Payment card industry compliance for financial institutions

February 2020

The security of information has been at the forefront of financial institutions' fiduciary duties since the passage of the Gramm Leach Bliley Act in 1999. The payment card industry (PCI) security standards council was launched in 2006 by the five global payment brands, Visa, Inc., Mastercard Worldwide, American Express, Discover Financial Services and JCB International, who assumed the responsibility on behalf of the industry for the development, management, education and awareness of the PCI Data Security Standard (DSS) for payment cards.

While the initial focus of PCI DSS compliance has been merchants and service providers, any organization that processes, stores or transmits cardholder data, including those that are financial institutions, is required to comply with the guidelines.

The PCI DSS is comprised of the following:

- PCI DSS—security standard for any organization that processes, stores or transmits cardholder data such as merchants and service providers
- Payment Application DSS (PA-DSS)—security standard for the development of application software that processes, stores or transmits cardholder data
- PIN Transaction Security (PCI PTS)—security standard for PIN entry devices such as credit card terminals or ATMs
- Point-To-Point Encryption (PCI P2PE)—security standard for secure devices, applications and processes that encrypt data from the point of interaction
- PCI PIN Standard (QPA)—security standard for secure management, processing and transmission of personal identification numbers
- PCI Card Production Logical Security and Physical Security Standard (CPSA)—security standard for card production and provisioning activities
- PCI 3DS Core Security Standard—security standard for 3D secure software development kits
- Approved Scanning Vendor (ASV)—external vulnerability scanning services

Financial institutions often experience difficulty understanding if they must comply with the PCI DSS. Further, if compliance is required, they may not understand which of the 12 requirements for protecting account data are applicable. This document has been developed to help institutions better understand the PCI compliance issues facing the industry and which standards should be followed in certain situations.

Noncompliance with applicable PCI requirements could result in significant financial penalties, the potential for customer accounts to be compromised, and reputational damage to the institution.

Does the PCI DSS even apply to financial institutions?

Unbeknownst to most financial institutions, the PCI DSS applies to them as well as to merchants and service providers. The PCI DSS states:

> "PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)."

According to the DSS, a financial institution is considered a merchant if it accepts credit or debit cards for payment of goods and services such as safety deposit boxes, public utilities, insurance policies or any other payments. An institution is considered a service provider if it is connected to card processing networks such as VisaNet, NYCE or First Data and processes card transactions on behalf of merchants or other entities.

If financial institutions issue credit or debit cards, they are considered issuers regardless of whether they physically issue the cards or have outsourced card issuance to a third party. Financial institutions are only required to conform to the relevant PCI DSS requirements for issuers if the financial institution physically issues cards with either the Visa or Mastercard logos.

Financial institutions are considered an acquiring bank or acquirer if they contract with merchants for the acceptance of credit or debit cards for payment. Even though the financial institution may have outsourced the processing of transactions to a third party, the financial institution is still considered the acquirer. Acquiring banks need to establish and maintain a merchant PCI compliance tracking and reporting system, as acquiring banks are ultimately responsible for any risks posed to sponsoring merchants and third-party service provider's payment systems, and must periodically report their compliance statistics to payment brands, for example, Visa, Mastercard, Discover or AMEX.

Both Visa and Mastercard have issued guidance to financial institutions regarding compliance with their respective customer information security program (CISP) and site data protection (SDP) cardholder data security programs. While neither card brand requires that financial institutions formally file their PCI DSS compliance documentation with either card brand, both card brands require financial institutions to ensure they comply with the guidelines.

What are some examples of how the PCI DSS affects financial institutions?

As the financial industry evolves to meet the needs of its customers, technology is increasingly at the forefront of significant disruption to long-standing processes for consumers. An example could be a bill payment solution, which is more and more common as a service offering for financial institutions. If the customer can enter credit cards into these systems to pay for a subscription service each month, the PCI DSS may come into play for any organization using these solutions, even if they are outsourced.

Another example of how technology is becoming a prevalent disrupter for financial institutions are fintech, or financial technology, organizations. These fast-moving companies cover a broad spectrum of industries, including retail banking and service lines, including data aggregation services. Customers using credit or debit cards, or financial institutions integrating credit or debit card technology may be affected.

Overall, the PCI DSS allows for organizations interacting with credit or debit cards to have a framework to secure their customers' data. In some contractual cases, institutions will need to comply with the PCI DSS.

Are financial institutions that outsource credit and debit card issuance and processing required to comply with the PCI DSS?

Many financial institutions outsource credit and debit card issuance and processing to a third party and may assume that they are not required to comply with the PCI DSS. Even in cases where a System and Organization Controls (SOC) report from the contracted third party exists, the need for the outward expression of assurance on PCI DSS compliance remains with the institution.

Even with outsourcing, financial institutions' applications and networks can still come into contact with cardholder data in a number of ways. The most common ways encountered are:

- The switching and transmission of ATM transactions over the institution's data network
- Storing of debit card full primary account numbers (PAN) in the institution's core application
- Accounting department PCs or servers storing spreadsheets from credit or debit card service providers (Visa or Mastercard) that contain full PANs
- Processing of credit or debit cards through dedicated card terminals or teller terminals for payments
- Storing credit or debit card full PANs in a statement consolidation and rendering systems or as PDF files from a third party that creates the institution's statements

These forms of contact are very common within financial institutions and trigger the requirement that the financial institution must demonstrate compliance with the PCI DSS.

Does PAN encryption and PA DSS certification negate the need to demonstrate PCI compliance?

A financial institution's application providers may have their applications PA-DSS certified. With these measures in place, many financial institutions may think that compliance with the PCI DSS is not necessary.

However, even when applications utilize encryption for storing cardholder data, that data still has to be processed or transmitted to or from those applications. Also, while an application may be PA-DSS certified, a financial institution must ensure that the application was implemented according to the vendor's explicit requirements to maintain this certification.

As a result, the financial institution is still responsible under the PCI DSS for ensuring, at a minimum, that:

- Cardholder data is securely transmitted over the financial institution's network
- Cardholder data is securely processed by the financial institution's applications
- Any encryption used is based on an industry-tested and accepted algorithm such as the Advanced Encryption Standard (AES)
- Any encryption algorithm used employs strong key lengths and proper key management practices

Do commercial financial institutions that do not issue credit or debit cards have to comply with the PCI DSS?

If the financial institution signs merchants up for accepting credit or debit cards for payment of goods and services and the financial institution processes card transactions for those merchants, then the financial institution is required to comply with the PCI DSS.

Even if the financial institution does not process merchant transactions, the institution is still required to establish a merchant PCI compliance program and periodically assess that program for Visa or Mastercard and report its merchant PCI compliance statistics to the appropriate card brand.

In addition, while commercial financial institutions may not physically issue credit or debit cards, they may issue PANs to their commercial customers to use such cards for airline reservations, purchasing office supplies and other business purchases. If those PANs are processed or stored by any of the financial institution's application systems or are transmitted over their networks, then it needs to comply with the PCI DSS.

Still unsure of whether your financial institution must be PCI compliant?

At a minimum, all financial institutions should conduct an assessment of their applications and networks to determine if cardholder data is processed, stored or transmitted by those applications or networks. Based on the outcome of the assessment, the financial institution will determine whether or not it needs to be PCI compliant, and which PCI DSS requirements are relevant to the organization.

An outside adviser can perform the assessment, which consists of taking your institution through the entire PCI Report on Compliance process, and identifying where potential compliance gaps exist. If PCI compliance gaps are found, guidance is provided on approaches to remediate those gaps.

If your financial institution is considered an acquiring bank, then you need to establish an appropriate merchant PCI compliance program for your affiliated card brand. This program entails quarterly reporting on your merchants' PCI compliance.

As the frequency of and methods for fraud continue to increase, the PCI DSS has become a critical area of focus for merchants, service providers and financial institutions that are subject to the guidelines. Noncompliance with the applicable PCI DSS requirements puts institutions in breach of their contract with their card brand and exposes them to undue risk.

Penalties vary on a case-by-case basis, but more importantly, any compliance concerns place your customer assets and your reputation at risk. It is imperative for banks to understand the correct level of compliance necessary and implement systems and controls in order to sufficiently achieve it.

+1 800 274 3978
rsmus.com

tl-nt-ras-fi-0620