Understanding Chargebacks

CHARGEBACK Advocacy℠
REDUCING TRANSACTION RISK

Target Data Breach:
Lessons for the Retailer To Consider

Bankers Insurance Group

Global Institutional Solutions

Originally published in
THE MERCHANT Advocate
Journal of Merchant Chargeback Services.
January 2014.

Nightmare before Christmas

Armageddon at Target: Forty Million Lessons from a Data Breach Gone Rogue

The Crime

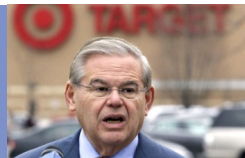
ON DECEMBER 19, 2013, TARGET CORP. CONFIRMED A previous-day report that hackers hijacked sensitive data from 40 million payment cards. The affected data included customer names and credit– or debit-card numbers. The expiration dates associated with those cards were also compromised, giving thieves the data required to make purchases at some retail web sites. The cyber criminals also made off with the CVV, or Card Verification Value code, which resides on the magnetic stripe of credit and debit cards.[2] Apparently, they did not access the CVV2 code, the 3- or 4-digit code used by many online retailers to verify that consumer making a purchase has the card in their hand. However, not all retailers ask for the CVV2 code. Therefore, there is some risk to e-retailers, and they should be on the alert, says one security expert.

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 around its highest of the year. Retailers try to lure shoppers to stores on Black Friday with "door buster" deals and overnight hours that often draw big crowds. The breach may have gone into the Monday after Thanksgiving. [4]

Target Cards and 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 December18, 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.



Potentially Horrendous Consequences

Reuters reported that Target, itself, did not detect the intrusion but was alerted by credit card processors who noticed a surge in fraudulent transactions involving cards used at Target. This information could have far reaching consequences. It was disclosed by a source familiar with the investigation who was not authorized to discuss the matter.[1]

The incident is the second-largest breach reported by a U.S. retailer. The 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 about 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.

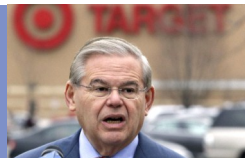
> *"Thank you Target for nearly costing me and my wife our identities, we will never shop or purchase anything in your store again," said one posting.*
>
> *"Shop at Target, become a target," remarked another. "Gee, thanks."*
>
> TARGET FACEBOOK PAGE

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.

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]

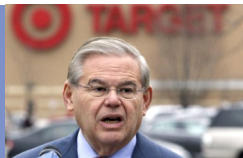
An Egregious Loss of Credibility

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 Cardholder 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

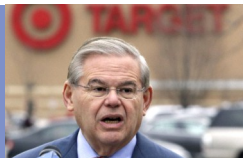
KrebsOnSecurity reports that credit and debit card accounts stolen in the Target data breach are flooding underground black markets, selling in batches of one million cards and priced from $20 to more than $100 per card. Banks are buying huge chunks of their own card accounts from illicit online "card 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 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 make same-state purchases, thus avoiding any knee-jerk fraud defenses in which a financial institution might block transactions out-of-state from a known compromised card.



Behind a Very Dark Curtain

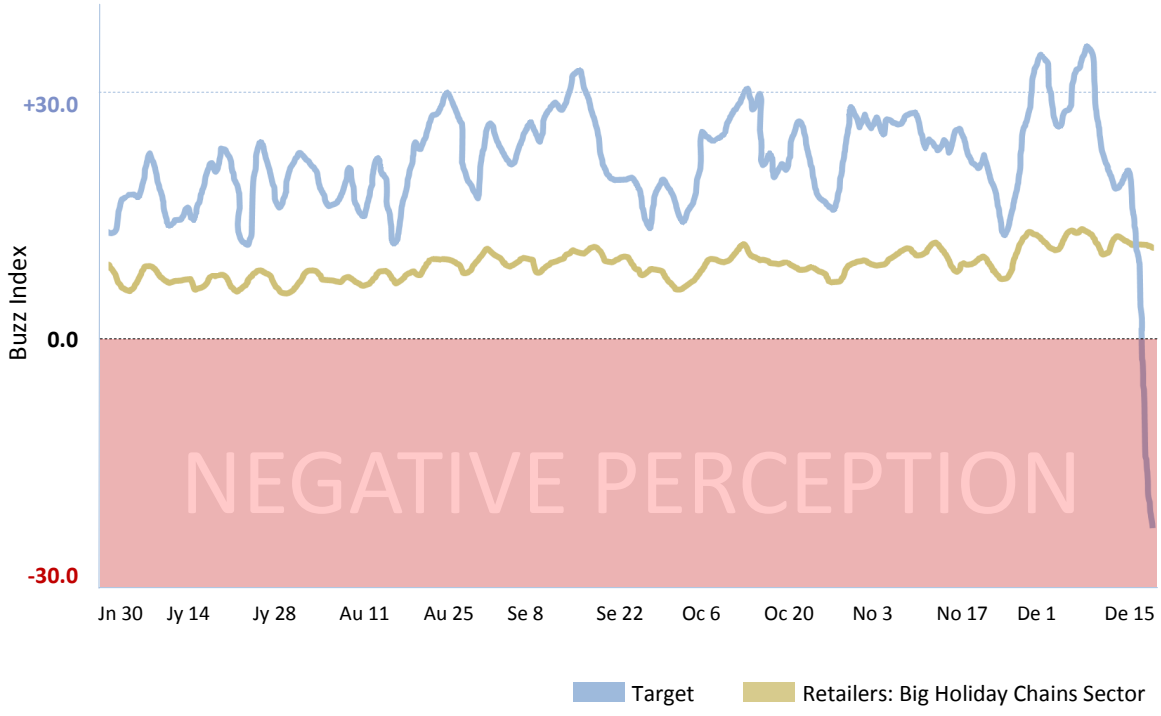
The bank quickly ran fraud and common point-of-purchase analyses on each of the cards purchased. The bank's database showed that all had been used by customers to make purchases at Target stores between November 29 and December 15. Some cards had already been tagged "confirmed fraud," while others were 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 (fraudulent) purchases at big box retailers, *"including – wait for it – Target."* [17]

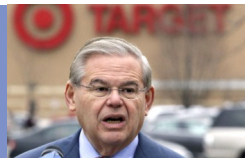
Fraud specialists explained that criminals often use stolen dumps to purchase high-priced items such as Xbox consoles and high-dollar amount gift cards that can be fenced, auctioned or offloaded quickly and easily for cash.

Consumer Perceptions Crushed

Consumer perception about the Target brand has dropped steeply since news of the data breach first surfaced. Perception is empirically measured by YouGov 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

Vaporizing Target's Customer Goodwill





Behind a Very Dark Curtain (Continued)

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]

Still Waiting for EMV Technology

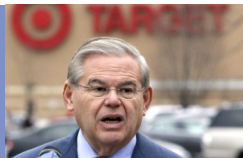
The Target data breach has focused a spotlight on America's woefully outdated credit card technology. No country other than the U.S. uses "swipe and sign" credit cards. Europe, Latin America, Asia, Africa, and the Middle East rely on EMV technology: Credit and debit cards with embedded chips that are 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

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.

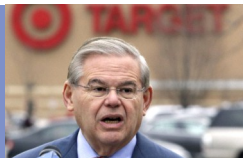
When a merchant identifies a fraudulent order, the merchant should note all order details, such as shipping address and e-mail address. *"It is more likely that fraud details will be used repeatedly during a data breach and this will help prevent repeat criminal attacks if it is the same organized crime 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.'"*



References

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

[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*. Dec. 22