Q&A: PCI Readiness, Risk Management, and Compliance for Financial Institutions

January 24, 2024

Q: If an FI manages their cards program in house and issues cards, are they also considered a service provider?

A: The FI would be considered an Issuer, and only be a service provider if they are managing processes on behalf of someone else. In the case of a CU, the CU might be a Service Provider if it has a CUSO that provides services to other CU's, and those services include or impact security of credit card transactions. An example where a Bank might be a Service Provider could be a situation where a holding company has centralized IT operations and/or card operations for one or more subsidiary banks.

Q: Will you be defining 'card data'? We aren't currently a merchant and we don't directly issue cards, so we have pieces of data on our core, but don't have the CVV.

A: Card holder data (CHD) as defined by PCI DSS includes: Primary Account Data (PAN), Cardholder Name, Expiration Date, and Service Code. Please see page 4 of the PIC DSS Version 4 document.

Q: If we use a third party to run our card transactions, then do we still fill out the SAQ-D? Does it need to be done by someone qualified and not internally completed? Or when should we outsource this review to an external party? What if the only card transactions we run are the cash advances and over the phone for loan payments?

A: Try not to fall into the trap of thinking about "daily transaction authorizations." Think in terms of the security of stored card holder (CHD) data related to transactions.

We suggest you first confirm/validate your PCI cardholder data environment (CDE) footprint: Where do you store, processes and transmit CHD. Then confirm/validate whether you have electronic stored CHD in your systems:

(1) Do you have CHD in the core? In other applications?
(2) Do you have stored account statements that have CHD?
(3) Consider processes related to instant issue, charge backs, disputes, fraud investigations, etc.

- *use the questions from the slides (slide 26) to drive this discovery.*

If you have stored electronic CHD, you must complete either SAQ-D or a ROC. Which one you complete depends on the volume/number of transactions:

- *>6M requires a ROC*
- *1M - 6M can use a ROC or SAQ-D*

ROCs must be completed by a QSA (you need to hire an outside entity for this such as CLA) or an ISA (internal staff trained and certified) and signed by an officer of the company. SAQ-D can be completed by internal personnel (ISA trained) or an external QSA.
You should be requiring the third party to provide you an Attestation of Compliance (AOC) annually (see requirement 12).

Q: In your experience have you found that the particular compliance requirement is negotiable with a processor? Ex. initially require a ROC for all entities but will accept an SAQ?

A: Negotiation for particular or specific controls? NO. For PCI DSS ver4 you must follow the Defined Approach or the Customized Approach for all controls that are in scope. If you believe a control is NA, you need to document the justification for the NA evaluation.

Negotiation re: can we report as a SAQ-D this year, and ROC next year? Maybe. That is most likely a case-by-case basis that needs to be discussed with whomever you are required to report compliance to..

Be careful about asking the party that can (contractually) demand compliance reporting. If you have not talked to them about this previously, this may put you on their radar, and they may or may not be open to flexibility.

Q: We outsource our credit card processing and servicing. I know we are still responsible for our risks, the risks can't be outsourced, but would this be done by our processor?

A: We would suggest that you first confirm/validate your PCI cardholder data environment (CDE) footprint: Where do you store, process, or transmit card holder data (CHD). Then confirm/validate whether you have electronic stored CHD in your systems:

(1) Do you have CHD in the core? In other application systems?
(2) Do you have stored account statements that have CHD?
(3) Consider processes related to instant issue, charge backs, disputes, fraud investigations, etc.

- *use the questions from the slides (slide 26) to drive this discovery.*

This will help define what you need to do for "internal" controls compliance and annual compliance reporting.

Requirement 12 defines what you need to do to hold your service providers responsible. You need to document which providers are part of your PCI scope, and for each service provider, which controls they are responsible for. From this, you can request from them (require?) they provide you with their PCI compliance report (AOC) for the controls they are managing.

Q: What are some examples of software development a CU may do that would meet this requirement?

A: This applies to ANY software development for systems that would be considered in scope — i.e., part of the cardholder data environment (CDE). Recall the flow chart in the presentation (slide 30) used to determine if something is in scope:

(1) Part of the CDE

(2) Within the same network segment as CDE systems, or
(3) Connected-to or security-impacting system

This could be development of source code for custom applications, development of web application/SharePoint type sites, database processing coding, API interfaces, etc.

There needs to be defined "secure coding" policies, standards, and procedures. See requirement 6 in the DSS.

Q: Is there a mapping of NIST 800-53 controls to the PCI DSS controls available somewhere?

A: The best "mapping tool" we have seen to date comes from Audit Scripts. They have built and maintain a controls framework mapping tool that maps nearly all significant control frameworks back to CIS Controls. You can use that to cross reference particular NIST controls to PCI controls.

https://www.auditscripts.com/free-resources/critical-security-controls

Q: You only mention credit cards, however PCI impacts debit cards as well, correct?

A: That is correct. CC and debit cards. This applies to cards that have a major card brand logo on them.

Q: Do ATM transactions add to the transaction count?

A: Classic consultant's answer: It depends.

- *NO for cash withdrawals from accounts.*
- *YES, if for purchase of "things for sale" such as postage stamps.*

Q: Even if you are relying on service providers, you still have to complete the targeted risk assessment as a means of identifying your CDE and verifying the AOC is all you need, correct?

A: We would suggest you turn this around:

First confirm/validate your PCI cardholder data environment (CDE) footprint: Where do you store, processes and transmit CHD. Then confirm/validate whether you have electronic stored CHD in your systems:

(1) Do you have CHD in the core? In other applications?
(2) Do you have stored account statements that have CHD?
(3) Consider processes related to instant issue, charge backs, disputes, fraud investigations, etc.
- *use the questions from the slides (slide 26) to drive this discovery.*

Then confirm/evaluate your controls.

Targeted Risk Assessments are defined in requirement 12 and are used to evaluate and establish the frequency for controls that are defined as "periodic." The Targeted Risk Assessment is NOT how you define your CDE.

When you rely on a service provider, you will need to validate and hold them accountable for the controls they manage on your behalf. The primary mechanism for this is to request their AOC, which is the summarized form of their complete compliance report (either a SAQ or ROC).

Q: Randy, what is your response to service providers that offer the ability to store CHD in their software, but state "We aren't in scope for PCI so we don't provide an AOC"?

A: Card holder data (CHD) is always in scope. Where the CHD resides is in scope. If CHD is stored in an application (provided by a third-party service provider - TPSP) the application storing the CHD is in scope.

- *If the CHD is stored in an application hosted by a TPSP, then Requirement 12 says you need to hold the TPSP accountable for the controls they are responsible for on your behalf.*

- *If the CHD is stored in an application and YOU host/run the application in-house, then TPSP may not need to provide an AOC. In this case, the application still needs to be fully compliant.*

The TPSP may state they won't provide PCI compliant services, in which case:

- *you need to implement and manage the controls yourself, or*

- *you need to find a different way to store the CHD, or*

- *you need to find an alternative service provider, or*

- *you decide to live with the consequences of not being compliant*

Their statement is usually code for we don't want to go to the effort or pay for the effort to become PCI compliant.

Q: We save all our card disputes which include card numbers. This is accessible to just our card department for audits, or questions from members, or for police dept should a police report be filed and they want info on the fraud loss, etc. Is it ok for us to keep this info which includes full card # for these reasons?

A: YES, you can save CHD for these purposes if it does not include Sensitive Authentication Data (SAD). SAD includes:

- *Full track data*
- *Card verification code*
- *PINs/PIN blocks*

You need to make sure the proper controls are applied to secure this data in line with the PCI DSS. This will require you to have a clear definition of your CDE.

Q: So, if we process over-the-phone credit card payments for loan payments on a website on an isolated iPad that only five people have access to, is that segmented?

A: Please keep in mind your description here is a very specific payment process or channel. This process has several components:

- *Over the phone*

- *iPad*
- *loan payment website*
- *a set of five staff*

Recall the discussion about the terminology "segmentation" and "isolation." Segmentation in the PCI terminology is meant to define how the CDE is isolated from non-CDE systems.
Whether or not the process you describe is segmented in a manner that provides isolation will depend on the configuration of the systems.

- *Is the card number spoken over the phone? Is the phone system VoIP?*
- *How is the iPad configured?*
- *Is the iPad on the institutions' Wi-Fi network?*
- *Is the iPad used for any other purposes?*
- *Is the iPad backed up to iCloud? Somewhere else?*

We recommend a clear understanding of all payment processes, followed by a definition of the CDE based on those payment processes. Once the CDE is defined, then analysis of required controls, including segmentation (i.e., isolation) controls can occur. That will provide the basis to conclude if the segmentation (isolation) is effective.

Q: Where could we obtain the position paper on VOIP?

A: The PCI Security Standards Council (PCI SSC) maintains a document library. This library contains the DSS, the various forms and templates, as well as "supplemental documentation" meant to provide added details related to the PCI DSS.

PCI Document Library:
https://www.pcisecuritystandards.org/document_library/

PCI blog post related to telephone payments:
https://blog.pcisecuritystandards.org/industry-guidance-on-accepting-telephone-payments-securely

PCI supplement on telephone-based payment card data:
https://listings.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf

Q: If your contact center "turns off" recording during the call when the member is sharing card info, is that considered a strong control?

A: Turning off recording is an excellent way to not store the card holder data (CHD). There are some call center software packages that allow this to be done manually, while there are others that do this for you "auto-magically."

Keep in mind that while this can help reduce or eliminate the storage of electronic CHD, this does not eliminate the transmission.

Furthermore, if the caller is speaking the card number, in all likelihood, the call center rep:

- *is typing the CHD into an application, a web page, or a notes document*

- *may be writing it down*

Q: If we are a card issuer, does that make us a service provider also? We provide instant issue?

A: The FI would be considered an Issuer, and only be a service provider if they are managing processes on behalf of someone else. In the case of a CU, the CU might be a Service Provider if it has a CUSO that provides services to other CU's, and those services include or impact security of credit card transactions. An example where a Bank might be a Service Provider could be a situation where a holding company has centralized IT operations and/or card operations for one or more subsidiary banks.

Instant issue should be considered one of one or more business processes that store, process or transmit chard holder data (CHD).

We would suggest that you confirm/validate your PCI cardholder data environment (CDE) footprint: Where do you store, process, or transmit card holder data (CHD). Then confirm/validate whether you have electronic stored CHD in your systems:

(1) Do you have CHD in the core? In other application systems?
(2) Do you have stored account statements that have CHD?
(3) Consider processes related to instant issue, charge backs, disputes, fraud investigations, etc.

- *use the questions from the slides (slide 26) to drive this discovery.*

This will help define what you need to do for "internal" controls compliance and annual compliance reporting.

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS