

Transitions in Payments: PCI Compliance, EMV & True Transactions Security

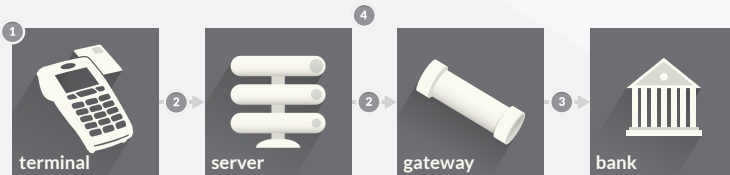
There have been more than 600 million records compromised from approximately 4,000 data breaches since 2005—and those are just the public records. As cybercrimes increase in frequency and complexity, the payment card industry and merchants continue to scramble to stay one step ahead.

With payment security being headline news, along with PCI 3.0 and EMV compliance deadlines looming, 2014 is a critical year for merchants. The optimal course of action to take is to reduce PCI scope and enhance security across all avenues of payment acceptance through encryption, tokenization and eventually Point-to-Point Encryption.

This document provides analysis of where merchants are vulnerable, upcoming PCI changes and the toolbox of products and services that CardConnect has developed to protect cardholder data.

I. Primary Points of Vulnerability

Four Vulnerabilities



- 1. Physical Device Security** – In many recent breaches, credit and debit cards were compromised by malware installed on POS systems. There have also been many instances of criminals using skimmers to grab credit card information-some which even use Bluetooth to do so wirelessly. PCI 3.0 will have stricter standards for maintenance, including recording a list of all devices and their unique identifiers. Merchants will also be required to periodically inspect their devices.
- 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.

II. PCI 3.0

What is the PCI Council asking you to do?

PCI 3.0 is designed to be proactive in helping businesses increase security of cardholder data, rather than just trying to maintain compliance. Furthermore, it intends to enhance awareness of payment security and educate merchants so they can protect themselves from attack. Testing procedures will be more rigorous, but merchants will have more opportunities to customize the way they address security.

The changes coming in PCI 3.0 fall under three categories: clarification, additional guidance and evolving requirements.

Clarification changes are meant to make the intentions of certain requirements easier to understand

Additional Guidance changes are meant to educate merchants and increase their understanding of particular topics

Evolving Requirement changes address the emerging threats in the market that could continue developing

These requirements include things like internal penetration testing, or "pen tests" for any merchant storing credit card data in their system. These test are manual, highly specialized and can cost up to \$6,000. Those not storing data are exempt from these tests.

Merchants will also have to keep a comprehensive inventory of all components, including software, hardware, and virtual machines. Another potential burden is the need for vulnerability management for all platforms. Malware protection programs will need to be in place for everything from your router to your point-of-sale terminal.

Additionally, risk assessments will need to be performed on any change—a potentially enormous burden for environments of all sizes. Alerts will need to be ticketed for review. Regular on-site inspection of PoS systems will also be required in response to recent breaches via Point-of-Sale (POS) malware.

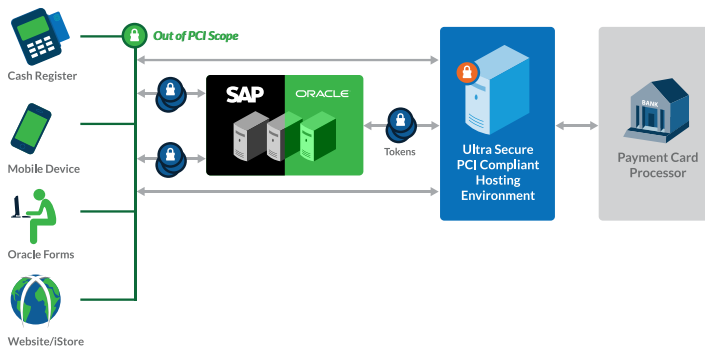
The coming updates should help organizations to better understand how payment security works and teach them to implement controls in an effective way.

What is CardConnect's response?

CardConnect's goal has always been to help merchants respond to payment card security requirements by reducing scope. One way we have done this is with our tokenization

solution. This process encrypts card data and replaces it with a mathematically irreversible token. Once a card has been replaced by a token, any system touching the token is no longer subject to PCI requirements.

We began with SAP and then moved onto Oracle, finding a way to completely remove both systems from the scope of PCI compliance.



As far as addressing the problem of protecting data at the point of entry, our PANPad solution, desktop tokenizer, Oracle Forms integration, and e-commerce solutions have been proven to significantly reduce scope for many of our merchants. The hosting of this data and processing of these transactions is also removed from the scope of PCI compliance with our SunGuard hosted environment and secure payment gateway.

Our focus has always been to simplify payment processing and security for our merchants and - ultimately - to eliminate the issue of PCI DSS entirely.

What is the difference between CardConnect and the cloud?

CardConnect is not a true cloud offering because we only store data on known machines and known networks, and we are the only ones with access to our systems. In a generic cloud offering, one purchases CPU cycles and generic amounts of memory in random data centers. They could even be in an entirely different country.

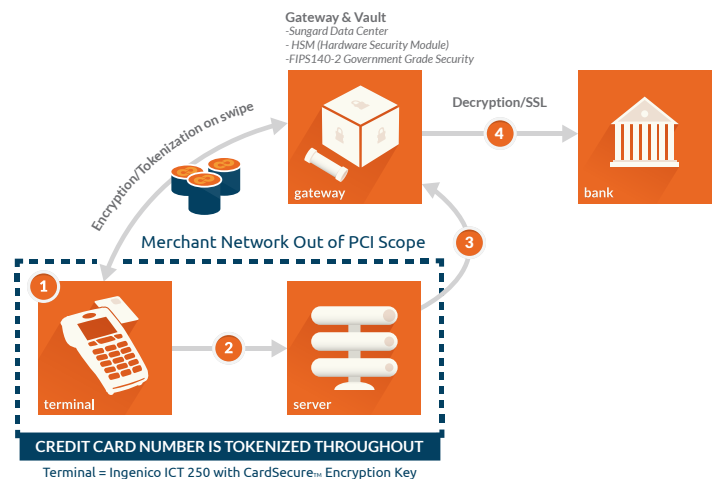
We allow all of our customers to tour our hosted environment and actually see where their data is stored. It's your data, and you are entitled to see where and how we are protecting it.

III. Transactional Security P2PE

The PCI Council has been developing their P2PE program for the past several years. After its official announcement last year, CardConnect has been working extensively on this project to bring our P2PE solution to market.

A true P2PE solution encrypts card data at the point-of-entry, regardless of device, and encrypts the data in a way where the merchant cannot reverse it all the way to a hosted environment. With a solution like this, a merchant would benefit tremendously.

These benefits include, most notably, total exemption from PCI requirements. Both Visa and Mastercard have said directly that merchants running a P2PE certified solution are no longer subject to PCI compliance. This is a huge step forward in CardConnect's mission and our program is advancing rapidly.

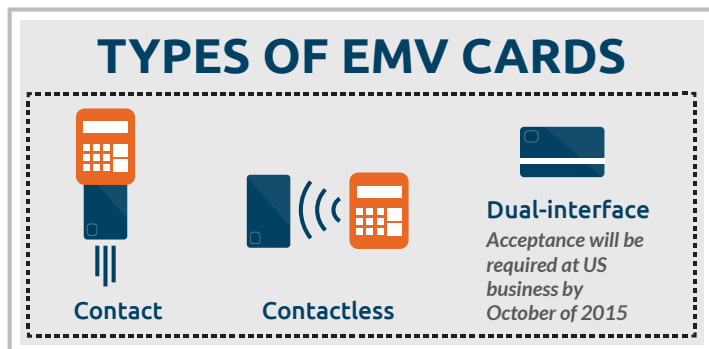


What requirements are we subject to when taking our system out of PCI scope?

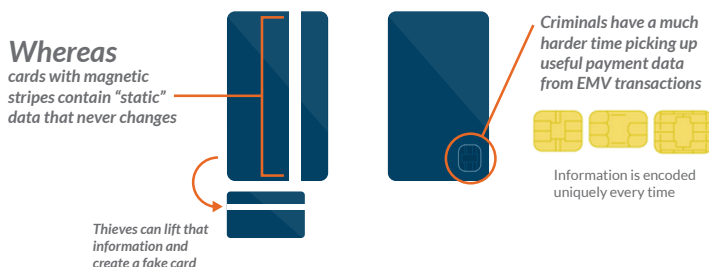
PCI DSS defines scope as the presence of 16 digit card numbers. CardConnect tokens have been proven to meet that criterion by completely replacing the card number, truly removing those systems from PCI scrutiny. Removal from scope reduces the number of PCI compliance-related questions a merchant must answer from more than 250 to nine.

EMV

The purpose and goal of the EMV standard is to specify interoperability between EMV-compliant cards and EMV-compliant payment terminals throughout the world. There are two major benefits to moving to smart-card-based credit card payment systems: improved security (with associated fraud reduction), and the possibility for finer control of offline credit card transaction approvals. It is also much more difficult and more expensive to replicate than magnetic stripe cards.



Magnetic Stripe vs. Chip



While Chip-and-PIN is absolutely a major step forward, EMV alone is not enough to keep data safe. The ideal solution is a combination of P2PE and EMV, which is why all of our out-of-the-box solutions will include EMV technology.

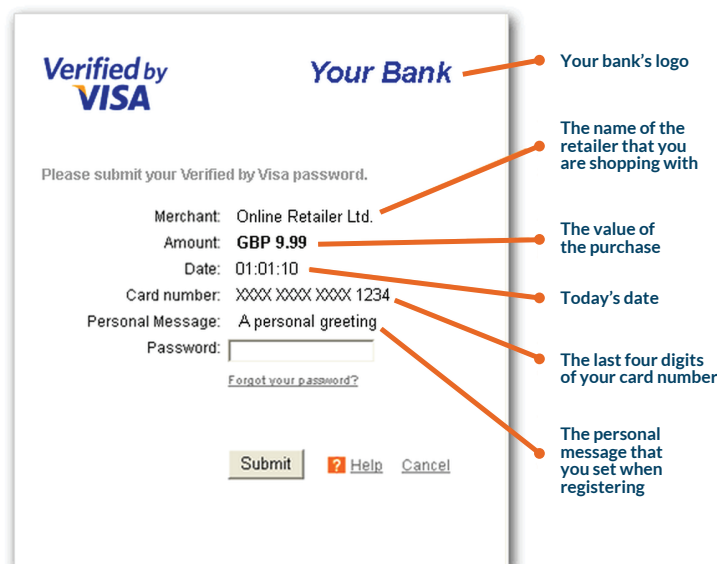
This is of course only relevant in card-present sales. In the instance of card-not-present transactions, solutions like the PANPad and the desktop tokenizer treat these sales in a P2PE-certified fashion, exempting your company from PCI DSS entirely.

3-D Secure

Since EMV has significantly reduced card present fraud in Europe, cyber criminals have begun to focus their efforts on card-not-present transactions. In response to this, Visa has developed an extra layer of protection for online credit and debit transactions called 3-D Secure. The other major card brands have adopted the technology as well.

How major card brands refer to their 3-D Secure solution:

Visa	Verified by Visa
Mastercard	Securecode
American Express	SafeKey
JCB International	J/Secure



The way it works is simple; a cardholder registers with their issuing bank for the service and creates a password. When they make online purchases on eligible merchant's websites, a pop-up will appear and require their password before authorizing the transaction. This is a significant improvement over using a card's CVV number, thus preventing fraud from card copying.

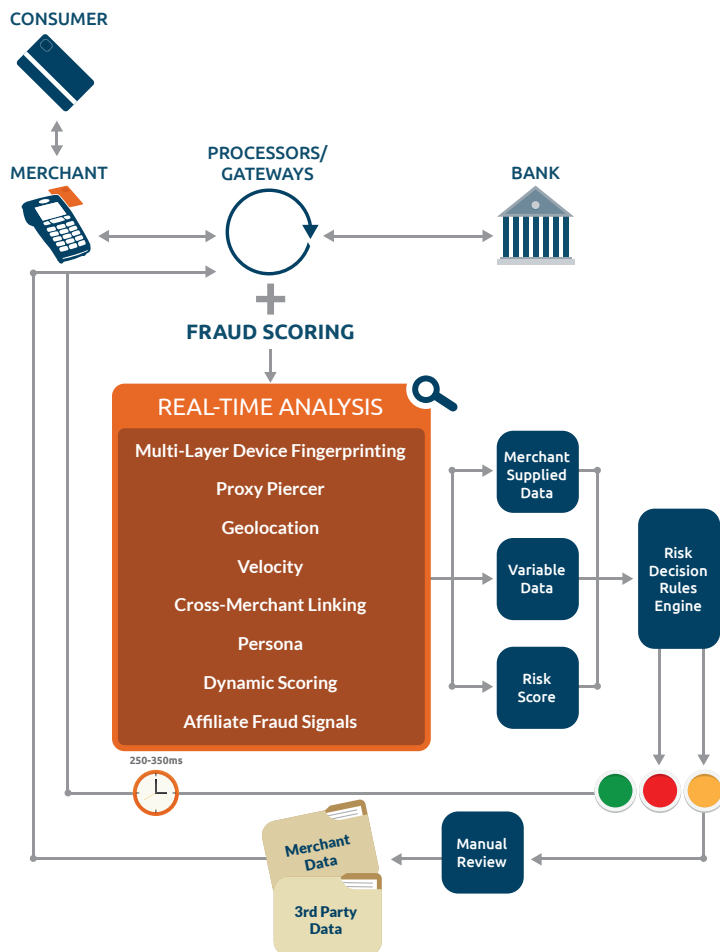
Very few banks currently support this in the US, but with the move to EMV, we expect many more to start supporting 3-D Secure and similar technologies.

Fraud Scoring

Merchants can use fraud scoring technology to determine the level of risk associated with a certain order in card-not-present environments. CardConnect has added the ability to conduct fraud scoring to our Gateway over the last year and checks data about time, location, and purchasing patterns against the current order to see if there are any

red flags. Some red flags include addresses that don't match with the cardholder account, large orders with rushed shipping and certain types of products.

The scoring is determined before the order is accepted to prevent potentially fraudulent transactions from ever taking place. If the order is found to be suspicious, the merchant may then review the order and contact the customer to verify validity, and then decide to accept or reject the order.

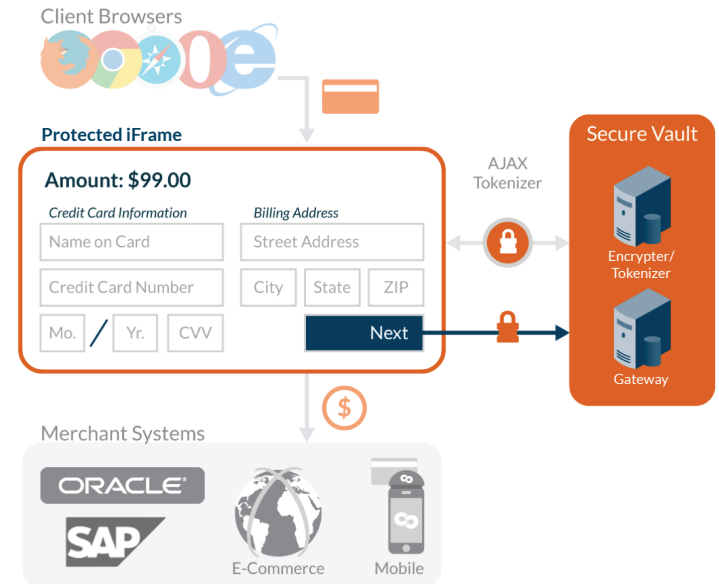


AJAX Tokenizer

The AJAX tokenizer has been another strategy that has had a lot of success in reducing the scope of PCI DSS requirements for our merchants. Through this tokenizer, the data is tokenized in the end user's browser. By tokenizing the card number entered on the merchant's checkout page prior to the card number ever touching the merchant's web environment, we can remove the entire website from PCI scope. This is exactly what our AJAX tokenizer does.

When a customer enters a card number, a call is made directly to the secure vault hosted by CardConnect. A token is delivered to the customer's computer, long before the

merchant's website ever receives the payment details. When the customer clicks to submit their payment details, that data is tokenized – removing the website from PCI scope.

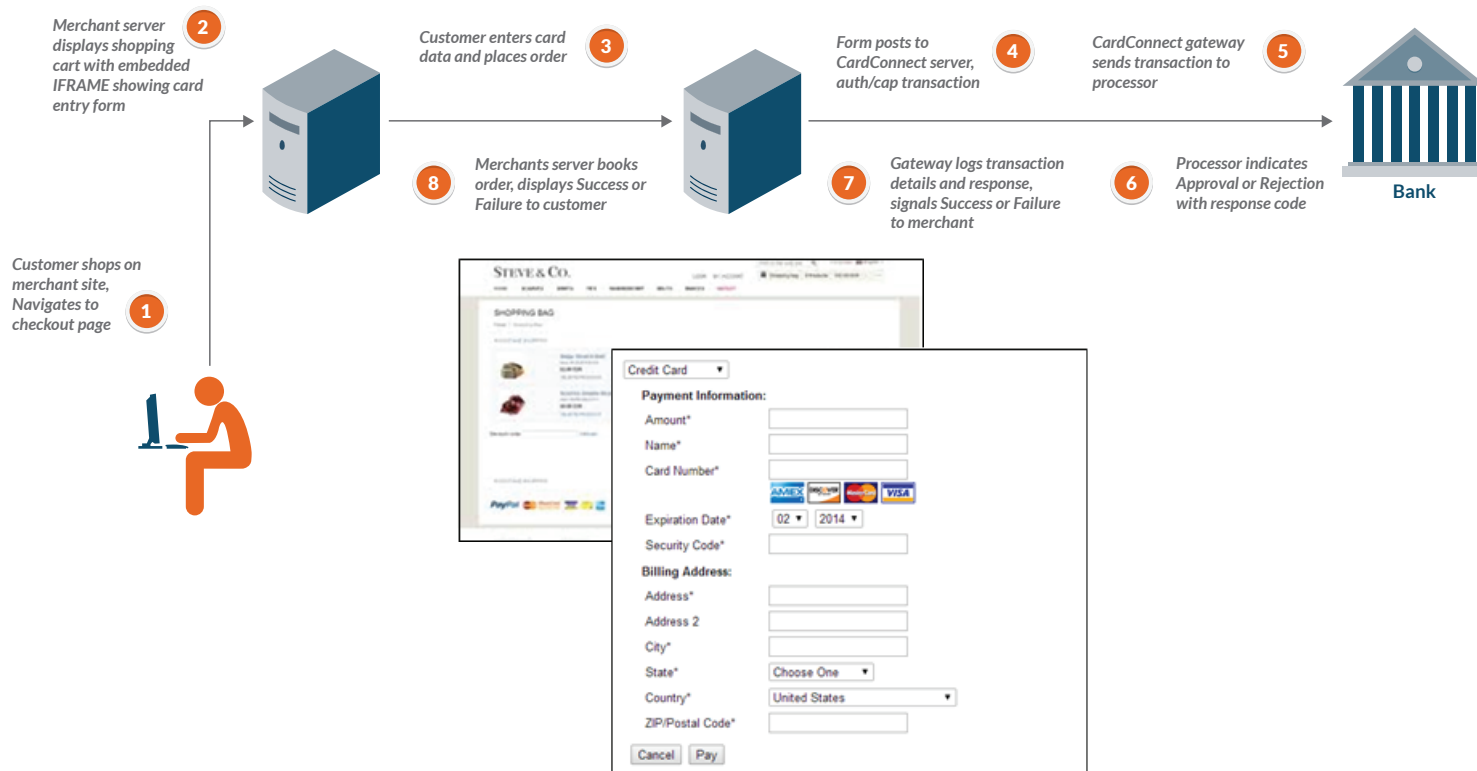


Can tokenization be used for PII and social security numbers?

Fundamentally, tokenizing PII is more challenging than card numbers because different systems have various formatting requirements and data constraints for how the fields are stored, edited and masked. That being said, CardConnect's tokenization approach overcomes these challenges as it has been successfully implemented in numerous environments for social security numbers, date of birth, bank account numbers, email addresses, etc.

Hosted Payment Page

Hosted Payment Pages are, in basic terms, a fuller version of the AJAX Tokenizer, in the sense that the entire checkout page is hosted in a secure environment. This means that all customer data is protected outside of a merchant's website, including cardholder name, address details – along with, of course, card number and expiration.



In developing the CardConnect Hosted Payment Page, we have anticipated many of the specialized configurations that a merchant might require. In terms of styling, all of the colors, fonts, fields and overall layout can be customized. In addition, merchants can make the buying process smoother by pre-populating the fields if that information is already on file. As for the actual URL where this page resides, it can be a redirect or embedded as an iFrame.

By mixing and matching the applications most appropriate for your unique environment, you will be protected from malicious threats and minimize the burden of PCI Compliance.

CardConnect is constantly developing products and services that address the ever-evolving universe of accepting payments. We'll let you know what we launch next!

connect with cardconnect

blog  