cardconnect™

The Path to Payment Security

A Clear Approach to Preventing Data Breaches and Protecting Your Business

Cybercrime is not only increasing in frequency, it's increasing in cost. With more sophisticated hacking methods constantly being developed, the danger of storing sensitive information is rapidly increasing. Recently, the massive Target data breach has taken over headlines. With up to 110 million customers at risk and a $1.2 billion potential price tag, their brand and bottom line are in jeopardy.

Despite EMV "Chip-and-PIN" technology being heralded by the media as the answer to payment data breaches, it simply is not true. In this document, we delve into the problems EMV and PCI 3.0 leave unsolved and offer a comprehensive solution through a combination of EMV, P2PE (Point-to-Point Encryption), Tokenization, and a secure, hosted Vault. By preparing merchants for EMV technology and taking them out of PCI Compliance scope, the risk of compromised data and the cost of constantly having to monitor your system for breaches are removed.

Robert Nathan
Chief Technology Officer

Rush Taggart
Chief Security Officer

The Emergence of the Data Breach

Over 600 million records have been compromised in the United States since January 2005.[1]

In reality, the number is actually much higher because for many of the breaches included, the number of compromised records is unknown. These security breaches not only negatively impacted the reputation of the companies involved, but also cost them significant amounts of money in lawsuits and fines. A 2013 study found that the merchant cost to a data breach victim is around $200 per compromised record.[2]

In recent years as hackers have become more sophisticated, these attacks have increased in frequency and effectiveness. In 2011, Sony's Playstation Network had to be shut down due to a major data breach, resulting in a class-action lawsuit and costs that have been estimated at up to $24 billion.[3]

Most recently, Target has been in the spotlight for their massive data breach. Target CEO Gregg Steinhafel confirmed to CNBC[4] that the breach was caused by malware installed on Point-of-Sale ("POS") systems. Between lawsuits, government fines, and reimbursements to customers, Goldman Sachs estimates total costs incurred by Target could be $1.2 billion.[5]

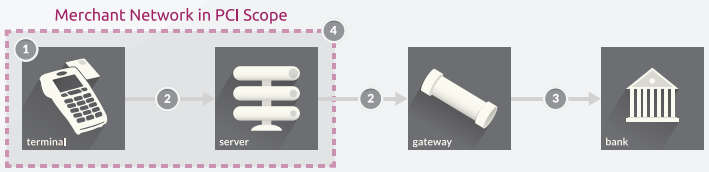
What should worry merchants most is the only thing unusual about the Target hack was its size—Target was one of over 600 security breaches in 2013 alone.[6]

Because Target likely invests heavily in security, this breach confirms vulnerabilities exist in current systems. As Stan Lippelman, VP of Marketing at Bass Pro Shops, puts it, "We feel very comfortable…But, the fact that it happens to Target means it can happen to anybody, right?"[7]

Where Your Payments Are at Risk

There are underlying vulnerabilities in the payment process for any given business or company due to the exchange of data between systems, the sensitive nature of that data, and the requirements and standards set forth by the Payment Card Industry ("PCI") Security Standards Council, which serves as the governing body of the payment processing industry.

Four Main Vulnerabilities



1. **Point-of-Sale/Terminal –** In many recent breaches, credit and debit cards were compromised by malware installed on POS systems. With Point-to-Point-Encryption ("P2PE") technology, these malware attacks would be prevented. P2PE hardware is designed to stop functioning if any foreign code or application is installed on the device.

2. **Terminal to Gateway Transmission –** As card data is transmitted from the terminal to the gateway, there can be points when data is left unencrypted, for example when card data leaves the merchant network. While the movement to EMV Cards will mask this data within computer chips, the only way for a business to protect itself from this vulnerability is to encrypt data at the Point-of-Interaction ("POI"), or in this case, the point at which the card is swiped.

3. **Gateway to Bank Transmission –** PCI Standards require payment gateways to only transmit data to a select list of IP addresses of certified processors. Payment gateways should halt data transmission to any foreign IP addresses outside of this small, select list. At this point of the payment process, data is leaving the merchant's system and carries inherent vulnerability since data must be unencrypted before reaching the bank or processor.

4. **Strict Network Monitoring/Vulnerability Management Program –** PCI DSS requires merchants to regularly track and monitor all access to network resources and cardholder data and regularly test security systems and processes. Without proper follow-through, especially for merchants with small IT departments, this presents a huge burden and vulnerability for a data breach.

Preventing Breach & Fraud

EMV is Not the Answer

Major breaches in the retail industry have produced one rallying cry that has become ubiquitous in the news media: EMV (also known as Chip-and-PIN) could have prevented this type of breach. Unfortunately, that is not entirely accurate.

Sure, there is no doubt that magnetic stripe credit cards are antiquated technology, as they are extremely simple and inexpensive to replicate. EMV is advantageous as it makes card replication harder and more costly, which is definitely a direct benefit to the cardholder.

What EMV does not address is protecting card data when it is in route to the processor, post-authorization storage of card data by the merchant and card-not-present fraud (such as sales via e-commerce, phone and mail).

The Problem with PCI DSS

On January 1st, 2014, PCI DSS 3.0 went into effect. As the PCI Security Standards Council put it themselves, the updates were based on "feedback from the industry" and "market needs." In essence, PCI DSS is reactionary, not anticipatory. One of the fastest growing methods of payment acceptance – mobile – was hardly addressed.

This is understandable. PCI DSS 2.0 was already seen as complex and merchants collectively spent billions to simply be compliant. While 3.0 includes some necessary changes that will heighten the overall security of our national infrastructure for accepting payments, it is predominantly believed that the victims of recent data breaches would still have suffered the same fate had they been compliant with the 3.0 updates.

The Answer is P2PE

If EMV doesn't protect card data and PCI Compliance doesn't guarantee safety from attacks, how should merchants protect themselves? One technology that could have potentially prevented the damage incurred by recent breaches is P2PE. As soon as a credit card is swiped, the data is encrypted and remains encrypted throughout the merchant's environment. If a breach were ever to occur on a merchant's network, the data the thieves stole would be encrypted, rendering it useless. Also, P2PE protects from malware being placed on the POS system. If any foreign application were to be placed on the device, it would stop working immediately.

P2PE is seen as such a secure approach that using a PCI-certified P2PE solution will completely remove you from PCI Compliance scope – even taking away the PCI DSS Self-Assessment Questionnaire ("SAQ"). The difficulty for merchants is determining if a vendor's P2PE claims are valid. Proper due diligence for implementing P2PE technology should include evidence of a proven track record in payment security, a discussion on where the vendor is at in the PCI-certification process, and a fully comprehensive roadmap for implementing a P2PE solution.

The Ideal Solution

With the negative repercussions of security breaches and the myriad vulnerabilities in the payment process, the path to payment security can seem daunting. Thankfully, CardConnect has introduced the ideal solution.

CardConnect's Payment Security Solution consists of P2PE hardware that is EMV-ready, our secure payment gateway that utilizes CardSecure™ encryption and tokenization, and a hosted vault that is designed to solely communicate with validated processors.

P2PE

CardConnect's Payment Security Solution utilizes a P2PE terminal, co-developed with Ingenico, which safeguards a merchant's customer data from the POI to the point at which it is sent to the processor. By removing sensitive data in this fashion from a merchant's system, CardConnect allows the merchant to remove itself from PCI Compliance scope.

EMV-Ready

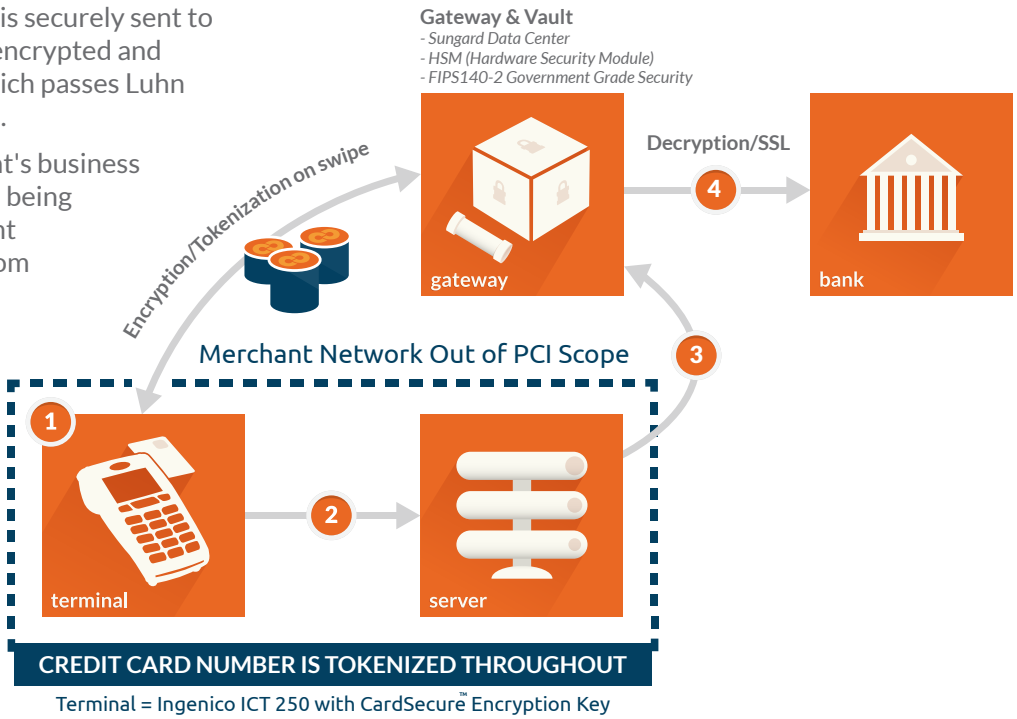
CardConnect's P2PE terminal is EMV-ready, ensuring merchants meet the EMV transition deadline. The card issuers have unanimously identified October 2015 as the date that all merchants must use EMV-compliant terminals. If a merchant fails to adhere to this requirement, the card issuers will transfer the liability of any security breach to the merchant.

Removal from PCI Compliance Scope

CardConnect's Payment Security Solution completely removes the merchant from PCI Compliance scope. This means no PCI audits, no vulnerability tests, and no SAQs.

CardConnect's Payment Security Solution

1. Upon card being swiped, card data is securely sent to the CardConnectVault where it is encrypted and tokenized. An intelligent token (which passes Luhn Test) is transmitted to the Terminal.
2. The token is passed to the merchant's business system. Since no actual card data is being transmitted or stored, the Merchant Network is completely removed from PCI Compliance scope.
3. The token is transmitted via the CardConnect Gateway to the secure, hosted Vault.
4. The card information is securely decrypted and transmitted via Secure Sockets Layer (SSL).



A History of Protecting Payments

CardConnect has a proven track record in developing security technology for the payments industry.

- ***1997:*** *CardConnect builds first payment gateway integrated to SAP for Fortune 500 corporations.*
- ***2004:*** *CardConnect builds CardSecure™, a payment card encryption solution for SAP.*
- ***2006:*** *CardConnect's payment gateway validated as PABP Compliant under Visa'a Payment Application Best Practices program.*
- ***2009:*** *CardConnect's payment gateway validated as PA-DSS Compliant and listed on the PCI Security Standards Council website.*
- ***2010:*** *CardConnect's payment gateway validated as PCI-DSS Compliant and listed on Visa Service Provider Registry.*
- ***2012:*** *CardConnect's PANPAD, a terminal that encrypts card data at the point of entry, named winner of Security Products Guide's Global Excellent Award.*
- ***2012:*** *CardConnect's payment gateway with CardSecure™ becomes the first Oracle Validated Integration for payment acceptance and security.*
- ***2013:*** *CardConnect develops proprietary P2PE solution in response to security risks for point-of-sale transactions.*
- ***2013:*** *CardConnect receives United States patent for token-based payment processing*

As referenced earlier, proper due diligence for implementing P2PE technology should include evidence of a proven track record in payment security, a discussion on where the vendor is at in the PCI-certification process, and a fully comprehensive roadmap for implementing a P2PE solution.

CardConnect is an innovative payments technology company that designs solutions to safely transmit credit card data. More than 50,000 businesses–including GE, Adobe and the New York Times–use our payment technology and processing services that make accepting payments as simple, easy and secure as possible.

Trusted By

[1] Privacy Rights Clearinghouse (as of January 2014) - http://www.privacyrights.org/data-breach

[2] Ponemon 2013 Cost of Data Breach Study: Global Analysis - https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[3] PlayStation Network Breach Could Cost Sony $24 Billion -http://www.businessinsider.com/playstation-network-breach-could-cost-sony-24-billion-2011-4

[4] CNBC Interview with Target CEO http://www.cnbc.com/id/101330060

[5] Goldman Sachs estimate on Target breachhttp://money.cnn.com/2014/01/13/investing/target-stock/

[6] 2013 Data Breach Investigations Report - http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[7] Stan Lippelman on Target Breach - CNBC http://www.cnbc.com/id/101330258