How to Validate PCI

A Helpful Guide for PCI Validation

April 2020

Webcheck SECURITY

Table Of Contents

Executive Summary 03

Step 1: How Many Transactions Per Year? 04
- Over One Million Transactions Per Year 04
- Under One Million Transactions Per Year. 05

Step 2: So How Do I Validate? 05

Step 3: Choose Your SAQ and Begin 05

Step 4: Where Do I Go For Help? 05

Resources 06

EXECUTIVE SUMMARY

By Greg Johnson, PCIP, CEO of Webcheck Security

This brief article is intended to assist businesses of all sorts who accept credit cards and who have been asked by their card processors, clients or other stakeholders to demonstrate PCI Compliance. If you're a *service provider*, and as a part of your value-add or main function facilitate the storage, transmission, or processing of card data for your clients, see my article Service Providers: Path to PCI Compliance

When I was first introduced to PCI in October of 2006, the PCI Security Standards Council or PCI SSC (see https://www.pcisecuritystandards.org/) had just been formed by the Card Brands – Visa (the 800-lbs. gorilla and stage-setting body), MasterCard, American Express, Discover, and JCB. At that time, the VISA CISP or Cardholder Information Security Program and those of the other Brands had evolved into the PCI DSS or Payment Card Industry Data Security Standard, which was then given to the PCI SSC as an independent body to develop, manage, evolve and promote.

Enforcement of compliance was left to the Card Brands, although technically your processor, also known as an acquiring bank (because they *acquire* the transaction) is the entity which levies mandates, fines and fees as they are fined by the Brands (Visa, MC, AMEX, etc.)

Although there is more to that story and the concept of "where the buck stops" with the top-level acquirers such as US Bank, Wells Fargo, TSYS, FiServ etc., for purposes of this article we will focus on *your* compliance requirements.

Step 1: How Many Transactions Per Year?

Over One Million Transactions Per Year. The first step to determining your compliance level and method of validation is to understand how many transactions per year you process. Level 1 and 2 merchants are doing over 6 million or 1 million *transactions per year* respectively and will have a higher level of validation and expectation. For such, this will usually involve an onsite audit by a QSA or Qualified Security Assessor annually, certified by the PCI Council.

In some cases*, the processor will allow the organization to self-assess if someone in the organization receives the ISA or Independent Security Assessor designation, also authorized by the PCI Council. What drives the option for this is whether or not the processor allows such, so if you're in this boat, check with your processor or acquirer. (*Mastercard requires self-assessment by an ISA or QSA for organizations in between one and six million transactions per year.)

Under One Million Transactions Per Year. If you're under the one million transaction level you are either a Level 3 or 4 Merchant and will be allowed to fill out a self-assessment questionnaire appropriate to the type of transactions you do, i.e. point-of-sale or POS, web-based e-commerce sales, virtual terminal or portal card entry, etc. More will be said about the appropriate self-assessment questionnaire (SAQ) shortly.

One thing you probably don't realize if you're reading this is that if you have not been submitting your SAQ and scan results (if applicable) to your acquirer, you have an annoying monthly compliance fee of anywhere from $25 - $60 or more in your statement. For small or Level 4 (under 20,000 transactions per year or non-ecommerce up to 1 million transactions) this is true even for you. This will go away once you demonstrate compliance.

You may be a small Mexican restaurant, hair salon, or even a multi-million-dollar manufacturer and be in this category, and yes you are paying a monthly non-compliance fee. It's a fine really. What you may not know is that if you're compromised while in a non-compliant status, there could be more fines. I've seen a "small Mexican Restaurant" close its doors after being levied an $80,000 fine from Mastercard.

Hence, whether your business is very small or very large, and merely doing less transactions than the Level 1 or Level 2 merchants mentioned above, it's in your best interest to invest the time and small resources to become PCI Compliant.

Step 2: So How Do I Validate?

Once you've determined your eligibility to self-assess (over or under 1 million transactions per year) you may proceed to either self-assess using the correct SAQ or hire a QSA firm, or as directed have an ISA on staff.

For most reading this article, you will fall into the self-assessment category. The *way* you process cards will now dictate which self-assessment questionnaire to use. Although there are nine different SAQ's, choosing one is made easier using this handy SAQ chart, which can be found on this link: Webcheck PCI At-a-Glance SAQ Chart™

Step 3: Choose Your SAQ and Begin

Once you've chosen your applicable SAQ from the chart posted above, you can review the requirements and begin. Some validation methods, such as SAQ A (for Card-not-present merchants, where all cardholder data functions fully outsourced) will not require a scan performed by an ASV or Approved Scanning Vendor or a penetration test performed by a qualified, objective 3rd party.

Other validation methods, such as the SAQ A-EP or SAQ D will require a scan *and* a penetration test. Other SAQ's, such as the P2PE (Point-2-Point Encryption SAQ) require no scan, no penetration test, and few questions and requirements in order to be deemed compliant.

Step 4: Where Do I Go For Help?

Despite the helpful SAQ Chart and the relatively clear direction from the Card Brands and PCI Council, it can still seem a maze of uncertainty. That's why we're here at Webcheck Security, and we are happy to advise at no cost! I will post all of the guidance and free resources, such as the ability to download the SAQ's at the end of this guide, but please don't hesitate to contact us by phone or form (www.webchecksecurity.com) and we will promptly respond. Our PCI Compliance Portal can also be a helpful way to manage your compliance, providing the applicable SAQ online, and we will be delighted to get you set up with the applicable scans or simply the online SAQ as your compliance needs dictate.

Resources

Visa: https://usa.visa.com/support/small-business/security-compliance.html#1

Mastercard: https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html

PCI Security Standards Council: https://www.pcisecuritystandards.org/

Webcheck Security: Webcheck PCI At-a-Glance SAQ Chart™

Webcheck Security PCI Portal and Requirements FAQ:
https://webchecksecurityss.pcicompliance.ws/#requirements

Office:

3367 E Castle Cary Circle, Eagle Mountain, UT 84005
www.webchecksecurity.com
801-854-2865