



## PCI Compliance 101 – Direct Marketers



BY KEN MUSANTE

Though much has been written about PCI, it is often too technical to use or too broadly written. My goal is to arm you with enough information, specifically addressed to direct marketers so that you may 1) understand the importance of complying; 2) know what type of program direct marketing merchants should pursue; and 3) where to seek additional resources.

The Payment Card Industry (PCI) Data Security Standards (DSS) were put in place because so many merchants, vendors and acquirers were not protecting card data. Issuing banks were losing the trust of their cardholders because fraudulent use from compromised cards was increasing. Issuing banks were also losing money because of the number of cards that needed to be replaced and the amount of fraudulent transactions that ensued every time a compromise occurred.

As a result, the Card Networks jointly put in place a set of rules that govern how cardholder data must be secured. These rules are in addition to the various and countless state laws, which—although are often similar—typically govern additional personal and non-public information like social security numbers and checking account data. Regardless, all acquirers are now requiring merchants to be PCI compliant.

### **PCI Compliance Is Vital**

Some acquirers will monitor more vigilantly than others, but all require compliance. Because a merchant account is a ‘vital organ’ for a direct marketer, you should comply not only to protect your customers’ data, but also to ensure the longevity of your merchant account. Should you not be in compliance, you may lose your merchant account. Should you suffer a breach, you will also face serious fines that could reach \$30 per card, *plus* additional fines that could reach \$500,000, *plus* the cost to conduct a forensic investigation, *plus* the cost of remediation. Short answer, even a small merchant can face several hundred thousand dollars in fines if you are breached and non-compliant.

**Even a small merchant can face several hundred thousand dollars in fines if you are breached and non-compliant.**

Hopefully, I have your acknowledgement; compliance is mandatory. Next, you need to understand what is required for a direct marketing merchant. Plenty of information is available on complying, but the requirements differ for each merchant type and size. Most merchants fall in to Level 3 or Level 4. Visa and MasterCard differ slightly on the definitions and requirements, but in general, Levels 3 and 4 refer to merchants processing up to 1 million annual Card Network transactions and the validation requirements include:

- Annual Self-Assessment Questionnaire (SAQ)
- Quarterly Network Scan completed by an Authorized Scan Vendor (ASV)

- Completion of an Attestation of Compliance Form

Merchants exceeding 1 million network specific card transactions must comply with additional monitoring, which is outside the scope of this article. The Self-Assessment Questionnaire (SAQ) is a list of questions used to assess your compliance with the PCI-DSS. Direct marketing merchants will complete either SAQ A or SAQ D. SAQ A is to be used if you have outsourced all cardholder processing, transmission and storage (to a PCI-compliant vendor. PCI-compliant vendors can be verified on Visa's website at <http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf> ).

Remember, just because you have outsourced all your card data does not mean you can ignore PCI compliance!

SAQ D is considerably more cumbersome, but should be used if you are storing, transmitting or processing cardholder data. If so, you also want to ensure you have a quarterly network scan completed (and you pass) from an approved scan vendor.

SAQ D will assist you in recognizing some data must never be stored. CVC2/CVV2 data may not be stored under any circumstances. Cardholder numbers and expiration dates may be stored but must be encrypted.

Ultimately, the goal of PCI compliance is not to check boxes, it's to get merchants to secure cardholder data. If you are not currently compliant, prioritize your actions to plug the biggest threats first. Additionally, if you are getting a PCI fee from your payment processor, either monthly or annually, understand why that fee is being assessed. Sometimes it is to allow the processor to comply and merchants unwittingly believe it is for their protection.

Finally, get help from professionals in the merchant services industry. Ask your payment professional who they recommend and more importantly, why. Your cardholder data is a valuable company asset. Protect it.