RISKS IN PROVIDING SERVICE PROVIDERS ACCESS TO CARDHOLDER DATA

Joshua Knopp, CISSP MasterCard Worldwide

BACKGROUND

Outsourcing business functions has become commonplace in the business world and the payment industry is no exception. As merchants look to reduce costs, they often rely on third parties to assist in managing some piece of the merchant's business processes. This assistance can come in the form of managed billing, hosted IT services (web hosting, storage, etc) or even document archival. MasterCard defines the terms Third Party Processor (TPP) and Data Storage Entity (DSE) as types of Service Providers[1].

The PCI Security Standards Council (SSC) defines a Service Provider (SP) as:

> *Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.*

A merchant often has a list of criteria it uses to evaluate each Service Providers' capabilities to ensure it meets the merchant's business needs. However, a critical criteria that is often overlooked is the type of security controls the Service Provider has in place to protect cardholder data.

The PCI Data Security Standard (DSS) requirement 12.8 addresses requirements for managing Service Providers. Specifically, requirement 12.8.2 states that an entity must: "Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess."

It is important to remember that a merchant's agreement with its acquirer or service provider generally assigns responsibility to the merchant to safeguard cardholder data in accordance with PCI DSS requirements. The merchant may be subject to various costs if the merchant is found to not have safeguarded cardholder data. For this reason it is prudent for any merchant that uses a Service Provider to ensure that the Service Provider will store and use cardholder data in a secure manner using appropriate security controls.

[1] For purposes of this paper, parties that are afforded access to payment cardholder data, such as transaction records, and whether on behalf of a MasterCard member financial institution or a merchant, are referred to as "Service Providers."

SHARED HOSTING PROVIDERS

A “Shared Hosting Provider” is a type of Service Provider that can pose unique risks to cardholder data. A Shared Hosting Provider generally provides Information Technology (IT) services to multiple customers. Frequently this means that one customer’s data (including cardholder data) is stored together with data of other customers in “shared space”, either physical or logical. Some examples of services provided by Shared Hosting Providers are web hosting, email hosting and data center services. Thanks to economies of scale, Shared Hosting Providers are often able to provide these services at lower rates than if the merchant were to manage these in-house. However, due to the shared nature of these environments, additional risks arise.

Risks

One of the more significant risks associated with Shared Hosting Providers is the possibility that a compromise of the data storage environment can result in the breach of many customers’ data. For example, a breach in Customer A’s environment could impact the security of Customer B. This risk is particularly notable for shared web hosting environments where virtualization technology is used. Suppose Customer A hosts a web application that is not involved in e-commerce, does not handle cardholder data and does not follow PCI DSS requirements for building secure applications. Customer B, on the other hand, is a large e-commerce retailer that does handle cardholder data and maintains a secure e-commerce application in accordance with PCI DSS Requirement 6. If an attacker is able to compromise Customer A, (for example, by a SQL injection attack), it may be possible for the attacker to exploit weaknesses in the Shared Hosting Provider’s segmentation controls between customer environments and also compromise Customer B’s environment – even though Customer B has strong application security controls. In this case, the attacker would likely compromise Customer B’s environment through a “back door” that the customer is neither aware of nor has control over, such as the firewall rules in the Shared Hosting Provider’s management network.

For these reasons, it is imperative that a merchant question and evaluate the controls that a Shared Hosting Provider has in place to ensure that a compromise of one of the Shared Hosting Provider’s customers will not pose a risk to the data of other customers. Merchants should ask their Shared Hosting Provider about the specific controls that they use to assure proper segmentation between customer environments. Extra scrutiny should be placed on shared resources including, but not limited to, the management network, disk storage systems, and virtual environment hypervisors.

The merchant should also address risks that arise if there is a network connection between the merchant’s local network and the environment provided by the Shared Hosting Provider (for example, an IPSec tunnel or dedicated leased line). Depending on the specific environment, the merchant will likely need to implement security controls, such as firewalls and intrusion detection/prevention, between the Shared Hosting Provider’s environment and the merchant’s own local network..

Who owns the controls?

A merchant should not assume that the Shared Hosting Provider is responsible to implement all security controls in the provided environment. For example, a Shared Hosting Provider may provide the security controls necessary to isolate customer environments from each other, but may not provide the security controls needed to protect the customer’s environment from internet based threats.

It is the merchant’s responsibility to have a clear understanding with the Shared Hosting Provider as to exactly which controls are to be provided by them and which are to be provided by the merchant.

SUMMARY – MERCHANT RESPONSIBILITIES

Merchants are typically responsible for the card data that they provide any Service Provider access to. For that reason, a merchant should ensure that their Service Providers have validated compliance with the PCI DSS for the services provided. As sharing cardholder data with a Service Provider raises additional risks to cardholder data, extra scrutiny must be placed on the Service Provider's controls. Some examples of steps a merchant should take before providing a Service Provider access to cardholder data include:

- Ask that the Service Provider agree, in writing, to appropriately protect cardholder data in accordance with the DSS for the duration of the relationship. This agreement should describe exactly which controls are to be provided by the Service Provider and which are to be provided by merchant

- Ask for a copy of your Service Provider's Attestation of Compliance (AOC) and understand whether it conducted the assessment itself or retained the services of a Qualified Security Assessor (QSA)

- Check the MasterCard Service Provider list to see if the Service Provider has registered with MasterCard

- If the Service Provider does not have an AOC and is not on the MasterCard Service Provider list, ask it to validate its PCI compliance or consider replacing it with a compliant Service Provider

- Maintain a list of all Service Providers with access to cardholder data.

- Check with your acquirer to identify how use of a Service Provider may affect your transaction level and reporting requirements.