paymentspring

the pain-free guide to PCI compliance

they're in the dishwasher

In December of 2013, a breach of Target's payment systems led to data theft of 40 million credit and debit cards. Hackers stole the retail giant's login credentials from its HVAC contractor and used that access to break into its network. Because of this breach, over 17 million cards were reissued, and Target paid $39 million to banks and card companies to settle lawsuits filed over the cost of replacing cards. A company financial statement revealed the breach cost $252 million in total. But Target's wallet wasn't the only thing that took a hit—the widespread publicity of the breach was a serious blow to the company's brand and reputation with consumers.

Hard as it may be to believe that something as innocuous as an HVAC system could lead to such a high-profile security breach, the future may hold even more instances of everyday objects being used as a jumping-off point for data theft. For example, the Internet of things (IoT), or the inter-networking of devices, vehicles and buildings has created a new industry for hacking into those connected devices. Not even dishwashers are safe: In 2017, an industrial dishwasher was discovered to have a vulnerability that allows attackers to access the device and use it as a bouncing point for compromising other devices on the same network.

Unfortunately, every innovation that makes life easier launches new opportunities for fraudsters. The good news: There are best practices that minimize the risk of card data breach.

meet your good friend PCI DSS

PCI DSS, often referred to as PCI compliance, is the Payment Card Industry Data Security Standard. PCI DSS for the layman is best summed up as card protection. It's the standard anybody who touches card data in any way is expected to follow to better protect the integrity of that data and lessen the likelihood it can be compromised.

The internet was a big impetus to PCI DSS creation, as tools from the internet made it easier for card data to be accessed and stolen. There are no federal laws mandating PCI compliance; it is an

the cost of card security

1
contractor's credentials stolen

40m
cards compromised

17m
cards reissued

$39m
paid out in settlements

$252m
total cost of Target breach

industry standard, created by the payments industry in an attempt to self-regulate. However, since its inception, several states have incorporated the standard into the languages of their laws.

Initially, each card brand created its own standard, which resulted in a certain degree of chaos. All the card brands then came together to create the PCI Security Standards Council (SSC), which released the first PCI DSS in 2006. As the council worked to define and evolve a cohesive set of standards, updates were made on a two-year cycle. Today, the PCI DSS is a mature standard; changes are still made as needed, but not as frequently or to the degree they have been made in the past. And while the SSC sets the standard for compliance and provides education about that standard, it doesn't handle compliance activity or enforcement. The card brands each have their own compliance rules, which they enforce and fine for accordingly (more on that later).

Any entity handling cardholder data is classified by level based on the number of transactions they handle each year. A business handling a small number of transactions would be considered Level 4, whereas a business handling a large volume of transactions is a Level 1 merchant or vendor.

PaymentSpring is certified as a Level 1 Service Provider. The Level 1 certification process is a grueling one. It involves a complete audit of data security policies and practices by an outside auditor, or a Qualified Security Assessor (QSA), who is certified by the SSC. Once the QSA arrives on site, the process involves a review of data, staff interviews and testing of processes and procedures. That audit must ensure, to the auditor's and company's own satisfaction, that all the measures being presented are in place 24/7/365, not just once a year.

alphabet soup

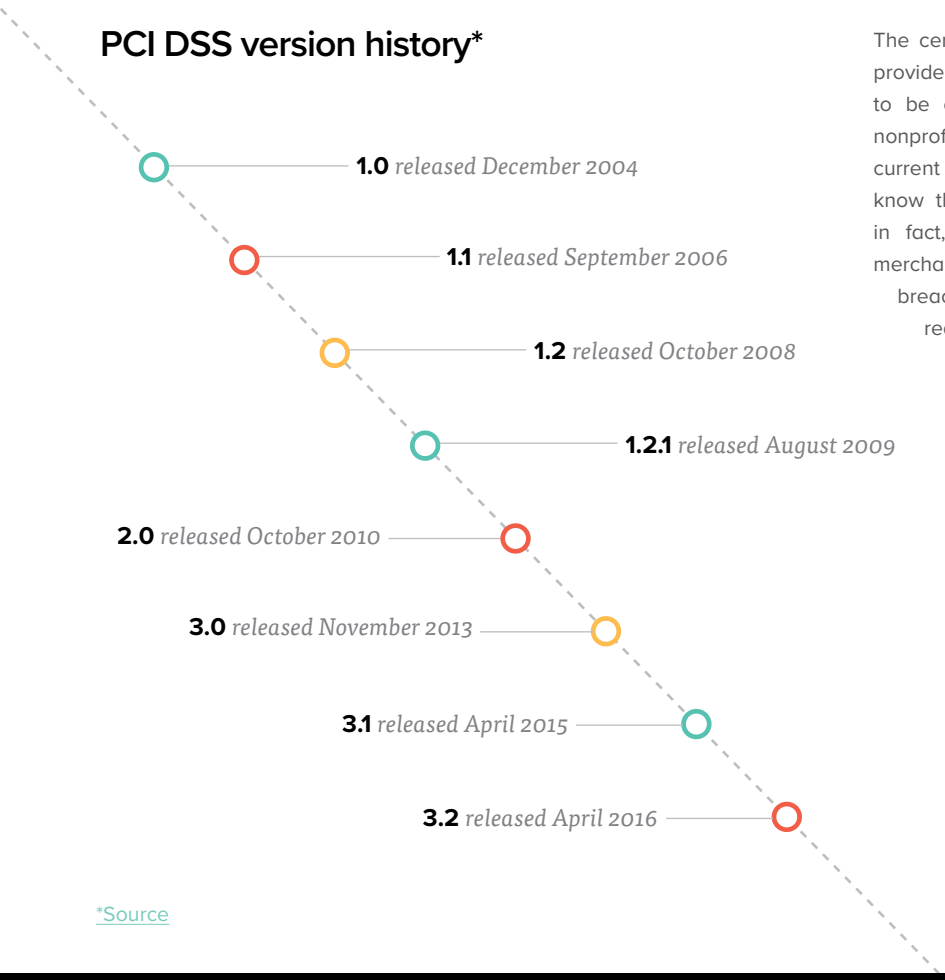
PCI DSS: Payment Card Industry Data Security Standard

PCI SSC: Payment Card Industry Security Standards Council

SAQ: Self-Assessment Questionnaire

QSA: Qualified Security Assessor

PCI DSS version history*



*Source

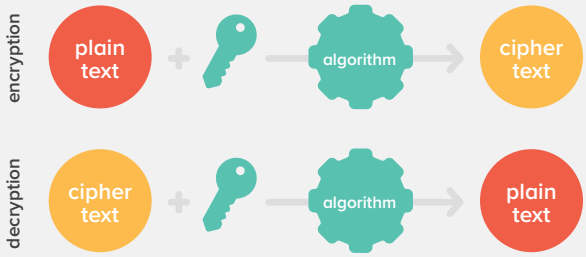
PCI DSS and you

The certification process varies depending on a merchant's service provider level, so it's important for all merchants and their staff to be educated on the basics of PCI compliance. For example, nonprofits need to be sure their service providers can show their current compliance assessment, and small businesses should know that being small doesn't make them immune to breaches—in fact, smaller merchants are often more likely targets. Small merchants, particularly those in the hospitality industry, are often breached because they use solutions that don't adequately reduce their PCI DSS scope, or because they were using those solutions incorrectly.

In the event of a breach, a small merchant will find themselves fielding technical questions from their bank, processor and card brands. Frequently the breach is big enough that the merchant must hire a forensic auditor, and the business will face a $5,000/month fine from card brands until they are back in compliance. For a small business, such costs can be crippling. And it's about more than lost dollars—it's about lost trust from customers.

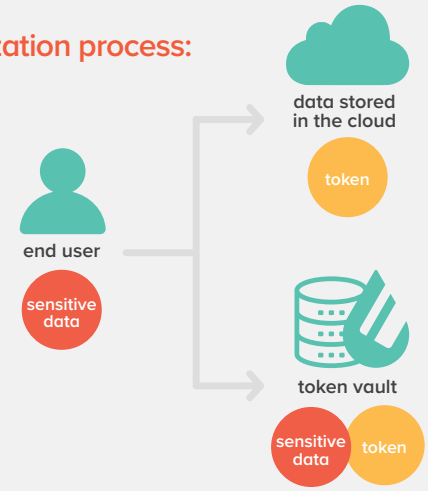
Software as a service (SaaS) companies and value-added resellers (VARs) need to prioritize security and education to better serve their customers. These organizations should communicate with their payment processor and their customers to be aware of obligations

encryption & decryption process:



*Encryption mathematically transforms plain text into cipher text using an encryption algorithm and key.***

tokenization process:



*Tokenization randomly generates a token value for plain text and stores the mapping in a database. Original data never leaves the organization.***

**Source

and accountabilities when it comes to handling card data. While SaaS and VAR companies are routinely innovating and creating desirable products for consumers, they must also keep data protection and compliance top of mind.

PCI DSS will always be impacted by innovation. For example, the recent rise of mobile has prompted the PCI SSC to update guidelines, and the use of encryption (the transformation of plain text into non-readable cipher text) and tokenization (the transformation of a meaningful piece of data into a random string of characters) has led the council to offer simpler Self-Assessment Questionnaires (SAQs) for merchants using those solutions.

compliance made less complicated

Speaking of simpler SAQs, merchants using PaymentSpring's Gateway solution will generally qualify for a more expedited SAQ. Merchants using the solution correctly will have little to no interaction with a user's actual card number due to encryption and tokenization. While this doesn't remove it entirely, it does greatly reduce the merchant's PCI DSS scope. PaymentSpring also offers a PCI DSS validation assistance program for its merchants that directs them to the appropriate questionnaire and provides a templated security policy, making the process as painless as possible.

> *"We didn't go into this business naive. We know that if we're touching card data and we're advertising that we'll help people with payments, we're a target. And we're not going to be an unwitting target. We know that to protect our customers and their customers, it's not an option to do anything other than everything that we have to do."*
>
> **Karen Markey**, PaymentSpring Senior Vice President, Compliance & Client Services

Not all payment processors give PCI compliance the attention it deserves, but security is PaymentSpring's top priority. To protect its merchants, PaymentSpring includes a breach protection program in its PCI solution where merchants are protected for up to $100,000 in costs.

If you're ready to work with a payment processor that minimizes your PCI compliance pain, give PaymentSpring a try at paymentspring.com/sandbox.

paymentspring

paymentspring.com
866.431.4637
12165 West Center Road, Suite 72
Omaha, NE 68144