Maintaining PCI DSS Compliance When Partnering with Service Providers

The discussions around the Payment Card Industry Data Security Standard (PCI DSS) typically revolve around merchants. How must a merchant validate compliance? What must be done to maintain compliance? To whom do merchants report their compliance? Lost in this conversation is the often-pivotal role occupied by Service Providers. Merchants often look to Service Providers to assist in achieving and maintaining PCI DSS compliance. Outsourcing large portions of data processing and data storage is certainly an effective means to reduce the burden of compliance, but merchants must conduct proper due diligence on their service provider partners.

1) What is a "Service Provider?"

A Service Provider, according to the Card Brand rules, is any entity that stores, processes, or transmits cardholder data on behalf of a merchant or an acquiring bank. Service providers may include billing software, payment processors, web-hosting providers and other similar companies. Working with companies like this often helps merchants with their day-to-day business operations. However, it is important to understand whether and how these service providers can affect a merchant's own compliance with the PCI DSS.

2) Why does it matter if a merchant uses a service provider?

Over the past several years, many service providers have developed services that specifically address PCI DSS compliance. They may provide PCI DSS compliant hosting space, or they may offer accounting software that supports compliance by enabling merchants to process transactions without storing cardholder data on their own computers. The important common thread in these scenarios is that the service provider can directly affect that security of payment data.

In fact, many data compromises originate with service providers. For that reason, the PCI DSS requires that merchants monitor the PCI DSS compliance of any entity that may store, process, or transmit cardholder data on their behalf. PCI DSS Requirement 12.8 states:

*"**12.8** Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:*
***12.8.1** Maintain a list of service providers*
***12.8.2** Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data that the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customers' cardholder data environment.*
***12.8.3** Ensure that there is an established process for engaging service providers, including proper due diligence prior to the engagement.*
***12.8.4** Maintain a program to monitor service providers' PCI DSS Compliance on at least an annual basis*
***12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider and which are managed by the entity".*

In short, a merchant cannot be compliant if its service provider is not PCI DSS compliant.

3) Do all service providers have to validate PCI DSS Compliance?

The long answer is, "it depends." Some service providers may themselves be using service providers of their own to outsource portions of PCI DSS compliance. As an example, a back-office software provider may be using another service provider that provides an End-to-End Encryption and Tokenization solution, like ProtectPay. The use of such a solution may reduce or even eliminate the service provider's need to validate compliance with the PCI DSS, depending upon its implementation. A service provider can choose to comply with the standard by not handling cardholder data.

Conversely, if that back office provider chooses to implement a platform to provide payment services, but that payment service does not encrypt and tokenize data, then the service provider will have access to cardholder data. In that instance, the service provider would be required to validate compliance because cardholder data is being stored, processed, and/or transmitted by the service provider.

It is incumbent upon the merchant to determine whether the service provider has access to cardholder data on their behalf, and thus would be required to validate compliance with the PCI DSS and to register with the card brands.

4) What is service provider registration and who has to do it?

Any merchant that is using a service provider should report that to its acquirer (ProPay). The acquirer is obligated to register the service provider with the card brands. This allows the card brands to identify entities that may have access to cardholder data and to identify accurately the sources of potential breaches.

5) What should a merchant do if one of their service providers is required to validate compliance and register?

A merchant must monitor the compliance of its service provider. It can do so by requesting an Attestation of Compliance (AOC) from the service provider. If the merchant says that it is not required to validate compliance because of its own service provider relationships, then a merchant can request the AOC of that entity's service provider.

Once the AOC is acquired by the merchant, the merchant must notify its acquirer, in this case ProPay, that it has a service provider that must be registered with the card brands. It is helpful to include a point of contact for that service provider so that ProPay can contact them directly.

6) Why is service provider registration important for merchants?

In simple terms, a merchant that is using a validated and registered service provider is not responsible for a breach that may occur at that service provider. The service provider would be liable for the costs associated with the card brand rules, PCI DSS non-compliance, re-issuance, and fraud reimbursement. On the other hand, if a merchant is using a service provider that is neither compliant nor registered, the merchant will be liable under the Card Brand Operating Rules. Ensuring the compliance of service providers is another way that merchants can protect themselves and their customers.

7) What can a merchant do if it is using a non-compliant service provider?

Merchants have a number of options if they are confronted with a non-compliant service provider. First, the merchant can choose to move its business to a compliant service provider. However, this is sometimes much easier in theory than it is in reality. In those cases, it is important to communicate clearly with the service provider in question. The service provider needs to have a clear understanding of its obligations. Often, a service provider may be unaware that they have an obligation to comply. They can validate compliance and register with the card brands in order to provide compliant services to its merchant clients.

In some cases, a service provider may find that remediation is required in order to become compliant. In that case, it is important to have open lines of communication between the merchant, the service provider, and the acquirer. A proactive approach to compliance is always the best approach. Ask the service provider to document a project plan with milestones and expected completion dates for any required remediation. This allows both the merchant and the acquirer to hold the service provider accountable to those dates. It also demonstrates that the service provider is actively addressing potential compliance gaps. The service provider should communicate regular updates to the merchant and finally provide an AOC once compliance has been achieved.

Some service providers may refuse to validate compliance. Unfortunately, merchants are left to try either to persuade the service provider of the benefits of compliance, or move to another service provider. If a merchant must change service providers, it is important to communicate that to the acquirer.