What Lawyers Need to Know:
Changing Requirements for Credit Card Processing

by Sharon D Nelson, Esq. and John W. Simek

Does your firm accept and process credit cards? If not, you probably should. Clients are more apt to pay their retainers or your invoices if they can use a credit card instead of writing you a check. The way you process credit cards is about to change in a big way (for all businesses), but let's start at the beginning.

Merchant Account

The first step in processing credit cards is getting a merchant account. A merchant account is essentially a contract with a "processor" that takes your transactions and processes them with the credit card companies (e.g. MasterCard, VISA, American Express, Discover, etc.). When you work with a processor, you will pay a variety of fees (e.g. discount percentage, transaction fee, etc.) for each one of your credit card transactions. Typically, the discount percentage will go down as you gather more and more information to validate the transactions. As an example, the discount rate will be lower if you have the cardholder's complete address (including zip code) and CVV (card verification value) versus only having the billing zip code. Companies such as LawPay, Sage Payment Solutions, Square and Authorize.net are credit card processors.

PCI-DSS

There are certain "rules" you will need to follow in order to process credit cards. The Payment Card Industry Data Security Standard (PCI-DSS) includes the "rules" that govern the methods and requirements for processing credit card transactions. If you fail to comply with PCI-DSS, you may be liable for fraudulent charges and even subject to fines from the credit card company or card processor.

SAQ

How do you know if you are compliant with the current PCI-DSS for processing credit card transactions? The Self-Assessment Questionnaire (SAQ) walks you through various questions concerning your infrastructure, procedures, technology, record keeping, security, etc. There are five types of SAQs that break down into nine different questionnaires depending on whether you use your own systems to process payments, store cardholder data and accept credit cards in-person and/or electronically, among other things.

- SAQ A - Card-not-present merchants: all payment processing functions fully outsourced, no electronic cardholder data storage
- SAQ A-EP - E-commerce merchants re-directing to a third-party, PCI compliant service provider for payment processing, no electronic cardholder data storage
- SAQ B - Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage
- SAQ B-IP - Merchants with standalone IP (Internet) connected payment terminals: No e-commerce or electronic cardholder data storage
- SAQ C - Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage

- SAQ C-VT - Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage
- SAQ D-Merchant - All other SAQ eligible Merchants, or those that electronically store cardholder data
- SAQ D-Service Provider - SAQ eligible service providers
- SAQ P2PE - Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage

The good news is that most credit card processors don't make you decide upfront which SAQ you need to complete. Typically, you login to a website and begin answering questions that will automatically walk you through the appropriate PCI-DSS SAQ questions that would apply. Think of it as a dynamic survey that presents a sort of decision tree path depending on how you answer the previous questions.

Current Guidelines

Why is all of this PCI-DSS "stuff" important to lawyers? The current version of PCI-DSS is 3.2 and is listed as a "best practices" guideline. However, it will become a **required** (by the terms of your merchant account contract) standard on February 1, 2018. There are some major changes to the standard that everyone should be aware of. The 3.2 requirements are focused on more protections of the card holder data. If you have already completed your SAQ for 2016, you've seen some of the differences when completing the questionnaire.

Impact

A lot of attorneys process credit card transactions from a computer that runs a virtual terminal to access their processor's system. Typically, you use a web browser to login to the processor's website and enter the credit card information. If you use a computer that shares the same network as all your other office computers, you'll need to implement a lot more stringent security controls. The actual SAQ question reads "Merchant accesses the PCI DSS-compliant virtual terminal solution via a computer that is isolated in a single location and is not connected to other locations or systems within the merchant environment." If you answer no to the question, other questions will appear asking about how you prevent the other computers from impacting the credit card process. The concern is to minimize risk of compromise of card holder data.

Connecting to the same network will require you to prevent the possibilities of other computers accessing the virtual terminal computer. This means turning off file sharing, configuring tighter internal firewall restrictions, blocking network access from local resources, preventing remote user access, etc. In other words, you don't want the potential malware infection of a user computer to potentially access the virtual terminal computer by "crawling" through your network. All of these requirements means more cost and complexity for your environment.

Recommended Solution

While it is possible to implement the security controls to comply with PCI-DSS 3.2 for all the computers on your network, it means implementing much tighter controls on ALL your computers. A better, easier and more cost effective solution is to install an isolated, dedicated credit card and online banking computer. You can create an isolated computer network by implementing a VLAN (virtual local area network) or a physically separate network. The stand-alone computer would only be used to process credit card transactions or perform online banking activities.

A single computer simplifies the security requirements for the device. Install security software and configure the computer to automatically install updates. You'll only need one local user ID since the isolated computer will not access any files or other data on your firm network. Since the computer is only using a browser to access the processor's system, you won't need a very powerful machine. You probably have an older computer that you can redeploy for this purpose. Just make sure it is running a currently supported operating system so that it gets security updates.

Chances are, many IT support folks are unaware of this change. Make sure you bring the incoming new standard to their attention. We have seen many law firms moving to the solution recommended above – and they are far more secure after implementing it.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com