# A Security Breach at Target: A Different Type of BullsEye

**Peter A. Stanwick**
Associate Professor
Department of Management
Auburn University
Auburn, AL36849-5241

**Sarah D. Stanwick**
Associate Professor
School of Accountancy
Auburn University
Auburn, AL36849-5247

## *Introduction*

Javelin Strategy & Research issued a 2012 report that stated approximately 16 million consumers were notified that the security related to their credit card information had been compromised. The number of consumers who had been impacted by a security breach by cybercriminals had increased 340 percent from 2010 to 2012 and resulted in a fraud loss of $4.8 billion.

## *The Cyber Attack*

On December 18, 2013, it was announced that Target was investigating a security breach in which the credit card and debit card information of an estimated 40 million customers had been acquired by cybercriminals. It was disclosed that the cybercriminals had focused on the point-of-sale systems in Target retail stores. The information that was stolen included credit and debit card information as well as personal identification numbers (PINs). The information obtained by the cybercriminals would allow creation of counterfeit cards. With PINs, the criminals would be able to not only purchase items, but also withdraw money from ATMs using the related PINs. The two most common methods for cybercriminals use to obtain access to customer information at the point of sale terminal is to either have a company insider insert the malicious software (malware) into the company machine or convince an unsuspecting employee to download the malware into the point of sale system. The cybercriminals are then able to gain access to the consumer information that is stored on the magnetic stripe on the back of the credit and debit cards. The magnetic stripe contains valuable information such as account numbers and expiration dates. In Europe, credit cards with a smart-chip are commonly used to restrict the potential information that can be obtained from cybercriminals. While some credit cards in the United States do have a smart-chip, American retailers have resisted using the smart-chip technology in the purchasing transactions which take place within the stores. The reluctance to use the smart-chip technology has resulted in a disproportionate amount of credit card fraud occurring in the United States. The United States accounts for more than 47 percent of the total worldwide credit card fraud, yet the United States generates only 24 percent of the global credit card spending. In addition, over 80 countries globally use smart-chip technology, yet less than 1 percent of current credit cards issued in the United States have smart-chip technology.

The magnetic stripe technology was developed in the 1960s.The key difference in the two types of cards is the transferring of the consumer information. When a debit or credit card transaction uses the magnetic stripe the same data is transferred to the point of sale system every time. When a smart-chip technology based card is used, the data is encrypted and uses a different mathematical value for every transaction making it much more difficult for the cybercriminal to capture the consumer information that is being transferred to the point of sale system. Visa, MasterCard and other major credit card companies had set the target date of October 2015 for retail merchants in the United States to have smart-chip technology in the point of sale system. It is at this date when credit card companies are planning on requiring that the retailers will be held responsible for information theft if a card is chip-enabled but was not used in the transaction.

It is estimated that only between 15 million to 20 million current debit and credit cards have the chip out of the 5.6 billion credit cards in circulation in the United States. It is estimated by the Aite Group that credit card fraud would be cut in half if the chip technology was used by retailers at Point of Sale. It is estimated that only 14 percent of all point of sale terminals in the United States are capable of using the chip cards. Once this conversion has taken place, the burden for addressing the card fraud issues will shift from the credit card companies to the merchants.

From 2001 to 2004, Target partnered with Visa and had implemented using the smart chips in their stores. The use of chip technology was discontinued because Target was concerned that using the chip technology would slow down the check-out process and the marketing benefits were not as expected when the program was introduced.

### *The Reaction by Target*

On December 19, 2013, Target announced that a breach took place from November 27 to December 15, 2013. This announcement resulted in customers flooding Target's credit card website and their phone lines demanding information related to the breach. Target had called in the Secret Service to investigate the breach and hired a forensics team from Verizon Communications to also investigate how the security breach took place. Target's advice to its customers was that they "…should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account summaries."[1]

On December 24, 2013, underground web sites had been identified offering credit and debit card information pertaining to the Target security breach for up to $100 per card. A number of sites including Rescator.la, Kaddafi.hk, Octavian.su and cheapdumps.org were ordering the consumer information for sale. By December 31, 2013, approximately 40 class action lawsuits had been filed against Target for allowing the breach of the point of sale system. The class action lawsuits alleged that Target was guilty of negligence, fraud, breach of contract, breach of fiduciary duty, invasion of privacy and conversion. By January 22, 2014, credit unions estimated that they had spent up to $30 million to address their customers' security issues related to the Target breach. The credit unions estimated that the average cost was $5.10 per card. This cost included reissuing the customers' cards, having additional staff at customer service centers and account notification and monitoring costs. In February 2014, it was announced that the cybercriminals got into the Target computer servers by stealing the login credentials of a heating and air conditioning contractor. By getting the username and password from Fazio Mechanical Services, the cybercriminals were able to move through the Target computer network and found the storage area of the debit and credit card information pertaining to the Target customers who had used their cards at the point of sale terminals. Fazio Mechanical Services was connected remotely to Target computer systems for services which included electronic billing, the contract submission process and for various project management requirements.

On January 10, 2014, Target announced that the security breach was much larger than was initially reported. Instead of the original estimate of 40 million stolen card numbers, Target now stated that up to 110 million credit and debit card numbers with related information was stolen by the cybercriminals. In addition, information pertaining to the customers' addresses and phone numbers was also taken by the cybercriminals. The malware was identified as "BlackPOS" and was created in Russia. The malware is available for purchase online in the black market for as little as $1,800 when the attacks took place. The malware becomes embedded in the Windows operating system in the point of sale terminals at Target. When the card is swiped at the terminal, the data from the card is temporarily stored in the terminal RAM (memory) and is unencrypted during this time period. The cybercriminals had access to the central data network so they were able to transfer the malware to every point of sale terminal at Target in the United States for at least two weeks.

### *The Consequences of the Cyber Attack*

By January 15, 2014, 68 class action lawsuits had been filed against Target alleging that Target did not follow the proper procedure to protect the data obtained from the credit and debit cards. One of the plaintiffs, the Alabama State Employees Credit Union, claimed that they were "swamped" by customers demanding new credit and debit cards because they had purchased merchandise at Target using the cards.

[1] Sara Germano, Robin Sidel & Danny Yadron. 2013. "Target Faces Backlash After 20-Day Security Breach." *The Wall Street Journal*. December 19, 2013.

The Alabama State Employees Credit Union claimed that Target should compensate them for this additional financial burden. By February 2014, it was estimated that the financial cost to financial institutions wanting to address the issues related to the Target security breach were estimated to be $200 million. It is estimated that Target may have to repay banks up to $1.1 billion for the total costs associated with the security breach. If Target had replaced the magnetic strip with the smart chip technology the replacement cost would have been $100 million.

The cybercriminals have obtained 11 gigabytes of customer data, containing 40 million payment card information and 70 million records of customer information. The 11 gigabytes is less that the memory in an Apple's iPad Mini. A security blogger, Brian Krebs, a specialist in cybercrime contacted Target's public affairs line on December 18, 2013 to ask whether Target was the focus of a big data breach that underground criminal forums were discussing online.

### *The Change in Management*

On March 5, 2014, Beth Jacob, Target's Chief Information Officer and executive Vice President for technology services resigned due to the fallout over the security breach. Jacob started as an assistant buyer at Target in 1984. After leaving Target to work for American Express Financial Services, she came back to Target to take charge of Target's call centers. In 2008, Jacob was promoted to CIO to help co-ordinate the development of Target's web site in house after Target cancelled its outsourcing relationship related to web development with Amazon.com. Jacob did not appear to have a background in computer science. She has a degree in retail merchandising and a Master's in Business Administration degree.

It was also disclosed that Target had multiple opportunities to correct its computer security problems before the cyber-attack. Target had installed security software that had alerted management that there was suspicious activity occurring before the attacks took place. The software identified activity taking place that showed that the cybercriminals were uploading tools within the Target computer systems that would be later used to capture credit card and personal information. Target's management decided not to pursue the warnings from the security software and did not re-evaluate its level of security within their computer systems.

Target had disclosed that security experts had raised concerns about the security of Target's computer servers before the cyber-attack took place but did not make any revisions in its computer security system. For example, the experts had suggested that Target have a separate security wall protecting its payment system in addition to the general computer security systems. It was also recommended that Target preform a comprehensive security review of all its computer systems before the Christmas buying season. This review did not take place until after the security breach occurred. In addition, subsequent to the cyber-attack, Target established the creation of a new senior management position, chief information security officer which was announced in March 2014. In April 2014, Target announced that Bob DeRodes would become the new Chief Information Officer. DeRodes was a former senior information adviser to the United States Department of Homeland Security. He also was an advisor to the Secretary of Defense and the Justice Department as well as having work experience with companies such as Home Depot and Delta Airlines.

On May 5, 2014, Target's Chief Executive Officer, Gregg Steinhafel resigned his position as CEO. In addition to struggling sales in Canada and lower than expected customer traffic, a major reason why Steinhafel was asked to step down was the cyber-attack on Target's computer systems. The Board of Directors had determined that it was time for new leadership at the top position in Target. An analyst at Cowen, Faye Landes, stated that "The board also may have come to the conclusion that the problems leading to the credit breach were the results of underinvestment, which is a C.E.O. decision, and the aftereffect of the breach may ultimately be quite costly, which we believe to be the case."[2]

### *Summary*

In September 2014, a former Target manager in charge of cyber and global intelligence, Karl Mattson, concluded that Target's lack of having a Chief Information Security Officer was the "root cause" of the computer system breach. Target, like other retailers must put computer security at the forefront of its strategic decision making.

[2] Elizabeth Harris. 2014. "Faltering Target Parts Ways With Chief." The New York Times. May 5.

As a result, Target learned the hard way that there needs to be specific people in charge of evaluating and helping to minimize the risk of potential cyber-attacks. It also supported the belief that retailing cannot ignore weaknesses in its computer systems. It is critical to not only have security software in place to prevent cyber-attacks but it is also critical for retailers to react to warning signs given by the monitoring software. If these warnings are ignored, the result can be catastrophic to the company.

***References***

Anonymous. 2014. "Target's Lack of CISO Was 'Root Cause' of Systems Brach." The Wall Street Journal. September 30.

Chaudhuri, S. 2014. "Cost of Replacing Credit Cards After Target Breach Estimated at $200 Million." The Wall Street Journal. February 18.

Germano, S. Sidel, R. & D. Yadron. 2013. "Target Faces Backlash After 20-Day Security Breach." The Wall Street Journal. December 19, 2013.

Harris, Elizabeth. Perlroth, Nicole, Popper, Nathaniel and Hilary Stout. 2014. "A Sneaky Path Into Target Customers' Wallets." January 18.

Harris, E. 2014. "Target Executive Resigns After Breach." The New York Times. March 5.

Harris, E., and N. Perlroth. 2014. "Target Missed Signs of a Data Breach." The New York Times. March 13.

Harris, E. 2014. "Faltering Target Parts Ways With Chief." The New York Times. May 5.

Kosner, A. 2014. "Target Breach of 70 Million Customers Data Used Bargain Basement Malware." Forbes. January 15.

Langley, M. 2014. "Inside Target, CEO Gregg Steinhafel Struggles to Contain Giant Cybertheft." The Wall Street Journal. February 18.

Maniloff, R. 2014. "Class-Action Lawyers Hope Target Is a Bull's-Eye." The Wall Street Journal. January 2.

Perlroth, N. 2013. "Target Investigates Breach Involving Credit Card Data." The New York Times. December 18.

Perlroth, N. 2013. "Target Struck In The Cat-And-Mouse Game of Credit Theft." The New York Times. December 19.

Perlroth, N. 2013. "Who Is Selling Target's Data?" The New York Times. December 24.

Pollock, L. 2014 "Target Names New Chief Info Officer Following Data Breach." The Wall Street Journal. April 29.

Schectman, Joel. 2014. "Target Faces Nearly 70 Lawsuits Over Breach." The Wall Street Journal. January 15.

Sidel, R., Yadron, D. & S. Germano. 2013. "Target Hit By Credit-Card Breach." The Wall Street Journal. December 19.

Sidel, R. 2014. "Credit Union Group Puts Price Tag on Target Breach." The Wall Street Journal. January 22.

Stout, Hilary. 2014. "To Regain Trust, Target Must Do More, Crisis Experts Say." The New York Times. January 10.

Yadron, D. and P. Ziobro. 2014. "Before Target, They Hacked the Heating Guy." February 5.

Ziobro, P., & R. Sidel. 2014. "Target Tried Antitheft Cards." The Wall Street Journal. January 20.

Ziobro, P. 2014. "Target Breach Began With Contractor's Electronic Billing Link." The Wall Street Journal. February 6.

Ziobro, P. 2014. "Target Technology Executive Resigns." The Wall Street Journal. March 5.