Prime Factors
Responsive Data Security

How Card Issuers Can Reduce Impacts of Retail Chain Data Breaches

Executive Summary

Recent data breaches at major retailers have shaken consumers and the payments industry that serves them. The attacks applied strategies that circumvented conventional applications of encryption for protection of data privacy, intercepting payment card and other data when in use in active memory of the point-of-sale device. Data stolen will be used to counterfeit payment cards for fraudulent transactions. In the future, counterfeiting of US payment cards can be reduced by migration from the legacy magnetic stripe cards to the EMV integrated chip cards.

Introduction

The end of 2013 brought stunning revelations of data compromise at some of the most trusted retail chains in the US. Target Stores and Niemen Marcus both announced breaches, with the number of potentially affected consumers exceeding 110 million from the Target breach alone. Announcements of other retail chain data breaches followed. While it will be years before all the technical details of these breaches are shared, the initial picture is a bewildering combination of teenage hacking, organized cybercrime, and surprising lapses in data protection best practices.

Details are emerging only slowly, with media reports colored by assertions of industry pundits based on statements of unattributed sources and personal conjecture. The consensus view of the Target breach seems to be that card issuing banks identified a trend of fraudulent activity associated with payment cards that had been used in Target stores and alerted the retail chain on or about December 15, 2013. Three days later, KrebsOnSecurity website broke the story before Target notified the press or consumers. Since then, shape of the attack has formed only slowly, with much speculation, allegation, and contradiction. There have been statements that the author of the malware was a Russian teenager, then that the teenager was only a technical support 'face' for the actual author. First comments anticipated that the breach occurred in Target's authorization switching system with later analysis of public information pointing to RAM scraping malware installed on many point-of-sale card reading devices. Speculations on the technical and logistic details of the breach continue.

Target has acknowledged that data was stolen, that it was the result of malware installed at the point-of-sale and on other systems, data stolen includes names, mailing addresses, card account numbers, phone numbers, CVV/CVC data (cryptographically generated verification values encoded on the magnetic stripe of the card), and encrypted personal identification numbers (PINs). Industry experts outside the investigation believe that the original code base for the malware was purchased from an online source for as little as $2,300, and that as much as 11 GB of data was harvested between the time the attack started and the date when Target removed it from their systems.

Then, after the turn of the year, Neiman Marcus conceded that 1.1 million consumers' data was compromised in a breach earlier in 2013, while sporting goods retailer Easton-Bell announced news of a breach impacting their online customers on January 21. No details of the nature of the attacks have been provided in either of these instances. Authorities warn that at least three other retail chains may also have experienced similar data breaches in the last six months.

What Happened and What Happens Next?

Many different groups urgently want to know what happened – how did breaches happen to such respected and professional retailers? Consumers who are affected want to know what to look for in retailers to better protect themselves. Regulators want to understand if the failure is in the scope of their standards, meaning every retailer is potentially at risk, or only in the individual implementations of those chains affected. Legislators want to know in the interests of the general common good and to appeal to the concerns of their constituencies. The card brands want to know so programs can be launched to reassure the public and encourage confidence in the payment systems. Card issuers, perhaps most of all, want to know so they can better understand their financial risk in providing payment cards to their customers.

In the face of all this fervent interest, the unfortunate truth is that the scope of what happened won't fully come to light for several years, for a variety of reasons. First, diagnosis of the issue is technically challenging work that requires tedious review of computer log files, audit reports, and other documents, without certain assurance that all the data required to reach a conclusion is available. The POS attack used malware written in both English and Russian, and used a sophisticated strategy of warehousing the stolen details inside Target for later pickup. Second, the perpetrators may never be caught and, even if caught, may be detained in foreign territories that do not provide judicial transparency. Third, if the perpetrators are caught and interrogated, they may never reveal the full detail of their operation. Last and perhaps most frustrating is that the practices of civil litigation in the United States prohibit the enterprises impacted from publishing details about a breach as those details are discovered, until such time as all pending criminal and civil litigation is settled. This position is taken very seriously due to the vast liabilities in play.

A very similar example to these recent events is found in the TJX Stores data breach beginning in 2005, where approximately 94 million customer credit card records were stolen. Final estimates of the costs to the retailer in fines, class action suit settlements, and associated fees run as high as $250 million. When the operational expenses of contacting and offering assistance to impacted customers and offering credit monitoring to those who wanted it is considered, total costs were estimated in excess of $1 billion. A breach of one of the top ten transaction processors in the US, Heartland Payments Systems, in 2008, affected 130 million card accounts. While new litigation continues to emerge even today, the breach has cost Heartland an estimated $140 million in direct costs so far. In both of these instances, little information about the specific nature of the breaches was released on the advice of counsel, anticipating the inevitable law suits that would be filed. It was only after all suits were settled that at least some degree of detail became publically available.

In this circumstance, though, some outcomes are predictable (beyond the inevitable litigation). First, the stolen card details include all that is needed to clone payment cards' magnetic stripe data (including the CVV/CVC values mentioned earlier), and will be sold on to counterfeiters through online black markets. Exact copies of the electronic data on the magnetic stripes of cards used at the retailers' points-of-sale will be duplicated onto stolen payment card bodies, and then embossed with account numbers, names, and expiration dates. These operations, once requiring large and expensive embossing machines, can now be accomplished using relatively inexpensive tabletop embossers with magnetic stripe encoders fed with convincing replicas of actual card stock to create high quality "clones" of the originals. Thieves then use the cards to purchase goods that can be resold or fenced to obtain ready cash. This appears to have happened immediately after the Target data breach, as two suspects were arrested in Texas after allegedly making tens of thousands of dollars of fraudulent retail purchases using as many as 96 counterfeit cards. ATM sponsoring banks also stand to lose cash directly in the immediate aftermath of the breach as criminals have reasonable chances of guessing the PIN associated with a given card for obtaining cash advances, particularly for cards from issuers that allow customers to select their own PINs.

When counterfeit cards are produced, criminals are restricted to the riskier approach of making purchases in person – at least in the period immediately after the breached data is made available. Most merchant chain data breaches only collect the CVV/CVC values encoded on payment cards' magnetic stripes but cannot collect the CVV2/CVC2 values displayed on the back sides of the payment cards (Visa/MasterCard/Discover), as the latter are not needed for in-store transactions. The CVV2/CVC2 values – the three-digit numbers printed on the back of these payment cards, usually at the end of the signature panel – *are* required when completing "card-not-present" transactions, such as online and phone purchases. The online forms or phone agents request the CVV2/CVC2 value before completing a transaction.

However, the Target data breach, at least, exposed additional information that may allow criminals to obtain the CVV2/CVC2 values. In addition to the payment card magnetic stripe data, the hackers also obtained additional customer information including mailing address, phone numbers, and email addresses of up to 70 million Target customers. With this information, fraudsters will be able to mount "spearphishing" campaigns, contacting those impacted and using various social engineering ploys to convince them to reveal the CVV2/CVC2 values and/or PIN numbers. In these attacks, a criminal poses as someone representing Target, the card issuing bank, a law enforcement agency or some other authority, contacts one of the impacted cardholders by email or phone and convinces the victim to reveal the sensitive data. Once in hand, the thieves no longer even need go to the trouble of creating a counterfeit plastic card, as they have all that is needed to place fraudulent card-not-present transactions over the Internet or by phone without taking the risk of entering a retail location. Successful attacks of this nature go even further, to the extent of providing the criminals all the information necessary for complete identity theft.[1]

The volume of cards compromised and the sophistication of the organized criminals taking advantage of them are so great that impacts will be felt for years. Fraudsters have learned the value of patience, building schemes to hold back use of compromised cards for months, even years, before using them. Both cardholders and the card issuing banks are lulled into complacency by the inactivity, leaving even greater windows of opportunity for fraudulent transactions to go undetected.

How EMV Reduces the Consequences of a Data Breach

There are several ways data thieves can use stolen data for fraud, and different protections that can or should be put in place. In particular, if EMV transaction processing is put in place before such data breaches, the POS data stolen would be worthless for creating counterfeit payment cards. EMV (acronym for Europay, MasterCard & Visa) is a transaction processing standard for using integrated chip (IC) cards for payments. Cards of this type are used widely around the world outside of the United States and have proven to be a strong deterrent to payment card counterfeiting.

From the card issuing banks' perspective, the integrated chip on the card manages over 100 cryptographically protected controls related to authorization parameters and use (compared with only two cryptographic elements on magnetic stripe cards). Likewise, the point-of-sale devices that accept EMV-compliant payment cards support more advanced cryptographic capabilities and, using unique data held on each, the IC cards and these EMV-compliant POS terminals must mutually authenticate to each other before transaction processing can proceed.

Equally, the chip on EMV-compliant cards applies advanced cryptographic techniques to generate a unique cryptogram that is included with each transaction transmitted on-line to the card issuing bank and only transactions with a valid cryptogram are accepted and posted. Any transactions that are not accompanied by a valid cryptogram are rejected and returned as denied to the merchant. The nature of the EMV infrastructure is such that the cryptographic keys are unique to each card, and stringent controls are applied to keep those keys completely protected and private from the point of creation, to injection during personalization of the IC cards issued to customers, and to use during cryptogram generation for transaction authorization. So long as security of the cryptographic keys is maintained, there is much less value in the data criminals might steal at the point of sale; the transaction cryptogram generated is unique and valid only for that specific transaction.

By Payment Card Industry (PCI) regulation, the foundation for EMV cryptographic key protection must apply a hardware security module (HSM) – devices that provide the highest degree of tamper detection, tamper resistance, and protection for cryptographic keys. This can be an obstacle as the programmatic interfaces of HSMs are complex and require significant knowledge of both cryptographic techniques and the EMV specifications.

[1] Please see http://www.technewsdaily.com/6828-protect-yourself-from-data-breaches.html for discussion of "How to Protect Yourself from Data Breaches"

Addressing EMV Cryptographic Key Security

Securing the cryptographic keys that form card issuers' foundation for EMV-compliant processing and all the benefits it brings becomes a critical focus for such issuers. Prime Factors leads the industry in providing EMV management software integrated with Thales® PayShield® HSM in its Bank Card Security System (BCSS). BCSS greatly reduces the time, effort, and risk of integrating HSM capabilities into banks' card issuing processes, by insulating users from the complexities of the HSM application processing interface (API). Moreover, it presents a tailored user interface for EMV card issuance administrators that allows them to select the cryptographic keys and configure the many cryptographic controls required for EMV-compliant card issuance in alignment with the card brands' regulations.

For more information about BCSS and how it can reduce the cost, time, effort and risk of migrating to EMV-compliant card issuance, please contact Prime Factors at (888) 963-6458.

Copyright © 2014

Prime Factors and Bank Card Security System are trademarks of Prime Factors, Inc. Thales eSecurity and payShield are the trademarks of Thales Group.