

What credit managers need to know to stay PCI compliant

Lucy Hubbard

Credit managers oversee high-value transactions every day, handling sensitive customer data every step of the way. These purchases make their businesses prime targets for fraudsters looking to intercept payments or get ahold of the card number used for the transaction. To protect their business and their customers' sensitive data, credit managers must take steps to ensure their companies are compliant with the standards laid out in the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS is a set of security rules regulating how businesses store, process and transmit cardholder information and other sensitive information to protect users' privacy. Major card brands banded together to form PCI DSS in 2004 following a rise in fraud coinciding with the popularization of e-commerce spaces.

"Noncompliance could lead to data breaches, threatening legal penalties and reputational damage with customers being more hesitant to do business using cards in the future," said Matthew Hacker, national sales executive for United TranzActions (Miramar, FL). "Compliance failures can even void certain contracts or trigger lawsuits. Companies that are consistently noncompliant can also lose their ability to accept cards in the future, hurting their business and reputation."

PCI regulations exist to build and maintain security that protects cardholder information within a business's software. Requirements aim to control who accesses sensitive information while monitoring systems for vulnerabilities and upgrading them to address evolving needs.

The following requirements from the PCI Security Council must be upheld to ensure data is secure and protected:

Install and maintain network security controls. Your process acquirer and IT team need to ensure that all the networks that payment details pass through are secure. "All system components need to be secure," said Hacker. "Your IT team is responsible for creating your internal network and making sure that all the data is secure on those different platforms and components and that information is segregated correctly."

Protect stored account data using cryptography. With customers you work with regularly, you will likely keep their card on file for future use. It's critical that their information is stored securely within your system. Cryptography, a system where a distinct, one-time code is used for each transaction rather than the real card number, can prevent real card details from being stolen and used nefariously.

"You can protect cardholder data with strong cryptography during transmission over open public networks," Hacker said. "You need to make sure that the solution that you're using can protect all of it and that you're avoiding passing raw card data across the network."

Protect systems from malicious software. IT teams should regularly scan networks for disturbances and have malware prevention in place so that sensitive information is not leaking unbeknownst to the business or customer.

Develop and maintain secure systems and software. PCI compliance is an ongoing effort, that requires businesses to consistently upgrade and refine systems as fraud becomes more advanced. "You need to be

able to constantly upgrade your systems to respond to any new and evolving threats that can emerge,” said Hacker.

Restrict physical access to cardholder data. PCI compliance requires that there is a clear segregation of roles and duties in your payment platforms, with not every employee given access to the full wealth of sensitive information.

“You’re going to have multiple users within your organization that need to run card transactions,” said Hacker. “Your users need to be created in the platform, but never every user needs to have admin access that allows them to pull data and reports or see transaction details. Admin access should be reserved for those in management or working at a supervisor level, you don’t want regular users to have access to everything.”

To protect cardholder details within a system, identify users and only grant them access to the components of the system needed for their duties. It’s also best to avoid storing cardholder data physically, whether that is written out in a spreadsheet, email or even text message. When written out, this information is not encrypted, making it more vulnerable

Monitor access to system components and cardholder data. To stay on top who is accessing what in your sprawling system, each user needs a unique username and password.

“You do not want to be sharing usernames and passwords to log into a payment platform,” said Hacker. “If you do that, you’re not going to know who was doing what within the system because it’s just going to show up as one username. So make sure everybody has a unique username and password to access any payment systems that you’re using.”

Test security systems and network regularly. “Your IT team needs to regularly patching security holes or flaws for any software changes that may happen,” said Hacker. “They can also assist with your quarterly network scans required for PCI compliance.”

Create company-wide policies that support security. The PCI Security Standards Council requires organizations to maintain a policy and program around PCI compliance.

“Depending on the size and complexity of your company, you might have to create a policy in-house,” said Hacker. “A lot of processors have a generic default policy and program that you can download from their PCI compliance portal. You can give that policy to your IT team and ask them to check that your current system meets the requirements.”

The bottom line: PCI compliance is an ongoing effort, not only within the credit department but across the company. To ensure customers’ private data is thoroughly protected, there must be a company-wide commitment to building a compliance policy and routinely testing and upgrading it to fit evolving needs.