Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)

Version: 2.0

Date: January 2013

Author: E-commerce Special Interest Group
PCI Security Standards Council

Information Supplement:
PCI DSS E-commerce Guidelines

SAMSUNG 1017

Table of Contents

1 Executive Summary 3

2 Introduction 4

2.1 Intended Use of this Information Supplement 4

3 E-commerce Overview 6

3.1 Third-party Entities 6

3.1.1 E-commerce Payment Gateway/Payment Processor 6

3.1.2 Web-hosting Provider 6

3.1.3 General Infrastructure Hosting Provider 7

3.2 E-commerce Infrastructure 7

3.2.1 Web Servers 8

3.2.2 Application Servers 8

3.2.3 Data Storage 8

3.3 E-commerce Components 8

3.3.1 Shopping Cart Software 8

3.3.2 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Encryption 9

3.3.3 Network Components and Supporting Infrastructure 9

3.4 Common E-commerce Implementations 10

3.4.1 Merchant-managed E-commerce Implementations 11

3.4.2 Merchant-managed Commercial Shopping Cart/Payment Applications 12

3.4.3 Shared-management E-commerce Implementations 13

3.4.4 Wholly-outsourced E-commerce Implementations 17

3.4.5 Outsourced E-commerce Implementations and SAQ A 18

3.5 E-commerce Roles and Responsibilities 18

Table 1: Summary of Roles and Responsibilities for Common E-commerce Implementations 21

4 Common Vulnerabilities in E-commerce Environments 23

4.1 Vulnerabilities Caused by Insecure Coding Practices 24

4.1.1 Injection Flaws 24

4.1.2 Cross-site Scripting (XSS) 24

4.1.3 Cross-site Request Forgery (CSRF) 24

4.1.4 Buffer Overflows 24

4.1.5 Weak Authentication and/or Session Credentials 24

4.2 Security Misconfigurations 24

5 Recommendations 26

5.1 Know the Location of all Your Cardholder Data 26

5.2 If You Don't Need It, Don't Store It 26
5.3 Evaluate Risks Associated with the Selected E-commerce Technology 26
5.4 Address Risks Associated with Outsourcing to Third-party Service Providers 26
5.5 ASV Scanning of Web-hosted Environments 28
5.6 Best Practices for Payment Applications 28
5.7 Implement Security Training for all Staff 29
5.8 Other Recommendations 29
5.9 Best Practices for Consumer Awareness 29
5.10 Resources 30
5.10.1 Information Security Resources 30
5.10.2 PCI SSC Resources 31
6 Acknowledgments 32
7 About the PCI Security Standards Council 33
Appendix A: PCI DSS Guidance for E-commerce Environments 34
Appendix B: Merchant and Third-Party PCI DSS Responsibilities 38

1 Executive Summary

Electronic commerce, commonly known as e-commerce, is the buying and selling of products or services over electronic systems such as the Internet. Merchants choosing to sell their goods and services online have a number of options to consider, for example:

- Merchants may develop their own e-commerce payment software, use a third-party developed solution, or use a combination of both.
- Merchants may use a variety of technologies to implement e-commerce functionality, including payment-processing applications, application-programming interfaces (APIs), inline frames (iFrames), or hosted payment pages.
- Merchants may also choose to maintain different levels of control and responsibility for managing the supporting information technology infrastructure. For example, a merchant may choose to manage all networks and servers in house, outsource management of all systems and infrastructure to hosting providers and/or e-commerce payment processors, or manage some components in house while outsourcing other components to third parties.

No matter which option a merchant may choose, there are several key considerations to keep in mind regarding the security of cardholder data, including:

- No option completely removes a merchant's PCI DSS responsibilities. Regardless of the extent of outsourcing to third parties, the merchant retains responsibility for ensuring that payment card data is protected. Connections and redirections between the merchant and the third party can be compromised, and the merchant should monitor its systems to ensure that no unexpected changes have occurred and that the integrity of the connection/redirection is maintained.
- E-commerce payment applications such as shopping carts should be validated according to PA-DSS, and confirmed to be included on PCI SSC's list of Validated Payment Applications. For in-house developed e-commerce applications, PA-DSS should be used as a best practice during development.
- Third-party relationships and the PCI DSS responsibilities of the merchant and each third party should be clearly documented in a contract or service-level agreement to ensure that each party understands and implements the appropriate PCI DSS controls. Appendix B of this document can be used as a high-level checklist to help all entities understand which parties are responsible for the individual PCI DSS requirements.

2 Introduction

There are simple principles associated with the use of e-commerce technology to accept payments over the Internet via payment cards:

a) If e-commerce technologies are used to accept payments, PCI DSS requirements apply to those technologies.

b) If a merchant outsources e-commerce technologies to a third-party service provider, the merchant is still responsible to ensure that PCI DSS is adhered to and that payment card data is protected, by both the merchant and the service provider.

c) Implementations of e-commerce technologies can vary greatly, and responsible entities need to thoroughly understand and document the unique characteristics of their particular e-commerce implementation, including all interactions with payment transaction processes and payment card data.

d) There is no one-size-fits-all method or solution for e-commerce environments to meet PCI DSS requirements. Specific controls and procedures will vary for each environment, according to how the e-commerce environment handles payment card processing.

For the purpose of this Information Supplement, electronic commerce (e-commerce) refers to environments where merchants accept payment cards over the Internet. The transactions that are processed under this architecture between merchants and consumers (cardholders) are often referred to as “Business to Consumer” (B2C). While some merchants may consider sales via e-mail, mobile devices, and telephones to be e-commerce sales; these use cases are not within the scope of this document.

E-commerce technology continues to evolve, encompassing a broad range of technologies, tools, and formats. As with any evolving technology, risks can arise in e-commerce “shops” that may be less commonly understood than those associated with more traditional “brick-and-mortar” stores.

2.1 Intended Use of this Information Supplement

The intent of this Information Supplement is to provide guidance on the use of e-commerce technologies in accordance with the Payment Card Industry Data Security Standard (PCI DSS). For the purposes of this document, all references are made to the PCI DSS version 2.0.

This Information Supplement is intended for merchants who use or are considering the use of e-commerce technologies in their cardholder data environment (CDE) as well as any third-party service providers that provide e-commerce services, e-commerce products, or hosting/cloud services for merchants. This document may also be of value for assessors reviewing e-commerce environments as part of a PCI DSS assessment.

This document provides supplemental guidance on the use of e-commerce technologies in cardholder data environments and does not replace or supersede PCI DSS requirements. For specific compliance criteria and audit requirements, e-commerce environments should be evaluated against the criteria set forth in the PCI DSS.

This document is not intended as an endorsement for any specific technologies, products, or services, but rather as recognition that these technologies exist and may influence the security of payment card data.

***Note**: This document presumes a basic level of understanding of e-commerce technologies and principles. An architectural-level understanding of e-commerce technologies is required to assess the technical and security controls in e-commerce environments. The nature of these environments may include complex technologies that are substantially different than traditional brick-and-mortar environments, such as DMZs, Internet-accessible cardholder data environments, shopping cart software, and/or service provider code embedded in, or interfacing with, a merchant website.*

This document also presumes familiarity with PCI DSS, including scoping guidance, and the detailed requirements and testing procedures.

3 E-commerce Overview

This section discusses typical e-commerce components and some common implementations, and provides high-level PCI DSS scoping guidance to be considered for each.

The scoping guidance provided in this section should be considered additional to the underlying principle that PCI DSS applies to all system components included in or connected to the cardholder data environment.

The terms "cardholder data," "cardholder data environment," and "sensitive authentication data" as used in this document are aligned with the definitions in *the PCI DSS Glossary of Terms, Abbreviations and Acronyms.*

Note: *Merchants often use card validation codes/values (also called card security codes) in e-commerce transactions. This value is the three- or four-digit number printed on the front or back of a payment card intended for "card-not-present" transactions. When the cardholder provides this value, it is considered proof that the cardholder has the card in his/her possession. This value is included in "sensitive authentication data" per PCI DSS Requirement 3.2 and must never be stored after the payment transaction is authorized.*

3.1 Third-party Entities

3.1.1 E-commerce Payment Gateway/Payment Processor

This entity authorizes payments for e-commerce merchants or, alternatively, may facilitate payment authorization by forwarding transactions to the processors/acquirers that perform the actual payment authorization. E-commerce payment processors often provide software to the merchant to interface with the merchant's shopping cart software and to facilitate collection and transmission of consumers' payment card data.

3.1.2 Web-hosting Provider

An e-commerce merchant may elect to outsource its website and/or servers to a hosting provider. These companies provide space on a shared server as well as Internet connectivity, and may also provide other security services such as encryption for secure transmission over the Internet. These companies also typically provide general types of server hosting, such as e-mail servers and Domain Name System (DNS) servers, which are essential for finding other servers on the Internet. The previously listed services are commonly referred to as "web hosting." Note that web-hosting providers may also offer a service that includes e-commerce functions such as a hosted payment page and/or shopping cart software.

It is common practice for web-hosting providers to host more than one—and often many—websites on a single server. In this type of "shared" environment, a merchant's website may be compromised through security weaknesses present in other merchants' sites on the same server or within the same environment. A merchant should always understand whether its website is being hosted in a shared environment. PCI DSS requirements are applicable to shared hosting providers, including PCI DSS Requirement 2.4 and *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers*.

3.1.3 General Infrastructure Hosting Provider

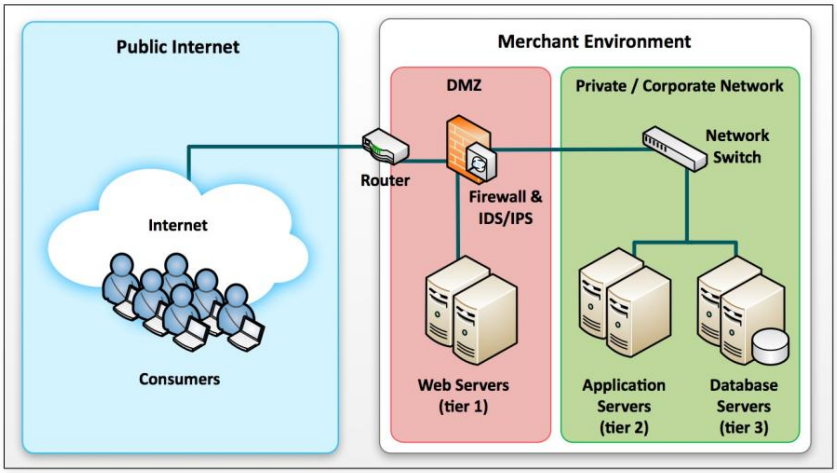
Another common form of hosting that may be used by e-commerce merchants is general infrastructure hosting. These hosting providers often provide Internet connectivity and may also provide a room, cage, or rack in an environmentally controlled and physically protected facility. Any servers in the room, cage, or rack are usually the responsibility of the hosting provider's customers to install, manage, and secure. Note that this type of hosting is not unique to e-commerce merchants, as it may be used by any entity to share the cost and responsibility associated with full management of a data center environment.

3.2 E-commerce Infrastructure

"Infrastructure" components can be considered fundamental information technology components, and are not necessarily unique to e-commerce. For e-commerce, these components may include the web server that delivers web pages to the consumer's browser, application servers, database servers, and any other underlying servers or devices (for example, network devices, etc.) connected to the cardholder data environment and/or providing support to the e-commerce infrastructure. The networking and operating system infrastructure supporting the merchant's systems such as firewalls, switches, routers, and any virtual infrastructure (e.g., hypervisors) are also included. This infrastructure can be distributed in a variety of ways such that part or all of it may be owned and managed by the merchant or hosted and maintained by a dedicated hosting company.

An e-commerce infrastructure typically follows a "three-tier computing" model with each tier, or layer, dedicated to a specific function, typically including 1) a presentation layer (web), 2) a processing layer (application), and 3) a data-storage layer.

Figure 1: Example of a Common "Three-tier Computing" e-Commerce Infrastructure



3.2.1 Web Servers

E-commerce web servers are publically accessible and are used to present information such as web pages, forms, advertisements, merchandise, and shopping cart contents to the consumer's web browser. Because web servers are publically accessible, sensitive or confidential information—such as payment card data—must never be stored on web servers (see PCI DSS Requirement 1.3.7). Web servers often communicate with other, more sensitive servers behind the firewall, particularly application and database servers.

PCI DSS Scoping Guidance: Because they receive payment card data from consumers and/or transmit that data to the merchant's (sometimes hosted) applications and databases, web servers are an integral part of the cardholder data environment and are in scope for PCI DSS.

3.2.2 Application Servers

Application servers perform a variety of processing functions and should never be publicly accessible. In most cases, consumers do not interact directly with application servers, as the application servers receive requests from the web server, to process, format, and prepare data for storage or transmission. Application servers may also receive responses or retrieve content from database servers and subsequently pass the results back to the web server for presentation to the consumer.

PCI DSS Scoping Guidance: Application servers are considered to be part of the cardholder data environment and are in scope for PCI DSS since they are primarily involved with the processing and/or transmission of payment card data.

3.2.3 Data Storage

The data-storage tier includes database servers and any other system or media used to store data. Since databases may store sensitive information, including payment card data, database servers must never be publically accessible, per PCI DSS Requirement 1.3.7. In a three-tier computing model, the database only accepts requests from and provides responses to properly formatted and authenticated requests, usually made by an application server.

PCI DSS Scoping Guidance: Database servers are frequently involved with the storage of payment card data, and therefore are considered part of the cardholder data environment and in scope for PCI DSS.

3.3 E-commerce Components

Typical components unique to e-commerce solutions include the following:

3.3.1 Shopping Cart Software

A "shopping cart" (also called a "shopping basket" or simply a "basket") is software used by a merchant to assist consumers with making purchases online, allowing them to accumulate a list of items for purchase. The software finalizes the consumer's purchase, often provides a means to capture the consumer's payment information within the web application, and may provide other functions to help an e-commerce merchant manage an online store. In a scenario where the shopping cart collects payment information from consumers, the shopping cart software communicates with an application programming interface

(API), which is often provided by the e-commerce payment processor. From there, the payment card data is transmitted to an e-commerce payment gateway and then forwarded on to the payment processor for payment authorization. There are several ways that a merchant may obtain shopping cart functionality including: 1) developing proprietary application code in-house, 2) buying custom application code developed by a third party, 3) buying or obtaining a standard shopping cart application, or 4) subscribing to a "hosted payment page" service from a web hosting provider and/or e-commerce payment gateway.

PCI DSS Scoping Guidance: The shopping cart software is in scope for PCI DSS compliance, and PA-DSS may also be applicable. The shopping cart/payment application should be developed securely and according to PA-DSS requirements to ensure either that 1) cardholder data is not stored after authorization, or 2) if the merchant has a business need for storing cardholder data after authorization, that it is protected during storage per PCI DSS Requirement 3.4 (for example, via encryption, truncation, or hashing). It is important to remember that storage of sensitive authentication data such as the CAV2, CVC2, CVV2, or CID is not allowed post-authorization, per PCI DSS Requirement 3.2, even if encrypted.

3.3.2 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Encryption

SSL/TLS is used to encrypt information sent between the consumer and merchant, and between the merchant and e-commerce payment gateway. PCI DSS Requirement 4.1 requires that payment card data be protected during transmission over open, public networks (to include the Internet). The proper implementation of SSL/TLS is one mechanism that can be used to meet this requirement. An indication that SSL is in place is the "HTTPS" prefix on the URL or address line of the web page that accepts payment card data. In addition, most browsers display a small padlock icon somewhere at the top or bottom of the browser window (most often in the address bar). The presence of the padlock icon indicates that data is being encrypted, and the user can click on the padlock icon to obtain information about the site and its SSL certificate.

PCI DSS Scoping Guidance: PCI DSS Requirement 4.1 includes specific requirements for SSL/TLS implementations. SSL relies on the validity of the certificate and must be configured securely to meet strong cryptography requirements. Note that SSL v2 is no longer considered to be secure and must not be used for e-commerce transactions. If merchants worry that some consumers without the latest browsers will not be able to access the merchant's site if the merchant upgrades to SSL v3.0, a consumer-education program should be considered that advises consumers how to easily upgrade their web browsers and which may also describe the security benefits of using a current browser to properly protect their payment card data.

3.3.3 Network Components and Supporting Infrastructure

Network components provide connectivity and communication between different systems (for example, between application and database servers), and between the merchant, consumer, and e-commerce payment processor.

The e-commerce supporting infrastructure includes all computers and networking technologies, such as web servers, application servers, database servers, routers, firewalls and intrusion-detection systems/intrusion-prevention systems (IDS/IPS), as well as any other technologies providing communication, processing, monitoring, or security functionality to the environment.

For larger e-commerce merchants and service providers, the supporting infrastructure may also include integration tools for different technologies—for example, service-oriented architecture (SOA)—as well as technologies that facilitate e-commerce operations—for example, load balancing, SSL acceleration hardware, and content caches.

Each environment will need to be thoroughly reviewed to ensure that all technologies are identified and secured appropriately.

PCI DSS Scoping Guidance: All of the network components that connect systems and/or transmit cardholder data are in scope for PCI DSS. It is important for a merchant to understand exactly where cardholder data flows throughout its network, as well as when and how that data is transmitted to a hosting provider or e-commerce payment processor.

3.4 Common E-commerce Implementations

Common e-commerce implementations are listed below with descriptions and examples of each:

- Merchant-managed e-commerce implementations:
  - Proprietary/custom developed shopping cart/payment application
  - Commercial shopping cart/payment application
- Shared-management e-commerce implementations:
  - Third-party embedded application programming interfaces (APIs) with Direct Post
  - An inline frame (or “iFrame”) that allows a payment form hosted by a third party to be embedded within the merchant’s page(s)
  - Third-party hosted payment page which redirects the consumer to a page on an entirely different domain for payment entry
- Wholly outsourced e-commerce implementations

These examples are intended to be representative of only a few of the most commonly found basic implementations. By no means are they meant to cover the vast range of deployments, hardware components, software applications, and hosting/services models that may exist.

The following section discusses the common e-commerce implementations as described above in detail and includes basic PCI DSS scoping guidance.

3.4.1 Merchant-managed E-commerce Implementations

Merchant-managed e-commerce implementations are generally those where the merchant 1) develops, or pays someone else to develop, their own payment application, or 2) uses a commercial payment application. These scenarios are described below.

PCI DSS Scoping Guidance: In general, the merchant's web application and e-commerce infrastructure are in scope for all applicable of PCI DSS requirements.

Merchants who develop their own e-commerce applications should consider developing the applications using PA-DSS as a best practice to ensure that the applications are developed securely and also help the merchant maintain PCI DSS compliance. These merchants should also consider creating an implementation guide, referring to the *PA-DSS Implementation Guide* requirements as a model, to provide guidance for internal use such as for installing and maintaining the application in a PCI DSS compliant manner within a PCI DSS compliant environment.

For commercial shopping carts/payment applications, it is recommended that they be PA-DSS validated, listed by PCI SSC, and identified as "acceptable for new deployments" in the listing at the time of purchase. Implementing and using PA-DSS validated applications in accordance with the *PA-DSS Implementation Guide* will facilitate the PCI DSS assessment process.

Note:

PA-DSS is the PCI SSC program for payment applications that 1) store, process, or transmit cardholder data as part of authorization or settlement, and 2) are sold, licensed, or distributed to third parties. The intent of this program is to ensure that payment applications obtained from a third party facilitate, and do not prevent, the merchant's or service provider's PCI DSS compliance. Validating a payment application as compliant with the PA-DSS ensures that when it is deployed according to its Implementation Guide, it contributes to the overall PCI DSS compliance of the merchant.

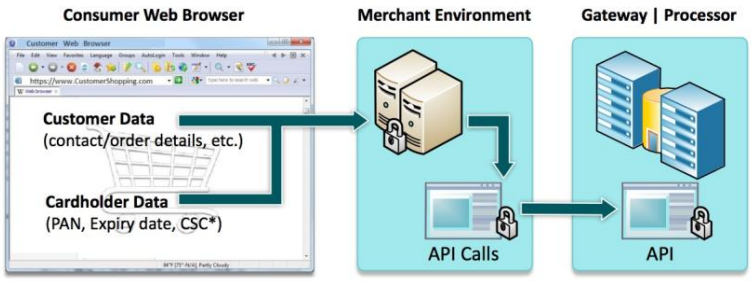
A commercial payment application that has been validated as PA-DSS compliant will provide a greater level of protection for cardholder data. For example, the assessor will have confirmed it was developed using secure coding standards and that it was thoroughly evaluated from a security standpoint.

Note that a merchant application is considered to "process" cardholder data either because the application handles the data before it is submitted to an e-commerce payment processor or during authorization and/or settlement.

3.4.1.1 Proprietary or Custom-Developed Shopping Cart/Payment Applications

For proprietary or custom-developed e-commerce implementations (also called "bespoke"), the application code for the merchant's shopping cart/payment application has either been developed by the merchant internally or custom-developed by a third party (per the merchant's specifications) as part of the overall development of the website. See Figure 2 below.

Figure 2: Proprietary/Custom Developed

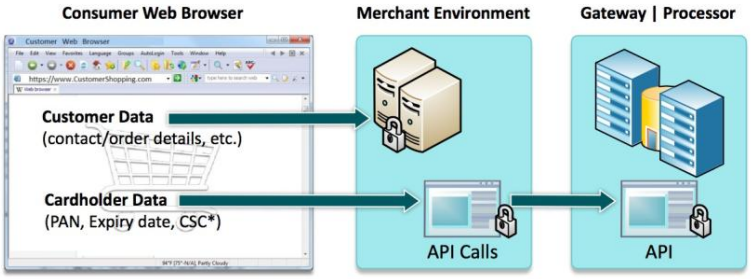


* Card Verification Code or Value/Card Security Code (CAV2, CVC2, CVV2, CID)

3.4.2 Merchant-managed Commercial Shopping Cart/Payment Applications

E-commerce implementations that incorporate a commercial shopping cart/payment application are similar to the previous case (Proprietary/Custom Developed), except that the payment functionality is delivered through commercially available software used in the merchant's site (the "payment application"). Such payment applications are developed and licensed for commercial use. See detailed explanation for "shopping carts" above (Section 3.3.1). See Figure 3 below.

Figure 3: Merchant-managed Payment Application



* Card Verification Code or Value/Card Security Code (CAV2, CVC2, CVV2, CID)

3.4.3 Shared-management E-commerce Implementations

Shared-management e-commerce implementations are those where the merchant maintains responsibility for some elements of the e-commerce infrastructure. For example, where the e-commerce implementation requires an application or code to be installed onto or delivered through the merchant's site, the merchant will be responsible for properly implementing and maintaining that code and for the security of the server on which the code resides, etc. Three common types of third-party provided e-commerce implementations are discussed below:

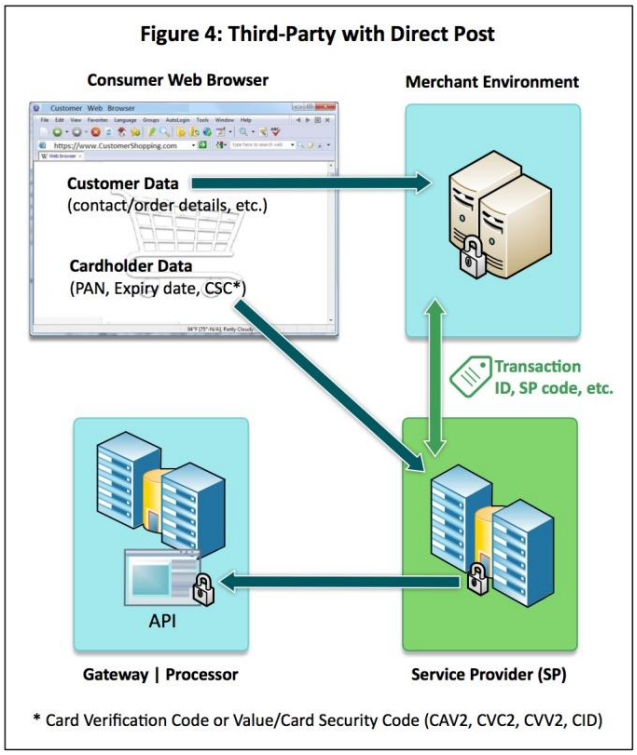
- Embedded APIs with direct post
- Inline frames
- Hosted payment pages

PCI DSS Scoping Guidance: Merchants should understand that outsourcing to a third party via a shared-management implementation does not allow the merchant to outsource PCI DSS responsibility, regardless of whether a merchant is eligible to complete a self-assessment questionnaire (SAQ). With each of these shared-management implementations, there is still security risk for the merchant since weaknesses on the merchant's website can lead to compromise of the payment card data during the transaction process. See "Security Considerations for Shared-Management E-commerce Implementations" on page 17 for risks specific to each implementation. Due to these risks to a merchant's website and payment card data, even in outsourced scenarios, it is recommended that merchants implement applicable PCI DSS controls as needed to ensure the security of the website.

3.4.3.1 Third-Party Embedded APIs with Direct Post

One popular third-party approach is to use application programming interfaces (APIs) licensed to the merchant by the e-commerce payment processor. In this implementation, the merchant hosts a web application using third-party APIs that redirect the payment data from the consumer's browser directly to the e-commerce payment processor. These APIs allow the merchant to send code from its web page to the consumer's browsers ("client-side" code) so that when card data is entered into designated fields, the consumer's browser posts the payment card data directly to the e-commerce payment processor instead of passing that data back to the merchant's web application infrastructure. The e-commerce payment processor accepts the payment card data from the consumer and passes a confirmation code (ID number, token, etc.) back to the merchant's web application. To complete the transaction, the merchant's application sends the code back through the e-commerce payment processor who retained authentication data specific to this transaction, and uses it to finalize authorization. See Figure 4 on the following page.

Alternatively, the e-commerce payment processor accepts cardholder data from the consumer and simply passes information back to the merchant, noting whether the transaction was successful. If successful, the merchant can complete the workflow for the consumer's purchase.



3.4.3.2 Third-party Inline Frames

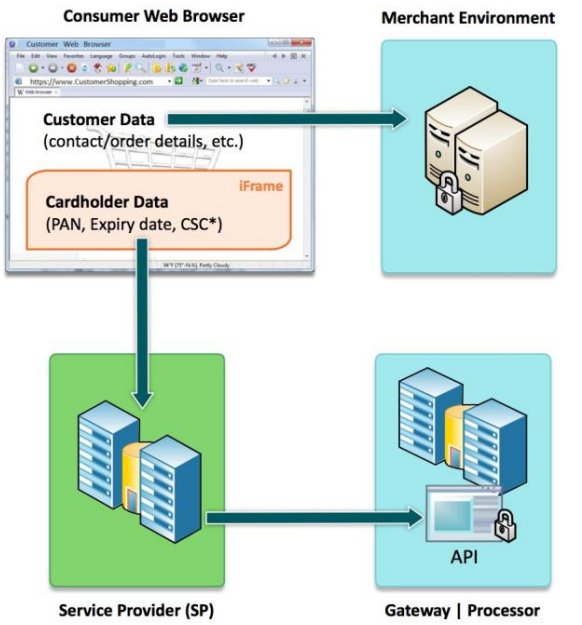
Inline frames or “iFrames” allow a web page to be embedded within another web page. The iFrame becomes a frame for a link to another page. A common e-commerce implementation is to accept card payments via an e-commerce payment processor’s hosted web pages. These web pages can be as simple as a short form containing only the fields necessary to process a payment transaction. The merchant’s web application then embeds the e-commerce payment processor’s web payment page as an inline frame so that it appears as part of the merchant’s page. When data is entered into the payment page, it is posted directly to the e-commerce payment processor’s web application server instead of the merchant’s. See Figure 5 on the following page.

There may be an additional third party between the merchant and the iFrame e-commerce payment processor. For example, a merchant may link to a third party that maintains inventory or other information, and that third party hosts the iFrame and posts to the e-commerce payment processor. This iFrame host is transmitting and processing (and possibly storing) cardholder data, and both service providers in this scenario can affect the security of the transaction. In this implementation, the merchant should consider both third parties—the intermediate party hosting the iFrame and the third-party processor who provides the iFrame—to be service providers for the merchant, and the merchant should monitor the PCI DSS compliance of both third parties. Best practices for third parties in Section 5.4 should be considered for all third parties that support iFrames.

Additional best practices for iFrames include:

- iFrames should be developed securely to ensure that unauthorized code is not executing inside of the iFrame.
- iFrames should not expose internal network address ranges.
- iFrames should be configured to prevent clickjacking (this occurs with when a user is tricked into performing unsecure actions by clicking on hidden links within a browser).

Figure 5: iFrames

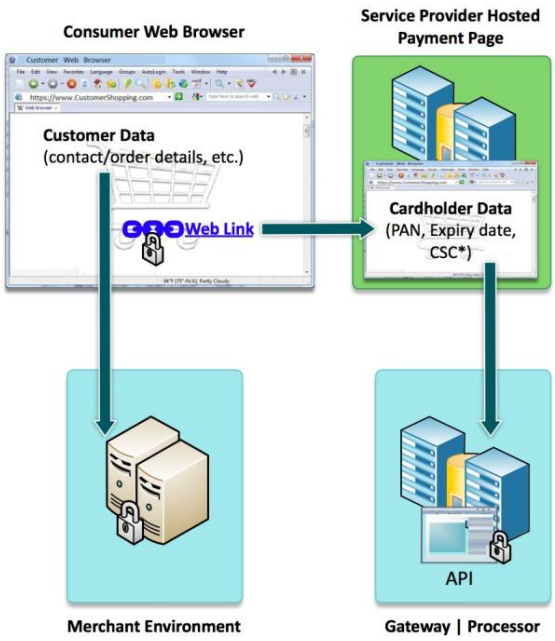


* Card Verification Code or Value/Card Security Code (CAV2, CVC2, CVV2, CID)

3.4.3.3 Third-Party Hosted Payment Page

E-commerce implementations that incorporate a hosted payment page take the iFrame approach (described previously) one step further. Instead of embedding the e-commerce payment processor's payment page in a frame on the merchant's web page, the merchant's customer is redirected to the payment page on the e-commerce payment processor's site to enter payment card data. Once payment is processed, acknowledgement is sent back to the merchant's web application. See Figure 6 below.

Figure 6: Hosted Payment Page



* Card Verification Code or Value/Card Security Code (CAV2, CVC2, CVV2, CID)

3.4.3.4 Security Considerations for Shared-Management E-commerce Implementations

As mentioned above, for each of these shared-management implementations, there is a security risk for the merchant since weaknesses on the merchant's website can lead to compromises of payment card data during the transaction process.

- *Direct-post API Approach:* With the direct-post API approach, the merchant is still responsible for the web page that is presented to the consumer, and the merchant hosts the fields on the payment page that accept the data—only the cardholder data is posted directly from the consumer to the service provider. Since the payment pages are hosted by the merchant, the payment pages are only as secure as the merchant's web site, and a compromise of the merchant's system could lead to a compromise of payment card data.
- *iFrame Approach:* With the iFrame approach, the iFrame must be configured and managed to prevent it from being modified to send cardholder data to an alternate and unauthorized source.

- *Hosted-payment Page Approach:* With hosted payment pages, a compromise of the merchant's server could lead to redirection of communications intended for the e-commerce payment processor, allowing payment card data to be intercepted and stolen as transactions occur.

Specifically, for all of the above scenarios, the merchant should monitor for any evidence that systems have changed and respond quickly to restore systems to a trusted state when unauthorized changes are detected. Merchants who adopt these shared-management outsourced models to minimize applicable PCI DSS requirements should be aware of the potential risks that are inherent to these types of system architecture. To minimize the chance of attack in these scenarios, merchants should apply extra due diligence to ensure the web application is developed securely and undergoes thorough penetration testing.

3.4.4 Wholly-outsourced E-commerce Implementations

Many merchants are interested in managing their PCI DSS responsibility by outsourcing all cardholder data storage, processing, and transmission to a third party hosting provider or e-commerce payment processor. In this case, merchants may elect to use a solution provided and hosted by a third party, which is wholly under the control and responsibility of the third party. This type of solution could consist of an e-commerce application, hosted servers, and hosted infrastructure, which are all provided and managed by the third party. A web interface is provided for the merchant to access the third-party site, and to manage the e-commerce store and customers.

PCI DSS Scoping Guidance: In this scenario, the merchant may be eligible for the *PCI DSS Self-Assessment Questionnaire (SAQ) A.* SAQ A reduces the number of applicable PCI DSS requirements for merchants that outsource all storing, processing, and transmitting of cardholder data to an e-commerce payment processor. More information about SAQ A can be found below under "Outsourced e-commerce Implementations and SAQ A."

Note that if the merchant has to install an application or code on a server, configure a server file, etc. for their e-commerce implementation, they should refer to Section 3.4.3, "Shared-management E-commerce Implementations," above.

3.4.5 Outsourced E-commerce Implementations and SAQ A

If a merchant is eligible to use an SAQ as a PCI DSS validation tool and has outsourced all payment card data storage, processing, and transmission to compliant third parties (for example, merchants using a wholly outsourced e-commerce implementation as described in 3.4.4), the merchant may be eligible to complete SAQ A which reduces the number of applicable PCI DSS requirements for the merchant. Merchants should consult with their acquirer(s) or the payment brands about individual PCI DSS compliance validation requirements and whether they are eligible to use an SAQ as a validation tool.

Outsourcing and manually entering payment data: Is SAQ A still applicable?

Many merchants outsource their e-commerce transactions to a PCI DSS compliant service provider, and they expect to qualify to use SAQ A. However, in many cases merchants find that they need to continue to process card-present, fax, or mail order/telephone order (MOTO) transactions. For customer-service purposes (e.g., when a consumer's Internet access is unavailable), it is not uncommon for staff at merchant locations to use their existing workstations to access the merchant's hosted order page and manually enter the transaction for the consumer. In some cases, the service provider may create a separate payment page to accommodate this activity.

The result is that these workstations effectively become "virtual terminals" when staff use them to enter transactions into a form on a web page either manually or, if the cardholder is present, by swiping or dipping a payment card through a card reader ("wedge") that is connected to the workstation.

Merchants that accept card-present transactions do not qualify for SAQ A, nor do merchants that have electronic cardholder-data storage, processing, or transmission within their facilities. They may have extensive PCI DSS scope as a result of manually entering payment data in this manner, and may not qualify to use any of the shorter SAQs. To reduce scope for the e-commerce environment in this scenario, consider segmenting the workstations used to manually enter payment data from the rest of the merchant's e-commerce processing environment, at a minimum. Such merchants should consult with their QSAs and/or their acquirers (merchant banks) to determine whether they are eligible for an SAQ and, if so, to determine which SAQ is applicable.

3.5 E-commerce Roles and Responsibilities

Roles and responsibilities for an e-commerce solution may be distributed as follows:

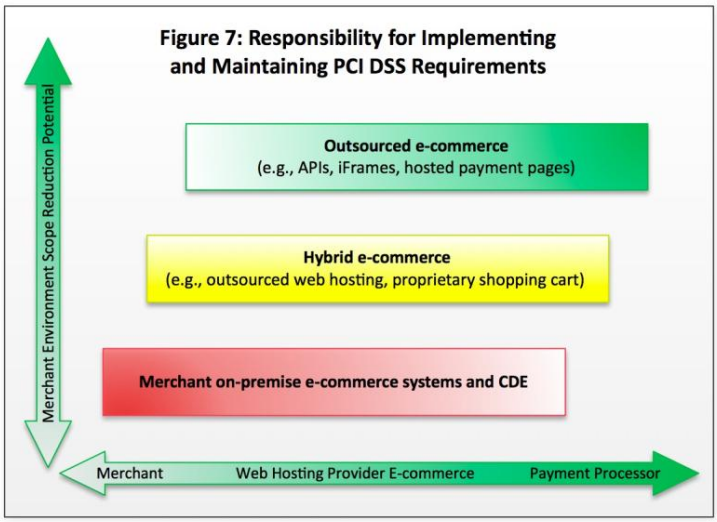
- In-house solution: The merchant manages all e-commerce components within its own IT infrastructure.
- Outsourced solution: The merchant outsources the management and hosting of all e-commerce components to a web hosting provider and/or an e-commerce payment processor.
- Hybrid solution: The merchant hosts and manages some e-commerce components while outsourcing others.

With an in-house e-commerce solution, the merchant maintains control over all components of the e-commerce system. In this scenario, the merchant is fully responsible for complying with all applicable PCI DSS requirements.

For an outsourced or hybrid e-commerce solution, responsibility for meeting PCI DSS requirements is shared

in varying degrees between the merchant and the service provider(s). However, the merchant is ultimately responsible for ensuring that each service provider protects the integrity and confidentiality of the payment card data that is being stored, processed, or transmitted on the merchant's behalf.

Figure 7 provides an example of how responsibilities may differ between a merchant and their service providers, depending upon how the solution is designed and managed.



Note: *Some PCI DSS requirements will apply to the merchant regardless of whether an e-commerce solution (or portions of an e-commerce solution) is outsourced. For example, PCI DSS controls apply wherever payment card data is processed, stored, or transmitted—such as at the point of capture or during transmission to a third party. Additionally, the merchant is required to implement and maintain policies and procedures to manage service providers: whenever cardholder data is shared; if the service provider is storing, processing, or transmitting cardholder data on behalf of the merchant; or if the service provider may have any impact on the security of the CDE.*

Who is a service provider? How do I know if the service provider is PCI DSS compliant?

A service provider is defined in the PCI DSS Glossary v2.0 as a:

> *Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services 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.*

Based upon this definition, a company that does not store, process, or transmit cardholder data may still be classified as a service provider. In this situation, if the entity has the capacity to "impact the security of cardholder data" it qualifies as a service provider and should be PCI DSS compliant. Examples of such service providers would include co-location facilities and document disposal (shredding) and storage companies.

As explained in PCI DSS, third-party service providers can validate their compliance by either: 1) undergoing a PCI DSS assessment on their own and providing evidence of compliance to their customers, or 2) including their services for review in each of their customers' PCI DSS assessments.

If the service provider has undergone its own PCI DSS assessment, the merchant's assessor will need to verify that the service provider's validation is current, that the assessment covered all services provided to or used by the merchant, and that all applicable requirements were found to be in place for the environment and systems in scope.

The questions below will help merchants identify how roles and responsibilities are distributed within e-commerce solutions and thereby understand who is responsible for maintaining compliance with individual PCI DSS requirements:

- Did the merchant develop its own proprietary code or purchase a commercial shopping cart?
  - Responsibility for the security of the code belongs to the developer.
  - Determines whether PA-DSS applies as a requirement for vendor-developed code or as a best practice for merchant-developed code.
- What components are managed by third party(s)?
  - Applicable PCI DSS requirements for these components are the responsibility of the third party.
- Which components are managed, installed, configured, etc. by the merchant?
  - Applicable PCI DSS requirements for these components are the responsibility of the merchant.
- How and where is cardholder data collected and transmitted? *Note: the answer to this question is specific to an e-commerce implementation, per above.*
  - Determines the parties and infrastructure components that are storing, processing or transmitting cardholder data.

As an example, if a merchant outsources the servers that host the e-commerce system to a web hosting/cloud provider, the provider would be responsible for ensuring that PCI DSS controls are applied and maintained in the environment where the servers are located. If the merchant also outsources the e-commerce application to an e-commerce payment processor, the e-commerce payment processor would be responsible for PCI DSS and/or PA-DSS requirements related to the shopping cart application and its functions.

Merchants planning to use an outsourced or hybrid e-commerce solution for their cardholder data environment (CDE) should ensure that they thoroughly understand the details of the solution being offered, including performing a detailed assessment of the potential risks associated with using the solution. Whether the roles and responsibilities are distributed among numerous organizations or combined within a single organization, the responsibilities for PCI DSS requirements—and any other controls that could impact the security of cardholder data—must be clearly defined between the parties involved and documented in a formal agreement (per PCI DSS Requirement 12.8), such as a contract or service-level agreement. See "Address Risks Associated with Outsourcing to Third-Party Service Providers" in Section 5.4 for more details.

Appendix B: Merchant and Third Party PCI DSS Responsibilities provides a checklist that merchants and service providers can use to document their respective responsibilities.

Table 1: Summary of Roles and Responsibilities for Common E-commerce Implementations

E-commerce Implementation	Roles / Responsibilities	
	Merchant	**Hosting Provider and/or e-commerce payment processor**
Merchant managed e-commerce implementations, including shopping cart/payment application (either proprietary/custom developed or commercial) Merchant develops or purchases software, implements and manages own e-commerce environment, including data center, typically sends payment to e-commerce payment processor. Merchant may outsource its data center to a hosting provider and/or send payment data to e-commerce payment processor.	Merchant has complete responsibility for PCI DSS requirements of their e-commerce environment. Responsibilities include: • Ensuring secure development of merchant-developed software • Confirming PA-DSS validation of third-party payment applications • Having written agreements with any third parties and ensuring that cardholder data (CHD) is protected in accordance with PCI DSS.	Any hosting providers, payment processors, or other third parties used by merchants should adhere to and validate compliance with applicable PCI DSS requirements, and provide adequate proof of compliance to their merchant customers.
Shared-management e-commerce implementations: Third-party embedded application programming interfaces (APIs) with Direct Post. Merchant website uses APIs licensed from an e-commerce payment processor to redirect payment data from the consumer's browser directly to the e-commerce payment processor, bypassing the merchant's web page.	Merchant still has responsibility for PCI DSS requirements for some elements of the e-commerce infrastructure even though they have outsourced much PCI DSS responsibility for storage, processing, and transmission of cardholder data. This is because compromise of the merchant's website may result in compromise of the API, which could allow compromise of CHD. Merchant is responsible for: • Managing website and servers (if self-hosted), including applicable PCI DSS requirements • If website/server hosting is outsourced, applicable PCI DSS requirements for management of third parties (e.g., Requirement 12.8) • Having written agreements with any third parties and ensuring they protect cardholder data on behalf of the merchant, in accordance with PCI DSS • Securing the web page(s) containing API code and/or function(s).	Any hosting providers, payment processors, or other third parties used by merchants should adhere to, and validate compliance to, applicable PCI DSS requirements, and provide adequate proof of compliance to their merchant customers. E-commerce payment processor should provide instruction and guidance to the merchant for secure implementation and practices for the API on the merchant's web site.

E-commerce Implementation	Roles / Responsibilities	
	Merchant	**Hosting Provider and/or e-commerce payment processor**
Shared-management e-commerce implementations: iFrames The payment processor's payment page is embedded into the merchant's web page as a separate but transparent "frame," such that consumer's payment data is submitted directly to the e-commerce payment processor; bypassing the merchant's web page.	Merchant still has responsibility for PCI DSS requirements for some elements of the e-commerce infrastructure even though they have outsourced much PCI DSS responsibility for the storage, processing and transmission of cardholder data. This is because compromise of the merchant's website may result in a compromise of the iFrame, which could allow compromise of CHD. Merchant is responsible for: ▪ Managing website and servers (if self-hosted), including applicable PCI DSS requirements ▪ If website/server hosting is outsourced, applicable PCI DSS requirements for management of third parties (e.g., Requirement 12.8) ▪ Having written agreements with any third parties and ensuring that they protect cardholder data on behalf of the merchant, in accordance with PCI DSS ▪ Securing the web page(s) containing the iFrame code.	Any hosting providers, payment processors, or other third parties used by merchants should adhere to, and validate compliance to, applicable PCI DSS requirements, and provide adequate proof of compliance to their merchant customers. E-commerce payment processor should provide instruction and guidance to the merchant concerning secure implementation and practices for the iFrame.
Shared-management e-commerce implementations: Third-party hosted payment pages Merchant's website redirects consumer's browsers to an e-commerce payment processor's website; consumer enters payment directly into the e-commerce payment processor's website.	Merchant still has responsibility for PCI DSS requirements for some elements of the e-commerce infrastructure even though they have outsourced much PCI DSS responsibility for storage, processing and transmission of cardholder data. This is because compromise of the merchant's website may result in compromise of the redirection mechanism, leading to compromise of CHD. Merchant is responsible for: ▪ Managing website and servers (if self-hosted), including applicable PCI DSS requirements ▪ Applicable PCI DSS requirements for managing third parties, (e.g., Requirement 12.8) ▪ Having written agreements with any third parties and ensuring they protect cardholder data on behalf of the merchant, in accordance with PCI DSS. ▪ Securing the web page(s) containing the redirection code and/or function(s).	Any hosting providers, payment processors, or other third parties used by merchants should adhere to, and validate compliance to, applicable PCI DSS requirements, and provide adequate proof of compliance to their merchant customers. E-commerce payment processor should provide guidance to merchant for secure implementation and practices for the redirection mechanism.

E-commerce Implementation	Roles / Responsibilities	
	Merchant	**Hosting Provider and/or e-commerce payment processor**
Wholly outsourced e-commerce implementations	Merchant has outsourced maximum PCI DSS responsibility for storage, processing and transmission of cardholder data. Merchant responsible for: ▪ Applicable PCI DSS requirements for managing third parties, (e.g., Requirement 12.8) ▪ Having written agreements with any third parties and ensuring they protect cardholder data on behalf of the merchant, in accordance with PCI DSS ▪ Ensuring that the outsourced/hosted environment receives a passing score from an appropriate ASV scan on a quarterly basis.	Any hosting providers, payment processors, or other third parties used by merchants should adhere to, and validate compliance to, applicable PCI DSS requirements, and provide adequate proof of compliance to their merchant customers. If a web-based interface/customer portal is provided for the merchant to manage their e-commerce store, customers, etc., the third-party should provide usage instruction and guidance to the merchant.

4 Common Vulnerabilities in E-commerce Environments

While e-commerce introduces many advantages, it also introduces unique risks and challenges. Web application vulnerabilities are one of the most common sources of data compromise. Therefore it is important for merchants to emphasize security when developing or selecting e-commerce software and services.

According to the Open Web Application Security Project (OWASP[1]):

> "Insecure software is already undermining our financial, healthcare, defense, energy, and other critical infrastructure. As our digital infrastructure gets increasingly complex and interconnected, the difficulty of achieving application security increases exponentially. *We can no longer afford to tolerate relatively simple security problems like those presented in the OWASP Top 10*." (Italics added.)

Industry best practices for vulnerability management—such as the OWASP Top 10, SANS[2] CWE Top 25, and CERT[3] Secure Coding—should be applied by e-commerce application/web developers. Merchants that purchase e-commerce applications should confirm that the application is validated according to PA-DSS. Merchants that develop their own e-commerce solutions should refer to PA-DSS as a best practice and/or confirm that the developer has knowledge of (and applies) strict and secure application coding/development practices.

[1] www.owasp.org
[2] www.sans.org
[3] www.cert.gov

4.1 Vulnerabilities Caused by Insecure Coding Practices

Some common vulnerabilities in web applications (such as e-commerce shopping carts) can be categorized as follows:

4.1.1 Injection Flaws

In addition to SQL injection, this category includes OS and LDAP injection. These flaws occur when data input to a website (for example, into a form or field) is not properly validated by the application code, and results in the injection of potentially malicious data to execute commands that may result in unauthorized access.

One of the most important items to request of an e-commerce service provider is a description of the security controls and methods it has in place to protect websites against SQL injection vulnerabilities.

Note that SQL injection flaws have been common knowledge for over a decade; while mitigating these vulnerabilities only requires simple, prudent coding practices, SQL injection continues to be one of the most common methods by which e-commerce websites are compromised.

4.1.2 Cross-site Scripting (XSS)

Also the result of poor application-level input validation practices, XSS allows an attacker to place code in the victim's browser to hijack the browser session and/or redirect the victim to a malicious website.

4.1.3 Cross-site Request Forgery (CSRF)

This website exploit allows unauthorized commands to be transmitted unwittingly by a trusted user/session. CSRF forces the victim's browser to send a forged HTTP request to a website, tricking the website to believe the victim's forged request is legitimate.

4.1.4 Buffer Overflows

A buffer overflow occurs when an application attempts to store more data in a buffer (temporary data storage area in the system's memory) than it was designed to hold. If an application lacks proper input validation, excess data may be permitted to overflow into adjacent buffers, which can corrupt or overwrite valid data. The extra data may also contain malicious code designed to trigger specific actions, such as sending new and unauthorized instructions to the compromised computer. A buffer overflow can modify system configurations, damage files, and change or disclose confidential data.

4.1.5 Weak Authentication and/or Session Credentials

Attackers often target vulnerable browser sessions, weak passwords, exposed protocols and services, and attempt to enumerate accounts, particularly administrative or service accounts with privileged access.

4.2 Security Misconfigurations

Secure configurations must be defined and applied to the entire e-commerce environment, including: servers, applications, network components (e.g., routers and firewalls), and logging/monitoring mechanisms. Commonly exploited vulnerabilities include weak or unchanged vendor default passwords and system

settings, and insecure remote access settings. Security configuration areas addressed in PCI DSS include:

- Secure configuration of the DMZ to limit inbound traffic to only those components intended to provide authorized, publicly accessible services, and to prohibit unauthorized outbound traffic (PCI DSS Requirements 1.3.1 and 1.3.4)
- Secure system configuration and changing vendor-supplied default passwords and settings (PCI DSS Requirement 2)
- Using secure encryption mechanisms when transmitting data over the Internet (PCI DSS Requirement 4)
- Protecting e-commerce components from known malware (PCI DSS Requirement 5)
- Keeping all software and network components up to date with vendor-supplied patches (PCI DSS Requirement 6.1)
- Using secure software development and coding practices for websites (PCI DSS Requirements 6.3 – 6.5)
- Implementing a process to address new security vulnerabilities (PCI DSS Requirements 6.1, 6.2, 6.6 and 11.2)
- Limiting access to only those users with a need to know and requiring strong authentication credentials for those with access (PCI DSS Requirements 7 and 8)
- Logging and monitoring (PCI DSS Requirements 10 and 11)

5 Recommendations

In addition to complying with PCI DSS, e-commerce merchants should consider implementing some or all of the security best practices noted in this section.

5.1 Know the Location of all Your Cardholder Data

Data-flow diagrams provide an important aid to understanding the scope of the cardholder data environment by showing the actual flow of cardholder data as it is being transmitted across various networks and systems. Periodic review will ensure accuracy as changes to the environment may occur.

A well-designed data flow diagram will:

- Identify each system involved in the storing, processing and transmission of cardholder data (CHD)
- Identify any system connected to the systems which store, process or transmit cardholder data
- Illustrate how cardholder data is processed, for example, how CHD is managed within a web application's functionality and pages, along with how the data flows within a network or across multiple networks
- Illustrate where security controls are implemented
- Illustrate and make a clear distinction between payments processed under the merchant's responsibility (whether developed internally or purchased from a third party and integrated with a shopping cart) vs. payments processed solely within third party environments.

5.2 If You Don't Need It, Don't Store It

Eliminating any cardholder data that is not needed per PCI DSS Requirement 3.1, consolidating necessary cardholder data in known and manageable locations, and isolating all cardholder data away from non-cardholder environments may reduce the number of locations and amount of cardholder data that require protection, as well as the number of access points to the CDE that need to be secured.

5.3 Evaluate Risks Associated with the Selected E-commerce Technology

Entities should thoroughly and carefully evaluate the risks associated with each e-commerce solution prior to selecting or implementing one. Whether an e-commerce solution is fully hosted and managed by the merchant, or is partially or fully outsourced to a third party results in different levels of risk for the merchant.

The flow and storage of cardholder data should be accurately documented as part of this risk assessment process to ensure that all components and third parties are identified and properly secured or managed. Once implemented, e-commerce environments should be included in an organization's annual risk-assessment process.

5.4 Address Risks Associated with Outsourcing to Third-party Service Providers

Security is a critical element for any website, shopping cart or other e-commerce service. The following best practices are offered for consideration when outsourcing any component of a merchant's e-commerce environment to third parties.

When evaluating potential services from third parties, e-commerce merchants should consider the following:

- Request quotes from multiple service providers in order to gain familiarity with the basic elements of a service offering and to learn about the available optional features.
- Ask for a description of security services. A company capable of supporting payment services should be able to describe their security capabilities in clear, non-technical terms and offer security as a part of their basic service.
- Buy payment services from an e-commerce service provider that can provide references from financial institutions or other payment service companies. Handling payments securely requires experience.
- Research prospective providers; there are numerous resources available online that provide customer reviews, service provider ratings, and even security breach history.

When engaging with service providers, merchants should have a contract or written agreement that:

- Specifies the responsibility for compliance with PCI DSS requirements for both the merchant and the service provider (per PCI DSS Requirement 12.8).
- Indicates how they meet applicable PCI DSS requirements.
- Identifies whether the service provider will undergo its own PCI DSS compliance validation or will support the merchant's PCI DSS assessment each year for the services provided by the service provider.

When managing third-party service providers, merchants should consider the following:

- If outsourcing web-hosting services, ask the provider for standard hardware and software configurations, a defined schedule for updating hardware and software patches and versions, a 7x24x365 active monitoring service, and support for investigations in the event of a security breach.
- If outsourcing data storage services, verify whether the service provider can independently manage encrypted backups and database administration. Clarify these features in the agreement or contract, along with appropriate PCI DSS controls as applicable.
- If a service provider's network infrastructure and processes have not been assessed for PCI DSS compliance, the service provider may find it difficult or costly to remediate identified security issues. When outsourcing environmental or network infrastructure, agree which company will pay to remediate such security issues before signing an agreement or contract.
- Review third parties' signed Attestations of Compliance (AOC) to confirm their compliance status is current (like merchants, service providers should validate PCI DSS compliance annually), and that the services being provided to the merchant are covered by the service provider's PCI DSS assessment.
- Verify that the service provider's PCI DSS assessment identifies them as a service provider (not as a merchant).
- Merchants hosted within a shared environment (i.e., more than one merchant's website is hosted on a common server) should note that shared hosting providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers,* in addition to all other applicable PCI DSS requirements. Confirm that the PCI DSS assessment of a shared hosting provider includes all applicable requirements.

5.5 ASV Scanning of Web-hosted Environments

PCI DSS Requirement 11.2 for external and internal vulnerability scanning applies to e-commerce websites because they are part of the cardholder data environment. When a merchant outsources website hosting and/or management to a third-party hosting provider, the merchant may not have control over the scanning process. The following best practices apply to merchants using third-party web hosting:

- Ensure that ASV scanning is being carried out as specified by PCI DSS Requirement 11.2.
- If a merchant's e-commerce site is hosted in a shared environment (more than one merchant's website on the same server), there are two options available for scanning:
  - The hosting provider can undergo ASV scans on their own and provide evidence of compliant scans to the merchant; or
  - The hosting provider can undergo an ASV scan as part of each of their merchant's ASV scans.
- Ultimately, it is the merchant's responsibility to ensure their hosted environment receives a passing result on a quarterly basis from appropriately scoped ASV scans.

5.6 Best Practices for Payment Applications

- Use SSL/TLS when transmitting cardholder data internally (for example, at cardholder data ingress and egress points) within the merchant's network.
- Due to the dynamic nature of e-commerce environments and frequent changes to websites and web applications, and as traditional firewalls may not have the capability to inspect the contents of encrypted network traffic, consider implementing a web-application firewall (WAF) or additional intrusion-detection technologies.
- Follow PA-DSS when internally developing and implementing payment applications/shopping carts to help ensure that the application will support PCI DSS compliance.
- Consider using third-party payment applications that are PA-DSS validated and noted on the list of Validated Payment Applications as "acceptable for new deployments" (see the PCI Council website for the current list of Validated Payment Applications).
  - Note that some payment brands require the use of PA-DSS validated payment applications where third-party payment applications are in use. Merchants should consult with their acquirers or the payment brands to understand applicable requirements.
  - The correct installation of a payment application is critical to the protection of payment card data. The payment application's *PA-DSS Implementation Guide* (obtained from the payment application vendor) should be followed when installing and configuring the payment application to ensure that the product is implemented in a manner that supports PCI DSS compliance.
- Regularly review any links (such as URLs, iFrames, APIs etc.) from the merchant's website to a payment gateway to confirm the links have not been altered to redirect to unauthorized locations.

5.7 Implement Security Training for all Staff

- Ensure all staff are trained to use systems securely and to follow defined procedures. Training should include awareness of potential security threats and the appropriate action to take in the event of a suspected breach.
- Train technical staff to properly manage security including firewalls, digital certificates, and SSL encryption.
- Train all internal staff to be aware of general security issues such as social engineering techniques used by unauthorized individuals to gain access to areas with cardholder data.

5.8 Other Recommendations

- Assign a specific team member(s) to monitor and report on any and all security alerts issued by the card brands and other security websites to stay current on emerging threats.
- Consider implementing an additional firewall between the application server and the database server to further reduce risks from the Internet-connected web server.
- Limit displays of account numbers to the minimum necessary for the consumer to complete their purchase. For example, once the account number is verified, don't display the full number back to the consumer in the order summary or receipt.

5.9 Best Practices for Consumer Awareness

Provide awareness for consumers to protect their payment card data when making online purchases. Examples of such guidance could include:

- Don't use public, untrusted computers for e-commerce transactions. Public computers may not be secure and could be capturing payment card data as it is being entered.
- Don't make purchases when connected to an unsecured wireless network (for example, using your laptop computer with a public WiFi connection), unless you have a personal firewall on your computer.
- Be aware of "shoulder-surfing" if entering payment card data in a public location.
- Keep personal computers up-to-date with security patches.
- Always ensure your computer is running anti-virus software that is updated with the most recent virus signatures and definitions before connecting to the Internet.
- Always check for signs of a secure web page, for example, look for the "HTTPS" prefix in the web address or the little "padlock icon" at the top or bottom of the web browser, a green address bar, or a security seal before entering payment card data.
- Use strong passwords that cannot be easily guessed (for example, don't use your date of birth or your name as a password).
- Keep your passwords private. For example, don't write them on a piece of paper attached to your computer (especially if you are in a public place), and don't save them in a file on a computer that is shared with others.

5.10 Resources

Organizations should familiarize themselves with industry-accepted best practices and guidelines for securing e-commerce environments. There are a wide range of resources at varying levels of depth and technical detail. Examples of resources that may provide guidance and technical security data breach reports include:

5.10.1 Information Security Resources

Information security resources provide an in-depth review of topics important to e-commerce, such as secure application development, analysis of attack patterns, and alerts on emerging threats:

- **Open Web Application Security Project (OWASP)** (www.owasp.org). OWASP is a global not-for-profit charitable organization focused on improving the security of web applications. OWASP's mission is to make application security visible so that individuals and organizations worldwide can make informed decisions about the true risks surrounding application development and security. OWASP provides a number of resources for training and application security awareness, including: podcasts, eBooks, online publications, news feeds, blogs, videos, conferences, and in-person classroom training.

  The *OWASP Development Guide* is a comprehensive reference manual for designing, developing, and deploying secure web services and applications. Individual guides include *Handling E-Commerce Payments*, *Security of Payment cards (Credit/Debit) in E-commerce Application*, and *Cornucopia E-commerce Web Site Edition*.
- **The SysAdmin, Audit, Network, and Security (SANS) Institute** (www.sans.org). The SANS Institute is a privately held, U.S. company providing information security resources, training, and certifications, as well as operating the Internet's early warning system—the Internet Storm Center. SANS develops, maintains, and makes available (at no cost) a large collection of research documents about various aspects of information security. SANS learning formats include instructor-led training, webinars, and blogs.
- **The Computer Emergency Response Team Coordination Center (CERT-CC)** (www.cert.org). CERT-CC is the global coordination center for information relating to security vulnerabilities and is run by the Software Engineering Institute at Carnegie Mellon University. Software developers can test code for conformance to CERT secure coding standards by using the CERT Program's Source Code Analysis Laboratory (SCALe). CERT offers learning opportunities in information security through Carnegie Mellon University and through CERT training courses.
- **The Center for Internet Security (CIS)** (www.cisecurity.org). CIS is a not-for-profit organization focused on enhancing cyber security readiness and response. In addition to hardening guides, daily tips, bi-monthly webcasts, and an Awareness Toolkit, CIS provides a list of products that were awarded CIS Security Benchmarks certifications.
- **ISACA** (previously known as the Information Systems Audit and Control Association) (www.isaca.org). ISACA is a nonprofit, independent membership association and a global provider of knowledge, certifications, community, advocacy and education covering information systems assurance, control and security, enterprise governance of IT, and IT-related risk and compliance. ISACA-administered certification programs include the Certified Information Systems Auditor

(CISA) and Certified Information Security Manager (CISM) designations. ISACA's learning formats include conferences, webinars, online certification courses, chapter review sessions, virtual conferences, and symposiums both live and online. ISACA also offers a broad view of the challenges associated with e-commerce in its book: *e-Commerce Security: A Global Status Report.*

5.10.2 PCI SSC Resources

The PCI Council publishes resources such as FAQs, guidance documents, and Information Supplements to assist merchants, service providers, and assessors with a variety of PCI-related information security initiatives. This e-commerce Information Supplement builds upon, and is supported by, a number of the resources provided by the PCI Security Standards Council. The following list is a sample of PCI SSC documents relevant to various technologies and PCI DSS requirements that may be particularly pertinent to e-commerce merchants. These documents (and many others) can be found in the Document Library on the PCI SSC's website:

- ***PCI DSS Virtualization Guidelines*** – Provides additional guidance on virtualization and how these technologies may affect, and be affected by, PCI DSS.
- ***PCI DSS Cloud Computing Guidelines*** (available Q1 2013) – Provides additional guidance on cloud computing and how these technologies may affect, and be affected by, PCI DSS.
- ***PCI DSS Information Supplement: Application Reviews and Web Application Firewalls Clarified*** – Provides additional guidance on PCI DSS Requirement 6.6, which includes options to address common threats to cardholder data in web application environments (e.g., e-commerce).
- ***Qualified Integrators and Resellers (QIR)™ Program Guide*** – Provides an overview of the PCI SSC Qualified Integrators and Resellers Program operated and managed by PCI Security Standards Council. QIRs are organizations that are qualified by PCI SSC to implement, configure, and/or support validated PA-DSS validated payment applications on behalf of merchants and service providers. The quality, reliability, and consistency of a QIR's work provide confidence that the application has been implemented in a manner that supports the customer's PCI DSS compliance. See also the QIR Implementation Statement and QIR Implementation Instructions.
- ***Approved Scanning Vendors (ASV) Program Guide*** – Explains the purpose and scope of PCI DSS external vulnerability scans for merchants and service providers undergoing scans as part of validating PCI DSS compliance, and also provides guidance and requirements for ASVs who perform these scans
- ***PCI DSS/PA-DSS Glossary of Terms, Abbreviations, and Acronyms*** – Provides definitions of terms and acronyms commonly used throughout the PCI standards, programs and supporting documentation
- ***PCI DSS Guidance: Requirement 11.3 Penetration Testing*** – Provides additional guidance on PCI DSS Requirement 11.3, "Penetration Testing," which is different than the external and internal vulnerability assessments required by PCI DSS Requirement 11.2.

PCI SSC also provides a variety of training and educational resources to further security awareness within the payment card industry. These offerings include PCI Awareness, PCI Professional (PCIP), and PCI DSS training for Internal Security Assessors (ISA).

6 Acknowledgments

The PCI SSC would like to acknowledge the contribution of the E-commerce Special Interest Group (SIG) in the preparation of this document. The E-commerce SIG consists of representatives from the following organizations:

403 Labs, LLC.
Acertigo AG, Stuttgart, Germany
Australia and New Zealand Banking Group Limited (ANZ)
Bankalararası Kart Merkezi (BKM) A.Ş.
Best Buy
Bozzuto's Inc
British Telecommunications Plc.
Capita plc
CHS Inc.
Citi
Coalfire
Comsec Consulting
Contour Networks
ControlScan, Inc.
Crowe Horwath LLP
DSW Inc.
EE
Equens SE
Evans Resource Group
First Data
FishNet Security Inc.
Foregenix
Fortytwo
Groupement des Cartes Bancaires CB
Interac Association
International Card Processing Services Ltd
Internet Security Auditors
IPS
IQ Information Quality
JPMorgan Chase & Co.
Kilrush Consultancy Ltd.
Kingston Smith Consulting LLP.
Knowit Secure AB
KPMG, LLP
LivingSocial
Lloyds TSB Cardnet
Market America Inc.
Merchant Link
Microsoft Corporation
Modell's Sporting Goods
Nationwide Building Society
NBCUniversal Media, LLC.
NCC Group plc.
Overwaitea Food Group
Pen Test Partners LLP.
Privity Systems Inc.
Protiviti
Rapid7
Retail Decisions, Inc.
Security Risk Management Ltd
Sense of Security Pty Ltd
SIX Payment Services AG
Specsavers
SRC Security Research & Consulting GmbH
Symantec Corporation
Tesco Stores LTD.
The UK Cards Association
TouchNet Information Systems, Inc.
Venda
Verizon Enterprise Solutions
Voltage Security
Wind River Financial
WorldPay

7 About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement, and dissemination of the PCI Data Security Standard (DSS), PIN Transaction Security (PTS) Requirements, and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors, and point-of-sale vendors are encouraged to join as Participating Organizations.

Appendix A: PCI DSS Guidance for E-commerce Environments

The following section provides some high-level e-commerce guidance related to the main categories of PCI DSS requirements.

In general, PCI DSS requirements apply to e-commerce environments, for both the merchant and any e-commerce payment processors used by the merchant. To understand which PCI DSS responsibilities are those of the merchant and which are the responsibility of any e-commerce payment processor(s), a merchant should identify and document (for example, via a simple diagram) their e-commerce environment, including systems involved and the cardholder data that flows to third parties. Regardless of the e-commerce implementation used by a merchant and regardless of the extent of the responsibilities outsourced by the merchant to a third party, there is still a connection between the merchant and the e-commerce payment processor that can be compromised. Understanding their e-commerce environment and cardholder data flows will help the merchant as they periodically monitor their systems to ensure no unexpected changes have occurred.

Note: *This appendix is intended as guidance only. It is important to remember that* ***ALL applicable PCI DSS requirements must be evaluated****. The following guidance identifies only some of the potential areas to consider for e-commerce environments.*

The guidance in this appendix does not replace, supersede, or extend PCI DSS requirements. All best practices and recommendations contained herein are provided as guidance only.

PCI DSS Requirements		E-commerce Guidance
Build and Maintain a Secure Network	**1.** Install and maintain a firewall configuration to protect cardholder data	Firewalls are required between the web server and the public Internet, and also between the web server and the internal network where application and database servers reside. The firewall and DMZ configuration should ensure that only permitted traffic from the Internet is allowed to reach the web server, and that only necessary traffic from the web server is permitted into the internal “private” network. Internet connections should never be permitted to internal hosts or networks beyond the DMZ. System components that store cardholder data must be placed in an internal network zone, segregated from the DMZ and other untrusted networks.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	Outsourcing services introduces multiple levels of administrative access and potential CHD “touch points.” All responsible parties and system owners should be identified and documented. Consider use of Appendix B of this document to help understand and document each party’s responsibilities.

PCI DSS Requirements		E-commerce Guidance
Protect Cardholder Data	**3.** Protect stored cardholder data	Document all instances of CHD—and the security controls to protect it—while in storage, processing, and transit throughout the e-commerce environment, including CHD with hosting/service providers. Collect and retain only the minimal data required to complete the e-commerce transaction, and only for the minimum duration required per your business processes. Do not develop or permit e-commerce technologies that store CHD or other sensitive information unprotected in cookies or temporary files.
	4. Encrypt transmission of cardholder data across open, public networks	Transmissions of cardholder data over public networks (for example, the Internet) are required to be encrypted via SSL, VPN, or IPSec—for example, between the consumer and the merchant's web servers and/or hosted payment gateways, and/or between the merchant and various hosted service providers. Such encryption can also be used to protect communication of sensitive resources (such as login, and customer account/ profile pages), and to encrypt transmissions of cardholder data over the merchant's internal network. ***Note:*** *Traditional firewalls may not have the capability to inspect encrypted network traffic. If the destination address and port meets the criteria defined in the firewall's policy, the traffic is permitted. In order to inspect the contents of encrypted network traffic, a web application firewall (WAF) or intrusion detection technologies should be considered.* If your e-commerce solution offers "chat" or other messaging technologies, consider employing a warning banner or other notice to the customer (prior to initiating the session) to alert them to refrain from sending CHD over unprotected communication channels. For SOA implementations, ensure SSL/TLS (or other options per PCI DSS Requirement 4.1) is used to protect the channel for message-oriented middleware.

PCI DSS Requirements		E-commerce Guidance
Maintain a Vulnerability Management Program	**5.** Use and regularly update anti-virus software or programs	As new viruses and malware emerge daily—equipped with craftier methods to bypass security controls—it is imperative to update antivirus software frequently. The antivirus solution should be configured to log events including (but not limited to) antivirus software updates, success and failures, any suspicious or malicious software or system activity detected by the antivirus solution, and events associated with the software or alerting features being tampered with or disabled. Testing the anti-virus solution on non-production/test systems before deploying to production is a best practice to verify that anti-virus mechanisms do not interfere with e-commerce functions.
	6. Develop and maintain secure systems and applications	Shopping carts and other e-commerce payment applications should be PA-DSS validated and implemented according to the *PA-DSS Implementation Guide* (if a third-party application) or developed according to PA-DSS as a best practice (if internally developed). Secure web application coding and development practices help ensure the web application is not vulnerable to attack. Any proprietary or in-house developed e-commerce payment applications not validated to PA-DSS must be included in the scope of the PCI DSS assessment to ensure the application functions in a PCI DSS compliant manner. PA-DSS validated applications are also included in a PCI DSS assessment, to ensure that the application was properly installed and implemented according to the application's *PA-DSS Implementation Guide* and in a PCI DSS compliant manner. Ensure the latest versions of software are installed and that vendor patches are implemented promptly per PCI DSS Requirement 6.1, including shopping carts, web browsers, operating systems, and for SOA implementations, the latest versions of message-oriented middleware and the enterprise service bus.
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know	Minimize the number of staff who can view account data. Just because access to clear text account data is possible does not mean every—or even any—merchant staff need to see this data to perform their jobs. Many service providers do not provide merchant customers access to clear-text account data unless the merchant specifically requests such access. Ensure passwords for user accounts on all e-commerce components (including, but not limited to web applications, servers, and network architecture components like SOA) do not have system administrative privileges, and that all administrative access is limited to only those with administrative job functions.
	8. Assign a unique ID to each person with computer access	Don't use simple passwords such as "password123" or your store's name. Consider instead using passphrases consisting of two or more words that are meaningful but not easily guessable, using a combination of upper and lowercase, alphanumeric, and special characters.
	9. Restrict physical access to cardholder data	The merchant may not have access to physical environment when hosting with a third party; care should be taken to ensure agreements with third parties cover the physical security of their facilities. Be sure to destroy both electronic and paper media (e.g., printed reports showing account data) when no longer needed for business or legal reasons.

PCI DSS Requirements		E-commerce Guidance
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data	Logs from web servers and activity on the website can show potential suspicious behavior (for example, unauthorized content being added to forms). Monitor web server and shopping cart application logs, and responses to invalid input to ensure that routine and functional changes do not accidentally cause cardholder data to be stored or displayed in error logs or messages, or sent to any destination but the processor. Logs should be enabled between merchant and any third parties they use to enable monitoring of activity between all parties. Agreements with third parties should ensure that logs (applicable to the services being provided) are available if needed, for example in the event of an investigation due to a compromise.
	11. Regularly test security systems and processes	Even where a merchant has outsourced all cardholder data to a third party, that data may still be at risk due to vulnerabilities on the merchant's own server. Quarterly external vulnerability scanning performed by an ASV and file integrity monitoring can help provide evidence if any systems have changed, to allow merchants to correct the system back to a trusted state. Thorough penetration testing also helps ensure the web application is not vulnerable to attack. For custom applications, it is also critical to demonstrate that the website is regularly tested for application vulnerabilities and that a record of security bugs and fixes is maintained.
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel	Develop your security policies and make sure that everyone knows their responsibilities. Per PCI DSS Requirement 12.8, keep a list of all service providers, confirm their PCI DSS compliance as a service provider, and require in your written agreement that they acknowledge their responsibility for securing cardholder data. Since the worst can happen with even the best of precautions, prepare an incident response plan, test it at least once a year, and check that all contacts remain current. Verify service-level agreements provided by third-party service/hosting providers. Research prospective service provider's history for past security breaches, past or pending lawsuits, business ratings, publically accessible audit reports, and any useful information that may help assure your organization is partnering with reputable providers.

Appendix B: Merchant and Third-Party PCI DSS Responsibilities

If a merchant is managing their own e-commerce environment, they are responsible for ensuring that all PCI DSS requirements are implemented. On the opposite end of the scale, a merchant that outsources their entire e-commerce environment to third parties has a minimal set of PCI DSS requirements that they are responsible for (12.8 and monitoring as recommended in this Information Supplement).

This appendix is intended as an example of a checklist for those merchants that have a "hybrid" or outsourced e-commerce environment (hybrid environments are discussed in Section 3.5 of this document), and it can be used to understand, for their specific e-commerce implementation, which PCI DSS responsibilities belong to the merchant and which belongs to the third party(ies). For each PCI DSS Requirement, merchants can use this appendix to identify which party is responsible for compliance in the first two columns, and specify details on the evidence of compliance in the third column.

Note that this is intended for optional use at the discretion of the merchant/third party; completion of this appendix is not a requirement.

PCI DSS Requirements		Merchant Responsibility	Third Party Responsibility	How third party provided evidence of PCI DSS compliance
Build and Maintain a Secure Network	**1.** Install and maintain a firewall configuration to protect cardholder data			
	2. Do not use vendor-supplied defaults for system passwords and other security parameters			
Protect Cardholder Data	**3.** Protect stored cardholder data			
	4. Encrypt transmission of cardholder data across open, public networks			
Maintain a Vulnerability Management Program	**5.** Use and regularly update anti-virus software or programs			
	6. Develop and maintain secure systems an d applications			
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know			
	8. Assign a unique ID to each person with computer access			
	9. Restrict physical access to cardholder data			

PCI DSS Requirements		Merchant Responsibility	Third Party Responsibility	How third party provided evidence of PCI DSS compliance
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data			
	11. Regularly test security systems and processes			
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel			