How firms can reduce PCI scope

ClientPay

THIEVES FOLLOW THE MONEY.

Willie Sutton is attributed as saying that he robbed banks “because that’s where the money is.” The PCI Security Standards Council says in our current digital age, that thinking is behind the prevalence of data breaches — especially financial fraud. Thieves follow the money.

Today, it’s no surprise that financial institutions are the most-targeted industry in data breaches. And professional services are only slightly down the list, ranking as the third most common victim in data breaches.

KNOWLEDGE IS POWER.

What are you doing with your knowledge?

When you look at the stats around data breaches, it’s tempting to feel defeated.

Knowing that, what can you do to keep your firm out of those statistics?

In 2018, in the United States:

- **There were 1,244 data breaches, which exposed 446 million sensitive records.**
- **50% of small businesses reported a data breach.**

Some data breaches — like the recent Capital One breach — are insider jobs. Because of the thief’s access and training, they are almost impossible to prevent. Most breaches, however, can be minimized or avoided entirely by following PCI standards.

WHAT IS PCI DSS?

PCI DSS is short for Payment Card Industry Data Security Standard. It's a set of standards that manages how businesses accept credit cards and store sensitive credit card data. Both things help protect consumers' private data.

There are 12 PCI requirements, and those are divided into 6 categories or goals.

PCI GOALS	PCI REQUIREMENTS
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data on a need-to-know basis 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for personnel

In this eBook, we'll look at the 6 PCI goals and the steps you can take to reduce PCI scope with each.

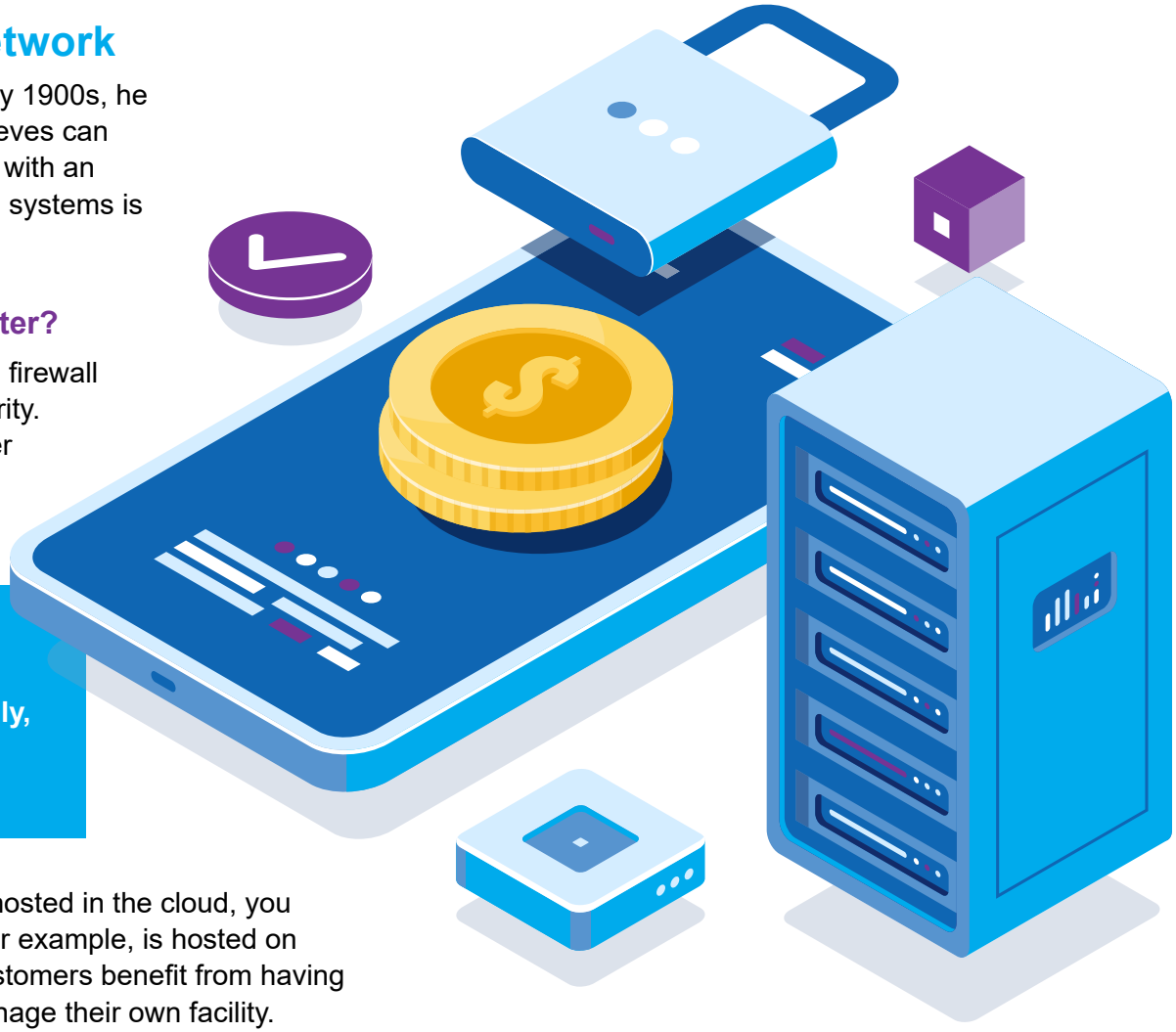
PCI DSS GOAL 1:
Build and maintain a secure network

When Willie Sutton was robbing banks in the early 1900s, he had to physically enter the banks. Today, data thieves can steal sensitive information from almost anywhere with an internet connection. One way they gain access to systems is by passing businesses' firewalls.

Who's responsible for the firewall and router?

Part of building a secure network is maintaining a firewall and router that are configured for maximum security. If you use the internet, having a firewall and router is essential. It's a minimum for businesses that accept credit cards.

One way you can add security — and reduce scope — is by piggybacking on another organization's firewall. Specifically, an organization with more security resources.



If your payment processing software is securely hosted in the cloud, you may get additional security benefits. ClientPay, for example, is hosted on Amazon Web Services (or AWS). This means customers benefit from having the highest level of security without paying to manage their own facility.

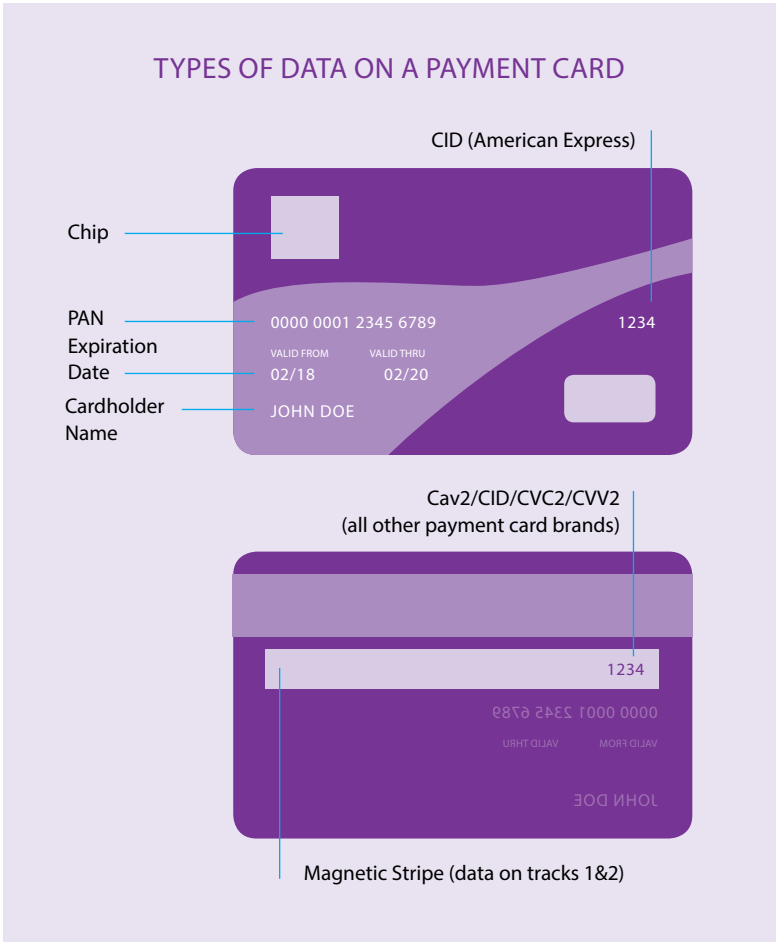
PCI DSS GOAL 2:
Protect cardholder data

The second PCI DSS goal is to protect cardholder data. To understand what this means, let's start by breaking down the elements of cardholder data. First, there's the data that's printed on the card:

- **PAN** (or primary account number) is the number that's printed on the front of debit and credit cards.
- **Expiration date**, which is printed on the front of cards.
- **CVV** (or card verification value) is the 3-digit number printed on the back of VISA, MasterCard, and Discover cards, usually on the signature line. On American Express cards, this is referred to as a CID (or cardmember ID) and is printed on the front of the card, usually above and to the right of the card number.

Data is also stored on the card's **chip** (which is on the front of the card) and on the **magnetic stripe** (which is on the back of the card).

Some firms meet this standard by writing the card number, expiration date, and CVV on paper and then storing it in a locked cabinet. This is a huge security risk.



Should you store cardholder data?

The PCI guidelines state that cardholder data should only be stored if it's necessary to meet the needs of your business. For businesses that need to regularly charge their clients' cards, it may be necessary and more efficient to store the cardholder data. After all, it's time consuming for firms — and annoying for customers — to repeatedly get and give card numbers.

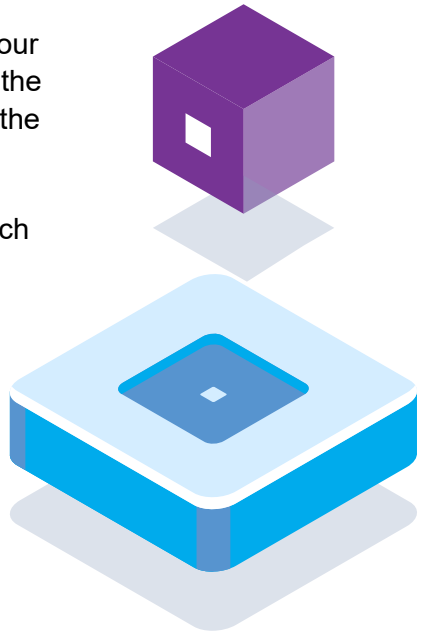
The best way to reduce PCI scope is by having a third-party vendor securely store and encrypt cardholder data. For maximum security, the vendor should be Level 1 PCI compliant.

How to reduce PCI scope — and securely store credit card information

The best online payment processing tools — such as ClientPay — can securely store credit card information in compliance with PCI standards.

With ClientPay, for example, credit card info is sent to a third-party payment gateway. The payment gateway stores the data and returns a unique ID, which is called a token and maps to the credit card information.

The token is stored in ClientPay's secure database, not with the firm. (Another step to reduce scope for professional service firms.) Then, when your clients are ready to pay, ClientPay sends the token to the payment gateway, who pulls the credit card info that the token maps to.



When you write the steps out, the approach sounds clunky. In reality, it's seamless to professional service firms and their clients. The entire process happens in milliseconds. This lets you accept credit cards and reduces the PCI scope associated with storing cardholder data.

PCI DSS GOAL 3:
Maintain a vulnerability management program

Managing your vulnerabilities means systematically and continuously finding and fixing weaknesses in your payment card infrastructure system.

What does this mean for firms? At the most basic level, it's using and regularly updating your antivirus software. But could you be doing more?

The best vulnerability managers monitor your system 24/7 for threats and irregularities. Even the largest firms — firms with a security team — can feel strapped by that level of surveillance. And for smaller firms, 24/7 surveillance monitoring can be a huge drain on resources.

Working with a payment processor who provides 24/7 surveillance monitoring is the most cost-effective way to reduce PCI scope related to vulnerability management.

ClientPay uses a vendor for 24/7 vulnerability monitoring. The vendor is a Level 1 PCI compliant security company. They provide ClientPay with services like 24/7 security, intrusion detection, and surveillance monitoring.

Code to the highest, most secure standards

Building a strong vulnerability programs starts with code. And when it comes to application security, OWASP sets the standard.

OWASP is the Open Web Application Security Project. It's an unbiased, international nonprofit that identifies the biggest security threats and provides guidelines about how to code against those attacks.

To reduce PCI scope, choose a company that codes to OWASP standards and conducts regular penetration tests to find security vulnerabilities that hackers could exploit.

Benefits to building on proprietary software

When developers build payment processing apps on open-source software, they rely on the community to create fixes for vulnerabilities that are discovered. By contrast, apps that are built on proprietary software can rely on the product's team to create and deploy patches for vulnerabilities.

The ClientPay app, for example, is built on the Microsoft stack. If there's a security vulnerability, the development and security teams at Microsoft find it and deploy a fix.

PCI DSS GOAL 4:
Implement strong access control measures

Access control is about limiting who has access to cardholder data. Access should only be granted on a need-to-know basis. However, when firms use outdated payment methods, cardholder data can land in a variety of places.

Never ask your clients to send credit card information by mail or email. Reduce PCI scope by emailing secure click-to-pay links or by including secure click-to-pay links on your website.

Who opens the mail at your office? Should that person have access to your clients' cardholder data? If you mail invoices and ask clients to pay by check or credit card, it's hard to control who sees the cardholder data that comes in by mail.

PCI DSS GOAL 5:
Regularly monitor and test networks

Networks are the glue that connect everything in the payment infrastructure. Vulnerabilities anywhere in the network make it possible for criminals to access the entire payment ecosystem.

Regularly testing the network is essential. And another equally important security measure is quickly deploying fixes to address any vulnerabilities you detect.

If you don't have a cybersecurity team at your firm, you can reduce scope by letting security experts find and fix vulnerabilities

PCI DSS GOAL 6:
Maintain an information security policy

Having digital safeguards to keep cardholder data safe is an important first step. The second step is ensuring that everyone who may encounter that data understands their role in keeping that information safe.

For security training to be effective, it shouldn't just be viewed as a checkbox that needs to be completed. Creating a formal security awareness program — and regularly reviewing it with your team — is one of the best ways to reduce PCI scope.

If cardholder data is shared with any business outside your team, ensure that they're Level 1 PCI compliant and that they only work with teams who are Level 1 PCI compliant.

CONCLUSION

The PCI DSS standards are prolific, but they follow common sense and mirror security best practices. Being vigilant and intentional about your payment processing standards is one of the best ways to reduce PCI scope.

Contact ClientPay for more information about how to reduce PCI scope.

ClientPay®