First Data™

A First Data White Paper

May 2010

Where Security Fits in the Payments Processing Chain

With over 20 billion credit card purchase transactions in the US in 2009 and a highly complex system for processing those transactions, it's not surprising that credit card information is a key target for thieves. Thieves have become adept at exploiting numerous vulnerabilities in the consumer-merchant-acquirer payment processing chain to gain access to this information. Fortunately, there are cost-effective solutions that are available to help secure sensitive data and reduce compliance costs.

By:
First Data Thought Leadership
and
Rob McMillon, Director of Solution Development – RSA, The Security Division of EMC

Executive Overview

The credit card industry has been very successful in its efforts to convince consumers to use credit cards as their primary form of payment. In the United States alone, there are 176.8 million consumers who collectively hold 609.8 million credit cards. The average number of cards per cardholder was 3.5, as of year-end 2008. In 2009, there were 20.2 billion credit card purchase transactions in the United States worth $1.76 trillion.[1] In the face of these staggering numbers, it's easy to see why thieves are drawn to the credit card industry.

Unfortunately, thieves also have been successful at stealing payment data and turning it into profit—and our collective loss. In 2008, the Verizon Business RISK Team investigated data breaches in all industries in which 285 million total records were breached. Fully 80 percent of those records comprised payment card information, and a significant number of those records were used fraudulently.[2]

What makes this sensitive data vulnerable? Card data for a purchase transaction must flow through a payments processing chain in order to be processed. This processing chain, which includes consumers, merchants, acquirers/processors, card brands and issuing banks, links many technologies including communication lines, databases and sophisticated applications. Data thieves have become quite sophisticated in their knowledge of how these technologies work, enabling them to exploit points of vulnerability in the payments processing chain.

The payment card industry (PCI) is fighting back. One starting point is the PCI Data Security Standard (PCI DSS), which provides guidelines to merchants about how to secure cardholder data. While PCI DSS has helped, it isn't enough; hundreds of millions of data records have still been breached in recent years.

Consumers, as well as companies in the processing chain, have a responsibility to reduce the risk of lost, stolen or otherwise exposed sensitive cardholder data. This paper looks at where security fits in the processing chain, especially the most vulnerable points where enhanced security would benefit the entire ecosystem. We discuss several cost-effective technology-based solutions that are readily available today to help organizations to secure sensitive data and improve their PCI DSS compliance posture.

Key Takeaways

As you read this paper, we hope that you take away and consider several key points in the context of your own business processes:

- → Payment security is complex. Many vulnerabilities exist in the payments processing chain, especially in the interactions between consumers, merchants and acquirers. The sheer volume of consumers and merchants provides a large window of opportunity for thieves to capture data that can be fraudulently turned into profit.
- → None of the technologies that exist today solves all the security problems in the payments processing chain. However, a select few technologies focus on solving the biggest problems and greatest vulnerabilities that affect most merchants, and they can do so in a cost-effective manner. Merchants can use these solutions to reduce their overall level of vulnerability.
- → New security methods are now available to secure sensitive cardholder data from compromise as close to the initiation of the transaction as possible. In addition, these technologies can help reduce a merchant's PCI compliance burden.

  End-to-end data encryption protects sensitive data from the point of capture through the handoff to the payment processor. Protecting the data in motion foils many of the high-profile attacks of recent years, and encryption is a proven technology that can be deployed effectively by any size of merchant.

  Tokenization is a process whereby sensitive data is replaced by a randomly generated string of characters that can be linked back to the original data only by an authorized party. By storing and using tokenized data instead of real cardholder data in back-end applications, merchants remove sensitive data from their environments, thus reducing the risks associated with a data breach as well as the scope of their PCI audits.

Background: Security in the Payments Processing Chain

The payments processing chain has many players: consumers, merchants, acquirers, card brands, issuing banks and sometimes other companies in between. As cardholder data flows from one entity to another and is aggregated at various collection points, it may be vulnerable to exposure, loss and theft. There are criminals who target the most vulnerable links in this chain, and so the payments industry is trying to reduce the vulnerabilities at every point. This requires diverse, layered solutions to seal the gaps where thieves are gaining access to sensitive data that they can potentially monetize.

The Flow of a Transaction Through the Payments Processing Chain

It's amazing to think of the complex set of processes that take place when a consumer swipes his credit card and is approved for his purchase in less than a few seconds. The average consumer doesn't think about where his card data (the primary account number, or PAN) goes or how many organizations in the processing chain must work with it in order to authorize or decline the credit transaction he wants to make. The chart on the next page provides a simplified view of the process.

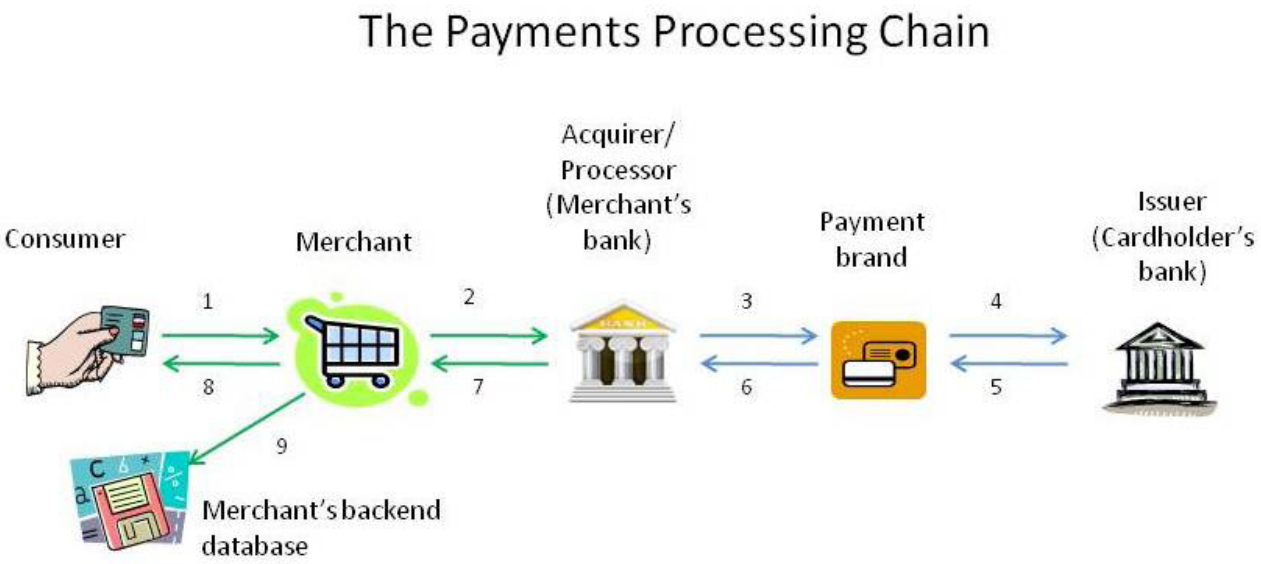


Figure 1 – Simplified payment transaction flow

In reality, this process is quite complex and may involve more organizations than those pictured here, but for the purposes of this paper, we can summarize the process in a few basic steps:

1.	A consumer wants to buy goods or services and pay for it using his credit card. The cardholder data is entered into the merchant's payment system, which could be a point-of-sale (POS) terminal/software or an e-commerce Web site.
2.	The card data (PAN) is sent to an acquirer/payment processor, whose job it is to route the data through the interchange system for processing.
3.	The acquirer/processor sends the data to the payment brand (e.g., Visa, MasterCard, American Express, etc.), who forwards it to the issuing bank.
4.	The issuing bank verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5.	If so, the issuer generates an authorization number and routes this number back to the card brand. The issuing bank agrees to fund the purchase on the consumer's behalf.
6.	The card brand forwards the authorization code and the PAN back to the acquirer/processor.
7.	The acquirer/processor sends the authorization code and either the PAN or a viable substitute number for the PAN (i.e., a token) back to the merchant.
8.	The merchant concludes the sale with the customer.
9.	The merchant may retain the transaction data long term for the processing of returns, retrieval requests or chargebacks, as well as for business intelligence reasons such as analysis of consumer buying behavior and creation of marketing programs.

The States of Data and Their Risks

Throughout the payments processing chain, sensitive data is at risk when it is in each of its three states: at rest, in transit and in use. A few simple examples illustrate what we mean by these states.

- → **At rest – Cardholder data is "at rest" when it is being stored or aggregated in a database or other storage device. For example, a merchant holds onto the PAN until he closes out his batch at the end of the day. Once the batch is completed, the data is cleared from storage. Another example of at-rest data is when a merchant stores card numbers in a data warehouse for post-sale auxiliary purposes such as returns, chargebacks, customer loyalty programs and other marketing activities. No matter where it resides, any data at an aggregation point is vulnerable to thieves. What's more, any card data stored anywhere in the organization's network puts that part of the network in scope for a PCI audit, regardless of whether or not the data is encrypted.**
- → **In transit – Cardholder data is "in transit" when it is moving across any communications channel as it passes from one entity (such as a merchant) to another (such as an acquirer). Examples of common communication channels include a store's local area network; a wireless connection from a POS terminal to a store server; the open Internet; and a private data line. When data is traveling along any of these or other types of communication paths, it's possible for thieves to "sniff" the data and divert a copy of it to an illicit destination.**
- → **In use – Cardholder data is "in use" when it is in a clearly readable state, being used by a part of the transaction process. For example, the acquirer's computer is reading the card data to determine which card brand to submit it to for processing, or the card brand's computer is reading the data to determine which bank issued the card. Thieves have been known to hack into the memory of computers that are actively processing card data in order to steal the clearly readable data.**

In each of these scenarios, a thief might be able to get information.

Why Security Must Be Improved From Consumer to Merchant to Acquirer

This paper looks at the security issues and technology solutions for the part of the processing chain between the consumer and the acquirer. There are several reasons why we chose to focus on these entities. First, this is where the greatest vulnerabilities exist and where the need for better security is most important. There are hundreds of millions of consumers and millions of merchants, and each one represents an opportunity to a thief. By comparison, there are fewer than 10 organizations in the United States that fulfill the role of acquirer/processor; only a handful of card brands; and a similarly small number of issuers. All of these organizations understand the extreme value and significance of the card data that they process and hold, and so they have built strong security measures to protect it. However, the breach of Heartland Payment Systems shows that even those systems could be vulnerable. Although thieves view the massive amounts of data within these organizations as key targets, they more often take the path of least resistance to get data. This path takes them back to the consumer-to-merchant-to-acquirer/processor segment of the transaction flow.

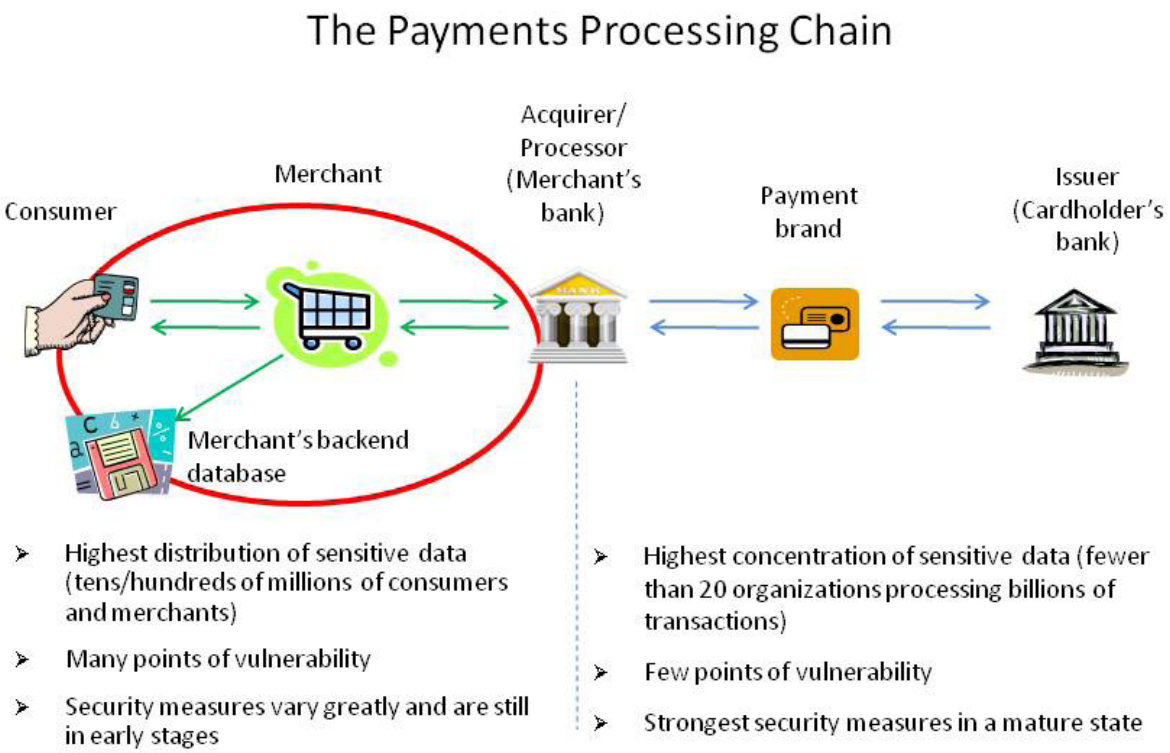


Figure 2 – The most vulnerable segments of the transaction flow

Many consumers and merchants are vulnerable

Millions of merchants in the United States accept electronic payments either in person, over the phone or over the Web, and more than 175 million Americans collectively use over 600 million credit cards to purchase goods and services. In fact, there were more than 20 billion credit card purchase transactions just in 2009. That volume more than doubles when we add in debit and prepaid cards, whose 2009 U.S. activity totaled 36.2 billion transactions worth $1.63 trillion.[3] That's a lot of financial activity, and it certainly has captured the interest of thieves who covet card data.

The underground business of buying, selling and using stolen card data is large—bigger than some national economies. Last year, thefts from stolen credit card and bank accounts had the potential to add up to $8 billion, according to data from Symantec, maker of the Norton antivirus software.

However, actual losses were lower because not every breached record results in fraudulent use. The fewer records exposed or stolen in a breach, the more likely those records are to be used for illegitimate purposes. When a thief gets a hundred or thousand cards at a time, it is comparable to a "local criminal" who steals the cards and then uses them for personal gain. In these cases, the gap between the theft and the use of the stolen card is short. In the more sensational breaches yielding tens of thousands or millions of cards, the crimes are perpetrated by organized and often widespread groups that profit through the resale of the cards on the black market rather than their direct use. In those cases, selling millions of card numbers in batches of thousands frequently takes so long that the breach is discovered and the compromised cards are deactivated before all of the cards can be used. It's this paradox of scope that make a breach so serious for small merchants; if a thief steals 100 card records from a small business, chances are very high that all 100 cards are likely to be used fraudulently and rather quickly.

But discovery of a breach doesn't mean the fraud can be stopped quickly. One hundred thirty million records were stolen in the Heartland breach, which was discovered in January 2009. And although the issuing banks have had more than a year to close the compromised accounts, there are still cards being used in a fraudulent manner today.

A merchant's primary job: selling takes precedence over security

PCI DSS provides guidelines to merchants on how to implement security measures to protect sensitive cardholder data. Still, the guidelines are a security baseline representing the minimum, not a comprehensive roadmap, therefore leaving to merchants the complex task of determining exactly what techniques and technologies to deploy to protect their own businesses. This approach results in merchants solving for securing card data in almost as many ways as there are merchants.

This comes as little surprise. Data security, after all, is not the primary job for merchants; their job is to sell goods and services. Even the largest merchants in the world are focused on the core business of selling merchandise, so this is where their resources are focused. Accepting electronic payments at checkout is a sales enabler, but payment security is not usually the highest priority or area of expertise for retailers.

Merchants are under pressure

Until PCI DSS forced their hand, many merchants didn't think much about cardholder data security. However, in recent years they have faced the daunting task of segmenting networks, upgrading POS hardware and software, implementing fraud detection techniques in their online checkout procedures and more. Merchants have to verify, through costly audits and attestations, that they've installed sufficient controls to meet the requirements of PCI DSS.

Members of the National Retail Federation have collectively spent more than $1 billion so far on PCI compliance as part of their security programs, and they sometimes question the value of this investment.[4] Merchants can be PCI compliant and still not have fully secure cardholder data environments. Some of the more noteworthy data breaches have happened to companies that had passed their PCI audits.

PCI is not the only pressure point for merchants. Many states have enacted legislation that requires consumer notification of personal data breaches. The costs of notifications, remediation, consumer credit monitoring, legal defense and other aspects of a breach continue to rise. A Ponemon Institute study assessed the cost of a data breach at $204 per compromised customer record in 2009, up from $202 in 2008.[5] Even a small breach involving only a few hundred records can be costly, especially for small merchants.

Liability is shifting to consumers and merchants

More of the liability of a data breach is shifting to consumers and merchants. There is an effort by the card brands to bring new technology to the United States within the next five years. EMV (Europay MasterCard Visa) specification provides technology that helps detect the fraudulent use of electronic payment cards when they are physically presented for use. If an EMV-enabled card is used in a fraudulent transaction, the onus of proof is on the consumer to show that it wasn't him who used the card. This could make consumers rather than banks and card companies liable for fraudulent purchases the consumers didn't make.

Merchants, too, could assume more financial responsibility for losses stemming from card fraud. This dollar figure is on top of the cost to implement new POS hardware to support EMV, which can cost up to $500 for each new POS terminal.

Major Vulnerability Points in the Consumer-Merchant-Acquirer Part of the Payments Processing Chain

Let's take a look at the most significant points of vulnerability to understand how thieves may capture cardholder data. Then we can begin to apply solutions that eliminate or reduce these vulnerabilities.

Vulnerabilities of Data in Transit

To make its way through the payments processing chain, cardholder data must be sent from one entity to another along some type of communications path. With a little bit of technical savvy, thieves can siphon off the PAN, track data and card expiration date and route a copy to their own storage medium.

From consumer to merchant

Whether a consumer swipes a card at a POS terminal or enters data in an online shopping form, the risk is that the data "in the clear" could be intercepted before it reaches the merchant's server over an internal network. This is the technique that was used in the TJX Companies breach in which 45.7 million credit and debit card records were compromised. A contributing factor in the breach was outdated and weak wireless security. Thieves were able to intercept the clear text card data as it was transmitted in-store between hand-held price-checking devices, cash registers and the store's computers.

Between merchant and acquirer/processor

Once the merchant collects a consumer's cardholder data, the next step is to send that data to the acquirer for processing. Again, the risk is interception of the data as it travels along a communications network. Across the retail industry, approaches to data transmission vary. Sometimes it is sent in the clear over private lines because it's assumed that private lines are secure. Occasionally the data is transmitted in the clear over public lines—a risky behavior. Some merchants encrypt the data before transmitting it to the acquirer, but then compromise the process by not properly managing the encryption/decryption keys. It's possible for a thief to steal a merchant's symmetric encryption key (i.e., one that also decrypts the data), which effectively unlocks all the encrypted card data, making it completely accessible to the thief.

In the case of the Hannaford Bros. grocery chain data breach, thieves are accused of having installed malware on store servers that allowed payment card data and the cards' expiration dates to be intercepted as the data was transmitted from the stores' servers to the acquirer for processing. More than 4.2 million credit and debit cards were compromised in this breach.

Vulnerabilities of Data at Rest

Requirement 3 of the PCI DSS explicitly states that merchants must protect stored cardholder data, yet this continues to be one of the most challenging compliance requirements. One of the top reasons merchants fail PCI audits—and a leading factor in data theft—is the failure to adequately protect stored data. VeriSign Global Security Consulting Services, a division of security services vendor VeriSign, has conducted hundreds of PCI assessments in recent years. Seventy-nine percent of the merchant companies assessed by VeriSign were cited for the failure to protect stored data—and thus failed their assessments.[6]

At a minimum, PCI DSS requires the PAN to be rendered unreadable anywhere it is stored, including portable digital media, backup media and computer logs. Better yet, the PCI Security Standards Council notes: "Requirement 3 only applies if cardholder data is stored. Merchants who do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves."[7]

Despite the risks, many merchants see the benefits of storing cardholder data and therefore they do maintain the data for business purposes. The leading reason why they have trouble protecting this sensitive data at rest is that they don't know all the places where the data resides. For starters, it may be on a POS server or store server, at least until the end of day when the transaction batch is closed out. Some merchants hold onto the data longer in case of chargebacks or returns. Large multi-store merchants may use card data in back-office applications, such as financial analysis, marketing and customer loyalty programs. And once the data is stored, instances of that data may proliferate. For example, employees may take data from a central database to desktop spreadsheets or printed reports in order to perform their jobs—jobs that have nothing to do with processing the original transaction.

PCI DSS accounts for this data proliferation by requiring that every place where cardholder data sits at rest be included in the annual PCI audit to validate that it is being secured properly. Collectively, these places are all part of the cardholder data environment (CDE). The broader the scope of the CDE, the more vulnerable the data becomes. What's more, the scope and the cost of the PCI audit grow with the CDE.

Technology Solutions to Address the Areas of Greatest Vulnerability and Greatest Need

Some of the current technologies in use by the payments processing chain today can put cardholder data at risk of compromise. For example, there's no question that cardholder data must be transmitted via some sort of communication line from the merchant to the acquirer in order to process the transaction. The merchant chooses his preferred technology for communication, and his level of risk is determined by his choice. A private data line such as a frame relay is certainly more secure than a plain vanilla connection, but typically only large merchants choose private lines. Since cost is a large factor in choosing technology, most smaller merchants choose public lines. Risk is a trade-off for cost.

A logical solution to this dilemma is to use other or additional technology that is effective at keeping the data secure, but at a reasonable cost for all. Leaders in the payments industry are attacking the problem where the most vulnerabilities are and where technology solutions can do the most good for the lowest cost. We are mindful that, while security is a necessary thing, it doesn't significantly add to a merchant's ability to sell more goods and services. Without good security, however, a merchant's ability to sell can certainly be affected. For instance, 43 percent of consumers who have been victimized by fraud avoid certain merchants where they believe their data could be compromised again.[8]

End-to-End Encryption

Encryption refers to algorithmic schemes that encode plain text such as the PAN into a non-readable form called ciphertext, thus providing privacy for the encrypted data. One or more keys is required to decrypt the data and return it to its original plain text format. The key, which thieves would not possess, is the trigger mechanism to the algorithm.

Perhaps the most important measure that merchants can take to protect cardholder data is to encrypt it at the time when the consumer presents it—either when the card is swiped at a terminal or entered into an e-commerce application—and allow the data to remain encrypted regardless of the network path until it is received by the acquirer/processor, where it is decrypted and sent to the issuing bank for authorization. This is referred to as end-to-end encryption, or E2EE. Through this process, the transaction data is never transmitted in plain text in the frame relay, dial-up or Internet connection, where it could be intercepted by thieves. If the data is siphoned off by a thief once it is encrypted, it is virtually useless.

However, not all encryption methods are equal. There are several varying types of encryption:

- → **Symmetric encryption uses one key (mathematical algorithm) to both encrypt and decrypt the data. It is similar to a door lock in which the same key is used to lock and unlock the door. Thus, whoever has the key has the power to access the original data. This means that additional security measures have to be built into the business processes to protect the key. For example, in the case of a multi-store merchant, the company might use one key per store. Then if a key is compromised, only one store and not the entire chain is affected.**
- → **Asymmetric encryption, also called public key encryption, uses one key to encrypt the data and another completely different key to decrypt it. There's no worry about securing the public key used to encrypt data, and so it can be freely distributed to all merchant locations because this key can't unlock the data. In the case of payments processing, merchants would have the public key to encrypt cardholder data, and the acquirer would hold the private key to decrypt it. It is this private key that must be secured.**

Where encryption fits in the payments processing chain

As described above, end-to-end encryption starts at the moment of cardholder data capture and remains in place until the acquirer has the data. This system reduces the possibility that a thief can obtain usable data if he is sniffing any part of the network that carries sensitive data. If data is not encrypted at the point of capture, it is vulnerable as it is transmitted in plain text to the POS server or the merchant's central server. (This is what is believed to have happened in data breaches involving Hannaford Bros., TJX and the Dave & Buster's restaurant chain.)

In situations where a card is presented in person, encryption can take place within the POS terminal application, at the time or immediately after the magnetic-stripe reader (MSR) obtains the card data track. While numerous Level 1 merchants have already enabled this capability, most other merchants have not, largely due to the cost of installing a card reader with the encryption capabilities.

Encryption can safeguard data in a card-not-present (CNP) scenario as well as when a card is swiped. The data can be encrypted as soon as it is entered into the sales application and prior to being submitted for approval of the transaction. This can be further enhanced by leveraging third-party hosted payment pages, eliminating the need for the CNP merchant to touch the card data at all.

To secure data at rest, some merchants choose to encrypt the cardholder data they have in back-end databases. Although this data is no longer needed for the original purchase transaction process, it is sometimes used for auxiliary uses such as reporting and data analysis. While encryption certainly helps to protect the data, it does nothing to reduce the scope of the cardholder data environment that must be audited for PCI DSS compliance. Regardless of encryption status, it is still cardholder data and it must be reviewed for compliance with the industry regulation. Thus security is improved but at an increased cost and effort.

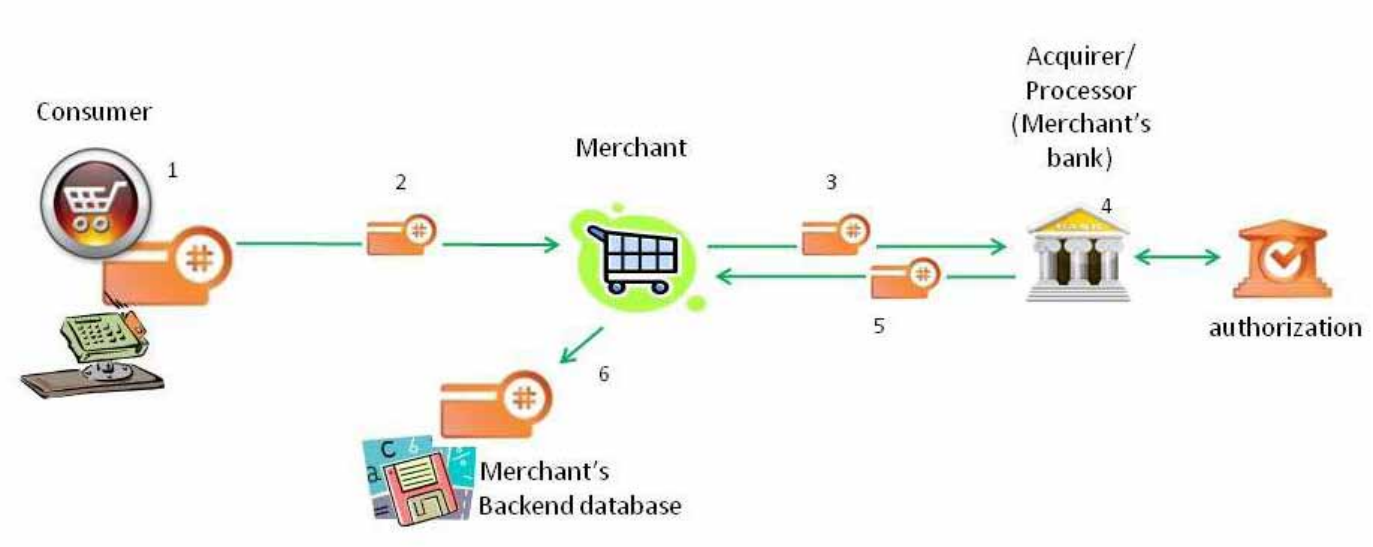


Figure 3 – Where encryption fits in the payments process

1.	When the cardholder data (the PAN) is captured at the POS (with a physical swipe or data entry), the data is encrypted.
2.	The data is encrypted as it traverses any in-store network.
3.	The merchant sends the encrypted PAN to the acquirer/processor.
4.	The payment processor decrypts the data and sends it via a secure channel to the appropriate network or association for authorization. When the transaction is authorized for payment, it gets sent back to the payment processor.
5.	After authorization, the acquirer/processor returns the encrypted PAN along with the transaction response to the merchant.
6.	The merchant may retain the encrypted transaction data long term for the processing of returns, retrieval requests or chargebacks, as well as for business intelligence reasons such as analysis of consumer buying behavior and creation of marketing programs

The problems that data encryption solves

Data encryption solutions solve for the problem of live (clear text) data in transmission as it moves upstream to the acquirer by encrypting the data as close to the point of capture as makes sense for a particular merchant. It also can solve for the problem of having clear text cardholder data in electronic storage environments when the data is kept for auxiliary use. These are two of the greatest vulnerabilities for most merchants, and by applying data encryption technology, merchants can reduce their risk of liability stemming from a data breach. If a breach does occur and a thief obtains encrypted data, he can't use it without also obtaining the decrypting key.

End-to-end encryption is not currently a requirement in PCI DSS. However, according to George Peabody, principal analyst with the Mercator Advisory Group, "end-to-end encryption may well be the end game recommendation of PCI and, if data breaches continue to plague the payments industry and occupy headlines, that recommendation may become a mandate within two years."[9]

Tokenization

An increasingly popular approach for the protection of sensitive data is the use of a token (or alias) as a substitute for a real credit card number. In the process of tokenization, actual cardholder data is used in a payment transaction and, once the transaction is authorized, this very sensitive data is sent to a centralized and highly secure server called a "vault," where it is stored securely. At the same time, a random unique number is generated and returned to the merchant's systems for use in place of the cardholder data. The vault manager maintains the reference database that allows the token to be exchanged for the real cardholder data if it is needed again for, say, a chargeback. Meanwhile the token, which cannot be monetized, can be used in various auxiliary business applications as a reliable substitute for the real card data.

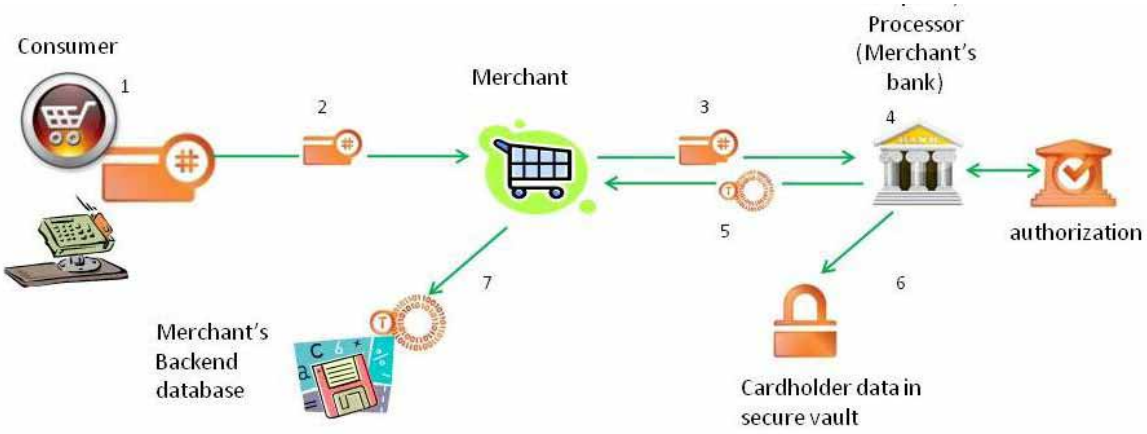
To anyone or any process that doesn't have authorization to access the vault, the token value is totally meaningless; it's just random characters. In the payments processing chain, the acquirer/processor is the most likely entity to manage the vault. Encryption tools and secure key management complement this approach by protecting the original data value within the vault.

Tokens can be uniquely tied to a single transaction or uniquely assigned to a single payment card regardless of how often that card is used. Which method is better depends on a merchant's needs. If the token is unique to the transaction, then a merchant cannot track when a specific consumer has used the merchant's services multiple times. This method hinders back-end use of the data for purposes such as marketing and customer loyalty programs. Small merchants may not have a need for such applications. Larger merchants, on the other hand, would benefit from a token methodology that uses a consistent token value for a single payment card. This approach enables the tracking of a consumer as he shops multiple times with the merchant, at a single store or across many locations.

Where tokenization fits in the processing chain

Any tokenization solution fits best at the end of the transaction authorization process. Once a transaction is authorized by the issuing bank and an authorization code is sent to the acquirer, there is no need to send the actual PAN back to the merchant. At this point, the acquirer can substitute a token to return with the authorization code. When the merchant receives the tokenized data, he can store it indefinitely and use it in multiple business applications without fear of compromising sensitive data. This scenario works just as well for CNP transactions as for card-present transactions.

Because the data that comprises a token is random, the token can have the same 16-character format as a credit card. Therefore, it can be used in back-end databases and business applications without modifying those systems in any way.



1.	When the cardholder data (the PAN) is captured at the POS (with a physical swipe or data entry), the data is encrypted.
2.	The data is encrypted as it traverses any in-store network.
3.	The merchant sends the encrypted PAN to the acquirer/processor.
4.	The payment processor decrypts the data and sends it via a secure channel to the appropriate network or association for authorization. When the transaction is authorized for payment, it gets sent back to the payment processor.
5.	After authorization, the acquirer/processor returns the encrypted PAN along with the transaction response to the merchant.
6.	The merchant may retain the encrypted transaction data long term for the processing of returns, retrieval requests or chargebacks, as well as for business intelligence reasons such as analysis of consumer buying behavior and creation of marketing programs.

The problems that tokenization solves

Tokenization solves the problem of having live cardholder data in storage or in use in business applications after the transaction approval. This process eliminates the possibility of having real card data stolen at this point because it doesn't even exist here. And unlike encrypted data, the use of tokenized data reduces the scope of PCI audits, again because there is no cardholder data that must be secured. Merchants can save significant time and money by reducing the scope of their PCI audits.

Conclusions

Payment security is complex, with risks and vulnerabilities at every point of the processing chain. Unfortunately, there is no single approach to security that can totally prevent or eliminate card data theft and fraud. As criminals become more inventive in their methods of thievery, the risks and vulnerabilities for data increase, and security methods must evolve as well.

Everyone in the payment chain—consumers, merchants, gateways, acquirers/processors, card companies and issuing banks—has a responsibility to become educated about the vulnerabilities and to take ownership of the aspects of security within their domain. This responsibility is especially important as each entity also assumes more liability for security breaches. All of these organizations can benefit from a combined approach of end-to-end encryption and tokenization—technologies that solve for some of the biggest security problems affecting the greatest numbers of consumers and merchants in the most cost-effective and timely manner.

Recommended Reading

For more information on this topic, we recommend reading:

First Data white paper: "Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance"

RSA's Speaking of Security Blog: "What is Tokenization and how does it work?"

RSA's Speaking of Security Blog: "Business Impacts of Tokenization"

"PCI Data Storage Do's and Don'ts," published by the PCI Security Standards Council

Sources

[1]Federal Reserve Bank of Boston, "The Survey of Consumer Payment Choice," January 2010 and Nilson Report, February 2010, http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php

[2]Verizon Business RISK Team, "2009 Data Breach Investigations Report," April 2009

[3]Nilson Report, February 2010, http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php

[4]Letter to Bob Russo of the PCI Security Standards Council from the National Retail Federation, et. al., June 9, 2009

[5]Ponemon Institute and PGP Corporation, "U.S. Cost of a Data Breach Study," January 2010

[6]VeriSign Global Security Consulting Services, "Lessons Learned: Top Reasons for PCI Audit Failure and How To Avoid Them, 2007," p. 4

[7]PCI Security Standards Council, "PCI Data Storage Do's and Don'ts," 2008

[8]Javelin Strategy & Research, "End-to-End Encryption, Tokenization, and EMV in the U.S.: Vendor Analysis of Emerging Technologies and Best Hybrid Solutions," January 2010, p. 14

[9]Mercator Advisory Group, Inc., "Merchant Security, Tokenization and the Fairy Tale of Outsourcing PCI," George Peabody, March 2009, p. 4

First Data™

The Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.

For more information, contact your
First Data Sales Representative
or visit firstdata.com.