mails are common after breaches, and criminals use these phishing e-mails to attempt to gain additional information from consumers.

References

[1] **Finkle, Jim and Skariachan, Dhanya.** *Target cyber breach hits 40 million payment cards at holiday peak*. ***Reuters***. December 19, 2013.

[2] **Davis, Don.** *Target confirms loss of 40 million card numbers.* ***InternetRETAILER***. December 19, 2013.

[3] **Germano, Sara.** *Target Faces Backlash after 20-Day Security Breach: Retailer Says 40 Million Accounts May Have Been Affected Between Nov. 27 and Dec. 15.* ***The Wall Street Journal***. December 19, 2013.

[4] **Sidel, Robin; Yadron, Danny; and Germano, Sara.** *Target Hit by Credit-Card Breach: Customers' Info May Have Been Stolen Over Black Friday Weekend*. ***The Wall Street Journal***. December 18, 2013.

[5] **Germano, Sara.** *Target's Data-Breach Timeline*. ***The Wall Street Journal***. December 27, 2013.

[6] **Webb, Tom.** *Target data breach creates social media buzz*. ***Pioneer Press***. December 30, 2013.

[7] **Christmann, Samantha.** *Behind the credit chip curve, U.S. playing catch-up with Canada, rest of world on card security.* ***The Buffalo News***. January 1, 2014.

[8] **Germano, Sara and Fitzpatrick, Dan.** *J.P. Morgan Chase Places Limits on Debit Cards Used During Target Breach: Caps Placed on Cash Withdrawals and Daily Purchases from Affected Accounts for Now*. ***The Wall Street Journal***. December 21, 2013.

[9] **Germano, Sara and Sidel, Robin.** *Target Discusses Breach with State Attorneys: Retailer Updates Officials on Investigation*. ***The Wall Street Journal***. December 23, 2013.

[10] **D'Innocenzio, Anne.** *Target: Justice Dept. investigates data breach.* ***USA Today***. December 23, 2013.

[11] **Abcede, Angel.** *Ramifications of Target's Data Breach: Impact may fuel push for either EMV or mobile strategies.* ***CSP Daily News***. January 2, 2014.

[12] **Hsu, Tiffany.** *Fallout from Target customer data breach shows in sentiment survey: Consumers' perception of Target has fallen to its lowest point since at least 2007, a survey by YouGov BrandIndex finds. An effort to soothe patrons apparently fell short.* ***Los Angeles Times***. December 23, 2013.

[13] **D'Innocezio, Anne and Fowler, Bree** (Associated Press). *Fury and Frustration Over Target Data Breach*. ***ABC News***. New York. December 20, 2013.

[14] **Marzilli, Ted.** *Target perception falls after data breach*. ***You Gov BrandIndex***. December 23, 2013.

[15] **Dudley, Renee.** *Target Says Some Holiday Gift Cards' Activation Failed.* ***BloombergBusinessweek.*** December 31, 2013.

[16] **Katersky, Aaron and Kim, Susan.** *Target Admits Customer PIN Data Removed but Says It's 'Secure'.* ***ABC News.*** December 27, 2013.

[17] **KrebsOnSecurity.** *Cards Stolen in Target Breach Flood Underground Markets.* https://krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target/

[18] **Fox News.** *Debit and credit cards stolen in Target breach reportedly for sale in underground black markets*. 12/ 22/ 13.

[19] **Harris, Elizabeth A.** *Target Breach Affected Up to 110 Million Customers.* ***New York Times.*** January 10, 2014.

[20] **Sidel, Robin.** *Neiman Marcus Breach Appears Smaller Than Target's: Fewer Than One Million Cards May Have Been Compromised.* ***The Wall Street Journal.*** January 11, 2014.

[21] **D'Innocezio, Anne.** *Neiman Marcus Is Latest Victim of Security Breach.* ***Associated Press.*** January 11, 2014.

[22] **KrebsOnSecurity.** *Hackers Steal Card Data from Neiman Marcus.* January 10, 2014.

[22] **Finkle, Jim and Hosenball, Mark.** *Exclusive: More well-known U.S. retailers victims of cyber attacks –sources.* **Reuters.** January 12, 2014.

About Institution Solutions

Institution Solutions

Institution Solutions I, LLC (ISI) of Richardson, Texas is a Third Party Administrator (TPA) licensed in 48 states —administering association, affinity and group insurance programs for credit unions and group carriers. Organized in 1996 and led by Paul Clampitt (sole Principal), ISI holds endorsements with more than 550 national and/or regional credit unions, giving ISI the authority to market and administer insurance programs for their membership. ISI's credit union membership business is administered on ISI's consumer driven enterprise platform. The platform has the functionality to support web-based, direct to consumer – marketing, enrollment, issue, billing/collection, disbursement of premiums; and data analytics. Service touch points are minimized with electronic population of member/employee information and use of conditional logic to deliver optional coverage options.

Institution Solutions makes available to credit unions a suite of highly sophisticated, enterprise-level fraud solutions. These programs include: ***Privacy TouchPoint Services***℠, a personal identity management program for the member and their family; ***Incident Response Services***℠, an integrated business response to a breach of sensitive information; ***Merchant Chargeback Advocacy***℠, a program for the merchant retailer to deal with and reduce the incidence of chargebacks and transaction fraud; and ***Employment Practice Services***℠, a program to mitigate EPL and EBL risk.

Paul Clampitt

Paul Clampitt is the Chief Executive Officer of Institution Solutions, a company he founded in 1996. Since then, Paul has been steward over an impressive period of growth and achievement, making his company one of the leading third-party administrators of insurance products in the affinity market space. Prior to leading Institution Solutions, Paul was President and CEO of the brokerage firm Financial Fitness. He attended the Southwest CUNA Management School at the University of Houston and the University of Texas at San Antonio. Paul is a Board Member for the Professional Insurance Marketing Association (PIMA) and a frequent speaker at Industry Conferences, most recently PIMA's 2013 Affinity Summit.