nisum®

consulting ≡ digital ||| innovation

WHITE PAPER

Tokenization: Beyond PCI Measures for Credit Card Fraud Prevention

WHITE PAPER SERIES FOR DEVELOPING ENTERPRISE-GRADE APPLICATIONS

Publication Number: WP015

Table of Contents

Introduction

This white paper presents various important techniques for the prevention of data security breach, particularly that involving credit card data. In this document, we will discuss the imperative of data security, and explain how credit card processing works. Further, we will explain the reasons why PCI Compliance is no longer enough, and examine the risks inherent in relying entirely on PCI. We've spent over 15 years helping Fortune 500 retailers adopt new technology and implement solutions to combat security threats. In this paper we report on a number of valuable measures that can be implemented to overcome dangerous gaps in data security.

Why Securing Credit Card Information Is So Important

There should never be a second thought when it comes to ensuring credit card security. The breach or theft of cardholder data affects the entire payment card ecosystem; a single instance of credit card breach can cause customers to lose trust in your brand or firm. Customers' credit can be negatively affected, causing enormous personal fallout. Merchants and banking institutions can lose credibility (and in turn, business) and be subject to damaging financial liabilities.

In addition to all the other credit card breaches that have taken place, the recent well-reported "Target Breach" should have all of us questioning the steps we take to keep our credit card information secure. The Target incident was by no means an isolated occurrence; in recent months there has been a wave of high-profile hackings at big merchants, including Home Depot, high-end retailer Neiman Marcus and grocery chain Supervalu. Hackers successfully made off with 56 million payment card details, including 53 million email addresses, of customers who shopped at North American Home Depot stores between April and September of 2015. Home Depot alone spent $43 million in the third quarter of 2015 dealing with the fallout from this security lapse, one of the largest data breaches ever. If there is one thing these cases demonstrate, it's the terribly high cost of security failures.

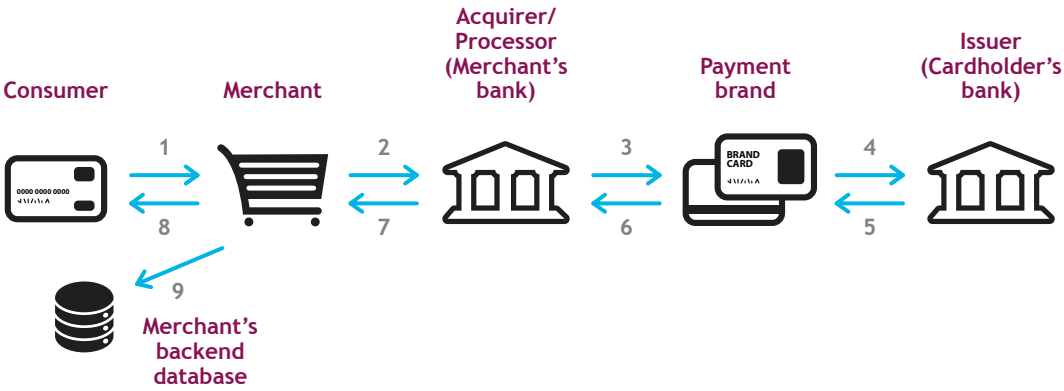
Recent Major Credit Card Data Breaches

# of Accounts and or Cards Exposed

In response to these threats, retailers are investing millions of dollars on internal investigations, and offering identity theft protection services to their customers. Sadly, companies are now investing thousands of dollars to cure a problem that they could have avoided by simply taking the proper measures in the first place. This is due to a lack of understanding of the ways in which credit cards are compromised, a reliance on inefficient approaches for securing credit card data – and blind faith in PCI compliance.

Before diving into the different techniques that can be employed to prevent credit card fraud, let's first understand how credit card processing works.

How Credit Card Processing Works



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

1. A consumer wants to purchase goods or services using his credit card. The cardholder data is entered into the merchant's payment system, either 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 cover the transaction.
5. The issuer generates an authorization number and routes this number back to the card brand, and the issuing bank agrees to fund the purchase on the consumer's behalf.

500 S. KRAEMER BOULEVARD, SUITE 301, BREA, CA 92821 ☰ (714) 579-7979 ||| NISUM.COM

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 (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 the analysis of consumer buying behavior and the creation of marketing programs.

Throughout the payment processing chain, sensitive data is at risk: when it is *at* rest, *in transit and in use*. A few simple examples illustrate what is meant 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: returns, chargebacks, customer loyalty programs and other marketing activities. No matter where it resides, any data at an aggregation point is vulnerable to hackers. 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, and being used for a part of the transaction process (for example, when the acquirer's computer is reading card data to determine which card brand to submit it to, 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 data thief might be able to extract information.

The typical approach to overcoming these risks is adherence to PCI Compliance. Below we'll explore the PCI irony, and talk about what other tools can be employed to better prevent security breach.

500 S. KRAEMER BOULEVARD, SUITE 301, BREA, CA 92821 (714) 579-7979 NISUM.COM

Blind Faith in PCI Compliance

The Payment Card Industry Data Security Standards (PCI DSS) are widely considered to be a global set of best practices for securing sensitive data. Their objective is to prevent payment fraud by securing cardholder data within organizations that either accept card payments, or are involved in the handling of cardholder data. PCI DSS procedures are an essential component in any merchant's holistic risk management program—but they are not without limitations.

Simply put, PCI standards do not allow credit card numbers to be stored on a retailer's point-of-sale (POS) terminal or in its databases after a transaction. To be PCI-compliant, merchants must install end-to-end encryption systems or outsource their payment processing to a service provider who provides a Tokenization option.

The Catch: The PCI Security Standards Council has been warning retailers that passing an annual audit may not be sufficient and that compliance monitoring should be an ongoing process.

The PCI standard only sets a minimum level of security requirements, and it might not be enough to meet your business's risk appetite. For example, one PCI requirement states external vulnerability scans must occur on at least a quarterly basis. For most organizations, however, a quarterly scan is not enough; the typical best practice is to run external vulnerability scans weekly, if not daily.

Ironically, stakeholders typically confine themselves to PCI audit results and proclaim their businesses are secure. Simply put, those measures aren't enough. Retailers must be proactive in staying on top of the methods hackers are using to steal customers' credit card information, and actively seek to employ the latest techniques to prevent such fraud.

Beyond PCI: Tokenization

Data encryption is a typical and common way to protect cardholder data. But there is a new approach to data security that goes beyond encryption, one that holds the promise of diminishing a merchant's risk of data breach and filling the gaps in PCI compliance. A viable solution for merchants of any size, this new and proven approach is called *tokenization*.

When applied to data security, tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent (referred to as a *token*) that has no extrinsic or exploitable meaning or value. The original value may be stored locally in a protected data warehouse, at a remote service provider, or not stored at all. The goal of tokenization is to reduce or eliminate the risk of loss of sensitive data, and to avoid the expensive process of notification, loss reimbursement and legal action.

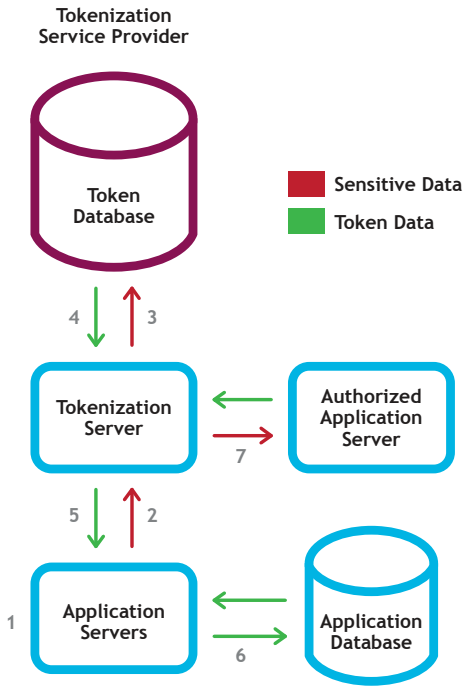
Tokenization has become a popular way to bolster the security of credit card and e-commerce transactions, while minimizing the cost and complexity of complying with industry standards and government regulations.

It works like this: the tokenization service provider issues a driver to the merchant which converts the credit card into randomly generated tokens (tokens can be either be numeric or alphanumeric). Since these are not actual cards, they can't be used outside the context of that specific unique transaction and that particular merchant. The service provider handles the issuance of the token value, and bears the responsibility for keeping the cardholder data locked down.

The surrogate token can even have the exact same format (size and structure) as the original value, helping to minimize application changes. But the token itself is effectively meaningless (rather than a scrambled version of the original data) and thus cannot be compromised to reveal sensitive data.

Conceptual Architecture for Tokenization

1. Application server collects or generates a piece of sensitive data.
2. Data is immediately sent to the tokenization server — it is not stored locally.
3. Tokenization server generates random token. Both the sensitive value and the token are stored in a highly secure and restricted database (usually encrypted).
4. Tokenization server retrieves token value from token database.
5. Tokenization server returns the token to the Application Server.



6. Application server stores the token in application database, rather than the original value.
7. When the sensitive value is needed by any authorized application, it can request it. The value is never stored in any local database, and in most cases access is highly restricted, dramatically limiting potential exposure.

Benefits of Tokenization

1. **Internal Protection:** Tokenization doesn't simply stop anonymous criminals. It also protects sensitive information from those connected to your organization, including employees, vendors and suppliers. Randomly generated payment IDs are unreadable except by the payment processor.
2. **Data Isolation:** The secured data is no longer associated with Customer or Personal data, so that in the unfortunate circumstance that any one piece of data is compromised, other data are still secured (i.e., customer's names are stored separately from date of birth, Social Security number etc.). Thus isolated, any compromised data is useless and poses no security threat.
3. **Reduced PCI scope:** Tokenization makes it easier for merchants to become PCI-compliant because retailers don't store any sensitive customer information.
4. **Online Protection:** Recently, all retailers started using EMV: chip-enabled credit cards that offer extra security. For a transaction to go through, the chip must be present and customers must supply either a signature or personal identification number (PIN). Unfortunately, in the online world this feature becomes obsolete, because the chip isn't physically present at the time of purchase. By contrast, tokenization offers unparalleled protection for both online and retail purchases.
5. **Compatible with Other Technologies:** Tokenization not only works with credit card plastic, but with gift cards, NFC payments, ACH transfers and Apple Pay; customer data is protected no matter how customers choose to send and receive money.
6. **Protection of Other Information:** With tokenization, retailers can protect a broad range of personally identifiable data and financial information, including:
   - Patient records
   - Employee files
   - Usernames and passwords
   - Email addresses
7. **Cost Effective:** Tokenization is incredibly cost-effective, not to mention easy to implement.

500 S. KRAEMER BOULEVARD, SUITE 301, BREA, CA 92821 (714) 579-7979 NISUM.COM

We Use Chip-Based Cards (EMV), So We're Covered. Really?

Several card brands argue that EMV is the preferred way forward for reducing payment card fraud at the point of sale (POS). True, EMV represents vast improvements over the basic security inherent to the decades-old technology of magnetic stripe cards, but it is fundamentally designed as an authentication technology, not a data security technology. As a result, the implementation of EMV alone does not protect the entire payment transaction process.

There are key areas of vulnerability in the payments process. From the point of card insertion or tap forward, when the card data is transmitted in the clear to the processor or later stored by the merchant post-authorization, data is open to threats that EMV can't be counted on to prevent: merchant-specific risks such as the interception of card numbers in transmission on the merchant network and attacks against repositories of card information within the merchant, acquirer, processor, network or issuer environments require further protections.

Lastly, EMV is designed for instances where a payment instrument is presented in person, so the simplest method for circumventing EMV is to use a stolen card number in a place where EMV validation does not occur, such as an ecommerce transaction.

Choosing A Tokenization Service Provider

Since there is no one single tokenization solution suited for all applications and organizations, one must choose a tokenization service provider with care. Many factors may influence this choice, including the type of information being handled (credit/debit, Social Security numbers, or other sensitive information), organizational structure, and the technologies involved.

As a general principle, tokenization and de-tokenization (getting the PAN via authorized applications) operations should occur only within a clearly defined tokenization system that includes a process for approved applications to submit tokenization and de-tokenization requests.

Below is a general outline of tasks to consider when choosing a tokenization service solution:

1. **Evaluation of Requirements:** Determine system topology, traffic loads, disaster recovery or failover plan and hardware requirements (including hardware security modules, load balancers, etc.). Identify types of data to be protected, the numbers and types of applications affected, and the techniques to be used to protect sensitive content. Lastly, make decisions regarding domain names, authentication methods (which may use existing LDAP or Active Directory resources) and preferred encryption format.
2. **Determination of target environments:** Identify development, testing, QA, staging, certification, and production environments as appropriate.
3. Evaluation of the need and count of secure data servers.
4. Identification of changes required for load balancers and network settings.
5. Acquisition and setup of certificates and firewall access.
6. **Integration of APIs:** Depending on the product features to be used, tokenization service provider supplied software components (APIs) must be integrated into their existing applications to take advantage of the security services now available.
7. Planning and execution of data conversion.
8. System testing, staging and production/rollout process.

Additionally, there are a number of other considerations to be mindful of when selecting a token server:

1. **Security of the Token Server:** What features and functions does the token server offer for encryption of its data store (tokens), monitoring transactions, securing communications, and the verification of requests?
2. **Scalability:** How can the tokenization service be grown to keep pace with increasing demand?
3. **Performance:** In-payment processing speed has a direct impact on both customer and merchant satisfaction. Does the token server offer sufficient performance for responding to new token requests? Can it handle expected and unlikely-but-possible peak loads?
4. **Failover:** Payment processing applications are intolerant of token server outages. In-house token server failover capabilities require careful review, as do service provider SLAs: be sure to dig into anything you don't fully understand. If your organization cannot tolerate downtime, be certain that the service or system you choose accommodates those requirements.

500 S. KRAEMER BOULEVARD, SUITE 301, BREA, CA 92821 (714) 579-7979 NISUM.COM

Additional Considerations

Beyond tokenization and PCI compliance, here are few additional aspects to consider for reinforcing data security.

Real-time Fraud Monitoring Hits Hackers Where It Hurts:

Real-time fraud detection mitigates risk, reduces manual reviews and streamlines order processing. Companies can reduce fraud risk by quickly and intelligently analyzing thousands of transactions in a stream and uncover relevant information for informed decision-making. Real-time monitoring allows your business to build and leverage the power of proprietary algorithms and scoring capabilities and connect them to identify fraud patterns.

BigData & Stream Processing Means There's No Excuse For Poor Records:

In the Dominos case, some accounts had anywhere between 50 to nearly two thousand purchase attempts in one month. Suspicious activity like this could have easily been detected through real-time stream processing. Stream processing has advanced dramatically in past 2 years; there are several open source and proprietary solutions out there to analyze data on the fly.

As for data, storing large amounts of data is not expensive anymore. It should be a given that your company is storing all possible access logs, cookies and session information to detect fraud patterns. What good can storing all of this information do? The insight of an access log, for example, could reveal that 5% of fraud is occurring from a specific IP address, or from users using a particular browser. Having that information on hand can protect you from a more malicious attack, and isolate the source of new threats.

Your Staff Are The Foot Soldiers of the Fraud War:

Training store staff on standards and security measures is imperative; they are the frontlines of your fraud prevention strategy. Ensuring they are knowledgeable about sensitive information protection is the first step to protecting your business, especially since hackers can tamper with physical devices. Educating your staff on spotting these very real threats is a strategy element you can't afford to skip.

End-to-End Encryption (E2EE)

E2EE is the ideal state in which credit card numbers and other sensitive information is encrypted from the point of entry (card swipe) to the other end (the issuing bank).

500 S. KRAEMER BOULEVARD, SUITE 301, BREA, CA 92821 (714) 579-7979 NISUM.COM

Point-to-point encryption (P2PE), sometimes referred to as end-to-end encryption (E2EE), is defined as a solution that encrypts card data from the entry point of a merchant's point-of-sale (POS) device to a point of secure decryption outside the merchant's environment, such as a payment processor like TSYS Acquiring Solutions. The purpose of P2PE is to address the risk of unauthorized interception associated with cardholder data-in-motion during the transmission from the POS terminal to the payment processor.

Hardware Based Encryption:

Enable off-site data storage with a physical device that stores all of your sensitive information, encrypts data and outputs the reference token.

Conclusion

While fraud risks can vary from company to company, but instead of blind faith in PCI compliance, retailers can employ real-time monitoring, tokenization, strong encryption, and a staff educated in recognizing red flags, retailers can gain a leg up and be vigilant about fraud detection in rapidly growing digital world.

References

http://www.bbc.com/news/world-us-canada-29946792

Who We Are

Nisum enables transformation for industry-leading brands: we know how to build strong emotional bonds between B2C clients and customers via smart technology solutions.

Nisum is a global consulting firm headquartered in Southern California. Founded in 2000 with the customer-centric motto, *Building Success Together*™, we've grown to comprise over 900 consultants and 8 offices across the United States, India, and Chile. Our philosophy and deep technical expertise result in integrated solutions that deliver real and measurable growth.

Whether you're a hot start-up or a major global brand, our approach is the same: forge the most powerful connection possible between people, processes and products to achieve unparalleled success. At the intersection of business and technology, Nisum has everything you need to grow your organization. From Strategic IT Planning, Agile Enablement and Business Process Engineering to Application Development, Test Automation and DevOps, Nisum has you covered. We specialize in building Adaptable Back-End systems such as Order Management, Inventory and eCommerce to facilitate true omni-channel success for our customers.

Nisum strongly believes in an organizational culture that is open, transparent and progressive. We encourage creativity and innovation and consciously maintain an environment that is conducive to positive employee growth, learning and performance.

500 S. KRAEMER BOULEVARD, SUITE 301, BREA, CA 92821 (714) 579-7979 NISUM.COM