Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)

Date: April 2017

Authors: Best Practices for Securing E-commerce Special Interest Group
PCI Security Standards Council

Information Supplement:

Best Practices for Securing E-commerce

Document Changes

Date	Document Version	Description	Pages
January 2013	1.0	Initial release	All
January 2017	1.1	Expanded and revised content based upon the Securing e-Commerce Special Interest Group	Various
April 2017	1.2	Corrected entries in table, Section 2.7 typographical and grammatical errors	Various

Table of Contents

Document Changes ..... **ii**

1 Introduction **5**

1.1 Background 5
1.2 Intended Audience 7
1.3 Terminology 7

2 Understanding E-commerce implementations **8**

2.1 Shared-Management E-commerce – URL Redirects 8
2.2 The iFrame 10
2.3 The Direct Post Method (DPM) 13
2.4 JavaScript Form 15
2.5 The Application Programming Interface (API) 17
2.6 Wholly Outsourced E-commerce Solutions 19
2.7 Advantages and Disadvantages of E-commerce Methods 20
2.8 PCI DSS Validation Requirements 21
2.9 The Intersection between E-commerce and Other Payment Channels 22
2.10 E-commerce Scoping Considerations 23
2.11 Additional Considerations 26

3 Public Key Certificate Selection **34**

3.1 Brief History on SSL and TLS 34
3.2 Selecting the Certification Authority 34
3.3 Selecting the Appropriate Type of Public Key Certificates 35
3.4 Tools for Monitoring and Managing E-commerce Implementations 36

4 Encryption and Digital Certificates **37**

4.1 Certificate Types (DV, OV, EV) and Associated Risks 37
4.2 TLS 1.2 Configurations 39
4.3 Merchant Questions on Certificate Types and TLS Migration Options 40

5 Guidelines to Determine the Security of E-commerce Solutions **44**

5.1 E-commerce Solution Validation 44
5.2 Validation Documentation 45
5.3 PCI DSS Requirement Ownership 46

6 Case Studies for E-commerce Solutions **47**

6.1 Case Study One: Fully Outsourced Redirect 47
6.2 Case Study Two: Fully Outsourced iFrame 49
6.3 Case Study Three: Partially Outsourced (JavaScript-Generated Form) 51
6.4 Case Study Four: Merchant Managed (API) 53

7 Best Practices **55**

7.1 Know the Location of all Your Cardholder Data 55
7.2 If You Don't Need It, Don't Store It 55
7.3 Evaluate Risks Associated with the Selected E-commerce Technology 55
7.4 Service Provider Remote Access to Merchant Environment 56
7.5 ASV Scanning of E-commerce Environments 56
7.6 Penetration Testing of E-commerce Environments 56

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 3

7.7 Best Practices for Securing e-Commerce 57
7.8 Implement Security Training for all Staff 58
7.9 Other Recommendations 58
7.10 Best Practices for Consumer Awareness 58
7.11 Resources 59

Acknowledgments 62

About the PCI Security Standards Council 64

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 4

1 Introduction

Electronic commerce, commonly known as e-commerce, is the use of the Internet to facilitate transactions for the sale and payment of goods and services. E-commerce is a card-not-present (CNP) payment channel and may include:

- E-commerce websites accessible from any web-browser, including “mobile-device friendly” versions accessible via the browser on smart phones, tablets, and other consumer mobile devices
- “App” versions of your e-commerce website, i.e., apps downloadable to the consumer’s mobile device or saving of the URL as an application icon on a mobile device that has online payment functionality (consumer mobile payments)

The objective of this information supplement is to update and replace the *PCI DSS E-commerce Guidelines* published in 2013. This information supplement offers additional guidance to that provided in PCI DSS and is written as general best practices for securing e-commerce implementations. All references in this document are for PCI DSS Version 3.2.

The guidance focuses on the following:

- Different e-commerce methods, including the risks and benefits associated with each implementation as well as the merchant’s responsibilities
- The selection of public key certificates and certificate authorities appropriate for a merchant’s environment
- Questions a merchant should ask its service providers (certificate authorities, e-commerce solution providers, etc.)
- General recommendations for merchants

1.1 Background

An e-commerce solution comprises the software, hardware, processes, services, and methodology that enable and support these transactions. Merchants choosing to sell their goods and services online have a number of methods 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 payment pages hosted by a third party.
- 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

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 5

providers and/or e-commerce payment processors, or manage some components in house while outsourcing other components to third parties.

Merchants may also decide to engage a third party to perform services that support their e-commerce solution. The service provider or the services may be considered in scope for a merchant's PCI DSS compliance if the security of the solution is impacted by this service and the service provider has not performed its own assessment. For more information, see the section on "Use of Third-Party Service Providers/Outsourcing" in the PCI DSS. Examples of common e-commerce support services that may affect cardholder data security include:

a) Software development on behalf of the merchant

b) Hosted website, either fully or partially managed by the solution provider

c) Hosted data center/network/physical systems in support of a website

d) Shopping-cart software (including software that hands off transactions or customer information to other systems)

e) Order-management software such as chargebacks, returns, etc. that may have access to cardholder data

f) Other hosting options (offline data storage, backups, etc.)—depending on whether the data is encrypted and whether the service provider has access to the decryption keys

g) Merchant plug-ins to support payment brand and issuer authentication mechanisms

h) Managed services, including WAF or log-management services

i) Any service that transmits cardholder data (CHD) or handles this data in some other fashion on behalf of the merchant services that have access to the checkout or payment-processing flow, including those without a need to access cardholder data, third-party fraud analysis, or analytics tools

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. A merchant is responsible for performing due diligence to ensure the service provider is protecting the CHD shared with it in accordance with PCI DSS. It is the acquirer or payment card brand, that determines whether a merchant must conduct an onsite assessment or is eligible for a Self-Assessment Questionnaire (SAQ).

- 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. More information on these relationships can be found in the *Third-Party Security Assurance* Information Supplement on the PCI SSC website.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 6

- It is recommended the merchant monitor connections and redirections between the merchant and the third party since the connections can be compromised. The merchant should ensure no changes have occurred and that the integrity of the e-commerce solution is maintained.
- It is recommended that e-commerce payment applications, such as shopping carts, 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.

1.2 Intended Audience

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

The guidance is applicable to merchants of all sizes, budgets, and industries. This document will be most useful to those merchants that have a solid understanding of their current e-commerce solution and environment. For small-to-medium sized merchants who do not know their e-commerce solution or environment, the recommendation is to review the PCI SSC Payment Protection for Small Merchants[1] first and then review the guidance in this document.

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.

1.3 Terminology

The following term is used throughout this document:

- **Payment Service Provider (PSP):** A PSP offers a service that directly facilitates e-commerce transactions online via its relationship with acquiring member banks of payment card brands. This category includes online payment processors, payment "gateway" service providers, virtual terminal services, and certain e-wallet or prepaid services that also process credit card payment for non-account holders at the point of sale. PSP services are discussed in this document.

For additional information on terms or definitions, please review the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*.

[1] This family of documents includes *Guide to Safe Payments*, *Common Payment Systems*, *Questions to ask Your Vendors*, and *Glossary of Payment and Information Security Terms*

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 7

2 Understanding E-commerce implementations

This section discusses different e-commerce implementations along with their potential impact to the merchant, recommendations for secure implementation, advantages and disadvantages of the implementation type, potential applicability of PCI DSS SAQ, other e-commerce implementations, scoping considerations, and additional features a merchant may want to consider. Some common e-commerce implementations include:

- Merchant-managed e-commerce implementations:
  - Proprietary/custom-developed shopping cart/payment application
  - Commercial shopping cart/payment application implementation fully managed by the merchant
- Shared-management e-commerce implementations:
  - URL redirection to a third-party hosted payment page
  - An Inline Frame (or "iFrame") that allows a payment form hosted by a third party to be embedded within the merchant's web page(s)
  - Embedded content within the merchant's page(s) using non-iFrame tags.
  - Direct Post Method (Form)
  - JavaScript Form
  - Merchant gateway with third-party embedded application programming interfaces (APIs)
- Wholly outsourced e-commerce implementations

These examples represent some of the most common implementations and are not all inclusive of every deployment option that may exist. Each implementation of hardware components, software applications, and hosting/service models will need to be individually evaluated to determine how this guidance may apply.

The following sections discuss these common e-commerce implementations in detail and include basic PCI DSS scoping guidance.

2.1 Shared-Management E-commerce – URL Redirects

2.1.1 What is a URL Redirect?

In the URL redirection model, the cardholder is redirected from the merchant's website to a third-party page. The cardholder then enters their account data into a payment page hosted by the third-party payment service provider (PSP). This may also be called a "punch out" since customers and application users are sent to a PSP's web pages. This is generally noticeable to the customer as the merchant's website URL—e.g., http://www.merchant.example.com—changes to that of the PSP—e.g., https://www.psp.example.com.

2.1.2 The Redirect Process

1. Merchant website sends a redirect command to the customer's browser.
2. The customer's browser then requests a payment form from the PSP.
3. The PSP creates the payment form and sends to the customer's browser.
4. The customer's browser displays the PSP's payment form.
5. The customer enters account data and sends to the PSP.
6. The PSP receives the account data and sends it to the payment system for authorization.

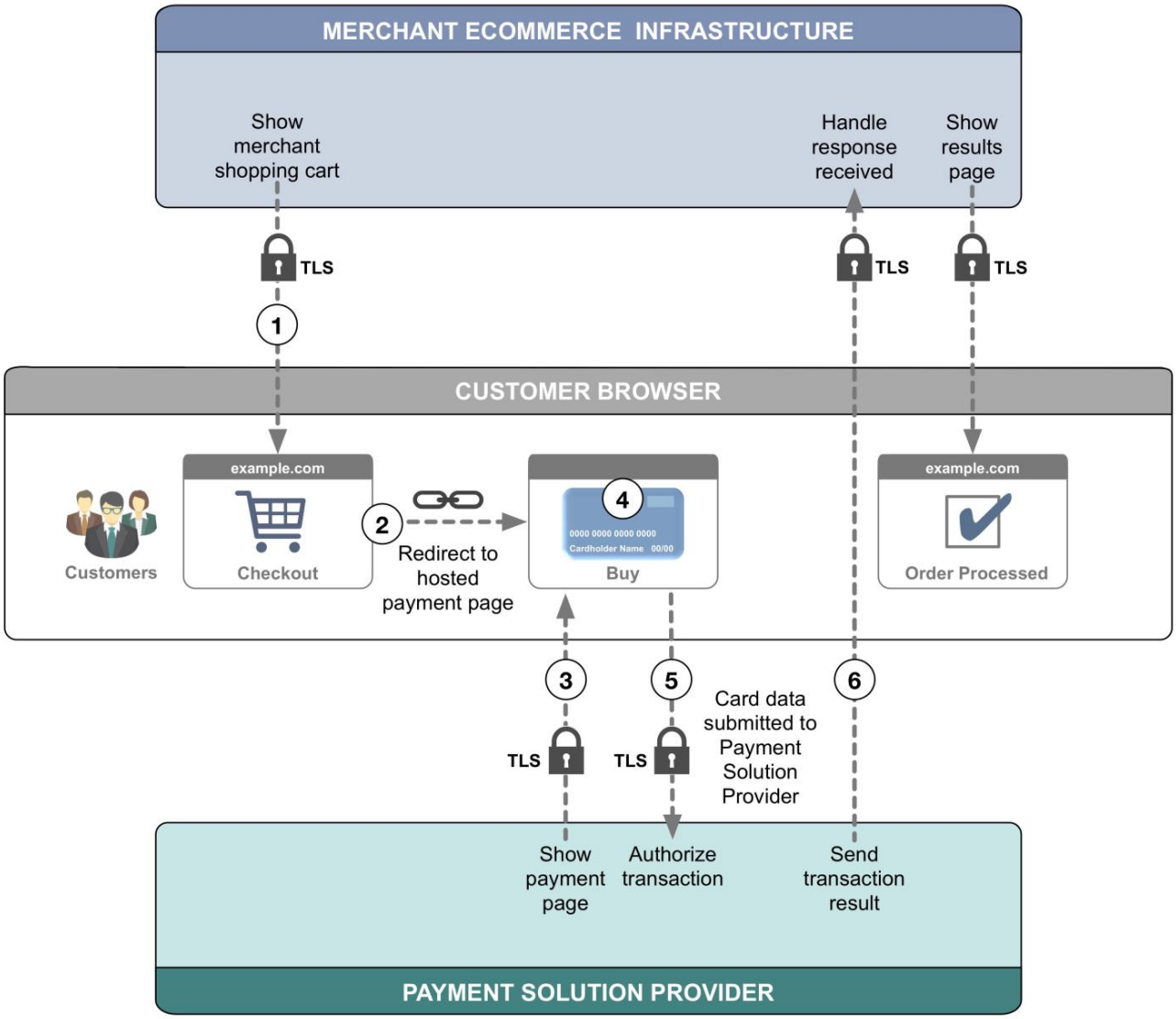

Figure 1 – An Example Redirect Payment Flow

2.1.3 Merchant Impact

As account data is not collected, stored, processed, or transmitted by the merchant's system, fewer systems need security controls. As redirects are commonly used by small and medium business organizations with lower-than-average cardholder data volume, it is less likely an attacker would target a merchant with this type of payment method. However, it is still important for merchants using a URL redirect to ensure their websites are secure, as a compromised web server could mean the redirect is changed to a bogus payment site in order to steal cardholder data—e.g., man-in-the-middle attacks wherein the web server collects and sends data to malicious individuals.

This e-commerce option provides an easier way for merchants to provide security for cardholder data, as most of the cardholder data security is performed by the PSP. As the PSP collects, stores, processes, and transmits cardholder data on behalf of the merchant, it is strongly recommended that a merchant ensure the PSP is validated as a PCI DSS compliant service provider to protect the merchant's cardholder data and enable an easier PCI DSS compliance route.

Merchants using a URL redirect e-commerce implementation may be eligible for PCI SAQ A or SAQ A-EP, providing they meet the eligibility criteria of that SAQ. Merchants should consult with their acquirer (merchant bank) or with the payment brands directly to determine whether they are required to validate their PCI DSS compliance and which reporting method they should use. The PCI SAQ A v3.2 currently includes as few as 22 PCI DSS requirements.

2.1.4 Recommendations

Since the redirect e-commerce method is usually easier for merchants to secure and results in fewer applicable PCI DSS requirements and lower risk of merchant systems being compromised, this method may be the best option for merchants with limited security or technical ability. However, this option may not suit many merchants wishing to provide advanced features or a more customizable customer payment experience. Merchants should consider the benefits and costs of customization versus the increased need for security controls and resulting increase in the security responsibility and number of applicable PCI DSS requirements.

2.2 The iFrame

2.2.1 What is an iFrame?

An iFrame (or Inline Frame) is a method of seamlessly embedding a web page within another web page—the iFrame becomes a frame for displaying another web page. The iFrame is unique. iFrame provides "sandboxing" to isolate content of the embedded frame from the parent web page, thus ensuring that information is not accessible or cannot be manipulated through various exploits by malicious individuals.

In e-commerce payments, the pages delivered during the checkout process would be supplied by the merchant's website, with an embedded iFrame supplied by the PSP within that process. The PSP's iFrame receives all cardholder data entered by the customer.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 10

2.2.2 *The iFrame Process*

1. The merchant website creates an iFrame within the current webpage. The customer's browser requests the payment form from the PSP.
2. The PSP creates a payment form and sends to the customer's browser within the iFrame.
3. The customer's browser displays the payment form within the iFrame located on the merchant page.
4. The customer enters their payment details into the iFrame containing the PSP's payment form.
5. The PSP receives the account data and sends it to the payment system for authorization.

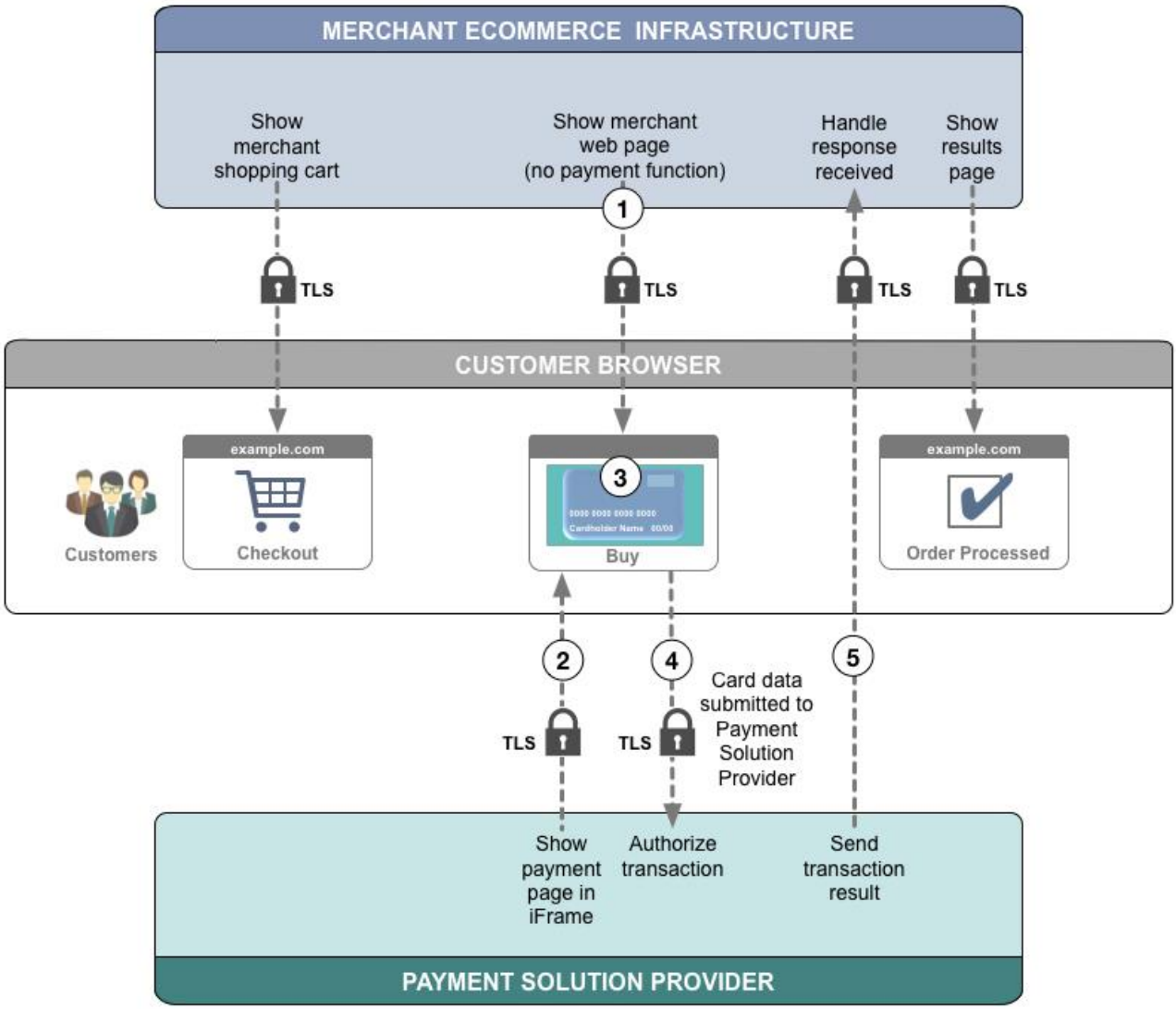

Figure 2 – An Example iFrame Payment Flow

2.2.3 iFrame security

At present, a merchant implementing an e-commerce solution that uses iFrames to load all payment content from a PCI DSS compliant service provider may be eligible to assess its compliance using a reduced list of controls identified in SAQ A, the smallest possible subset of PCI DSS requirements, because most of the PCI DSS requirements are outsourced to the PSP. The full list of eligibility requirements for use of this reduced self-assessment questionnaire is outlined within the SAQ A document.

However, despite the fact that merchants using iFrame implementations may be eligible for SAQ A, these types of e-commerce solutions are susceptible to compromise by a determined attacker, and merchants should ensure that they are appropriately addressing this risk. To that extent, SAQ A 3.2 was updated with additional requirements including changing default passwords (Requirement 2) and implementing some basic authentication requirements, such as requiring a unique user ID and strong password (Requirement 8). These requirements are intended to help protect merchant websites from compromise and maintain the integrity of the redirection mechanism. Additional information can be found in the PCI SSC FAQ knowledgebase found on the PCI SSC website document library.

iFrames provide a degree of security by relying on a technique known as the same-origin policy, which is enforced by all modern web browsers. The assessor will need to verify the merchant is getting the protection expected. This prevents malicious scripts on the merchant's website from interacting with the contents of the third-party content (i.e., the payment form) in the frame. This makes it more difficult for an attacker with control of the merchant's website or other third-party content providers to silently monitor and steal cardholder data.

If an attacker has compromised the merchant's website, however, they can create alternative content for the frame, which then allows completion of the payment process as well as creation of a copy of the cardholder data for the attacker. Without monitoring and alerting controls on the merchant's infrastructure, attacks of this nature might be impossible to detect.

Merchants should consider complementing their PCI DSS compliance program with additional security controls to reduce e-commerce risk, even if such controls are not stated as required by SAQ A. Hardening of servers, vulnerability management, and monitoring of server activity are effective controls for these implementations.

Merchants should also consider the use of additional layers of monitoring and defense provided by their PSP to promote additional security for the iFrame implementation. While not required under PCI DSS, it is recommended that PSPs provide configurable tools that detect and report suspicious transactions or unusual activity that may be indicators of compromised systems. While PCI DSS does not prescribe specific controls to monitor suspicious activity, it is a best practice for merchants to make use of PSP tools that are applicable to the merchant's e-commerce implementation. Some of these methods are discussed in Section 2.11.2, "Payment Service Provider Best Practices to Detect Suspicious Activity."

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 12

2.2.4 Merchant Impact

This architecture is limited in PCI DSS scope and is significantly lower risk for merchants than accepting payment information directly such as with the Direct Post Method or API. Payment card data is not collected, stored, processed, or transmitted by the merchant, so there are fewer systems that need security controls and lower risk of the merchant's systems being compromised.

This e-commerce option provides an easier way for merchants to provide security for cardholder data as most of the cardholder data security is performed by the PSP. However, as the PSP stores, processes, and transmits cardholder data on behalf of the merchant, it is strongly recommended that a merchant ensure the PSP is validated as a PCI DSS compliant service provider to protect the merchant's cardholder data and enable an easier PCI DSS compliance route.

Merchants using an iFrame e-commerce implementation may be eligible for PCI SAQ A, providing they meet the eligibility criteria of that SAQ. Merchants should consult with their acquirer (merchant bank) or with the payment brands directly to determine whether they are required to validate their PCI DSS compliance, and which reporting method they should use. The PCI SAQ A for PCI DSS v3.2 questionnaire currently includes as few as 22 requirements.

2.2.5 Recommendations

The iFrame e-commerce method is usually easier for merchants to secure, and results in fewer applicable PCI DSS requirements and lower risk of merchant systems being compromised (although not as low as the redirect method). However, this method also offers a better customer payment experience, as the customer remains on the merchant website throughout. The inline payment form can provide a better "look and feel" than the redirect payment method as the payment page can be customized to match the website design.

2.3 The Direct Post Method (DPM)

2.3.1 What is a Direct Post?

The Direct Post Method for e-commerce payment is generally used by larger merchants that require more control over their payment form "look and feel" and are able to understand and implement the extra PCI DSS security controls that are required to protect their systems.

The Direct Post Method uses the merchant's website to generate the shopping cart and payment web pages. The merchant's payment form, loaded in the customer's browser, sends the cardholder data directly to the PSP—not via the merchant's website or systems—ensuring cardholder data is not stored, processed, or transmitted via the merchant systems. However, the payment form is provided by the merchant; therefore, the merchant's systems are in scope for additional PCI DSS controls, which are necessary to protect the merchant website against malicious individuals changing the form and capturing cardholder data.

2.3.2 The Direct Post process

1. The merchant's website creates the payment page.
2. The customer's browser displays the payment page and sends cardholder data directly to the PSP.
3. The PSP receives the cardholder data and sends it to the payment system for authorization.

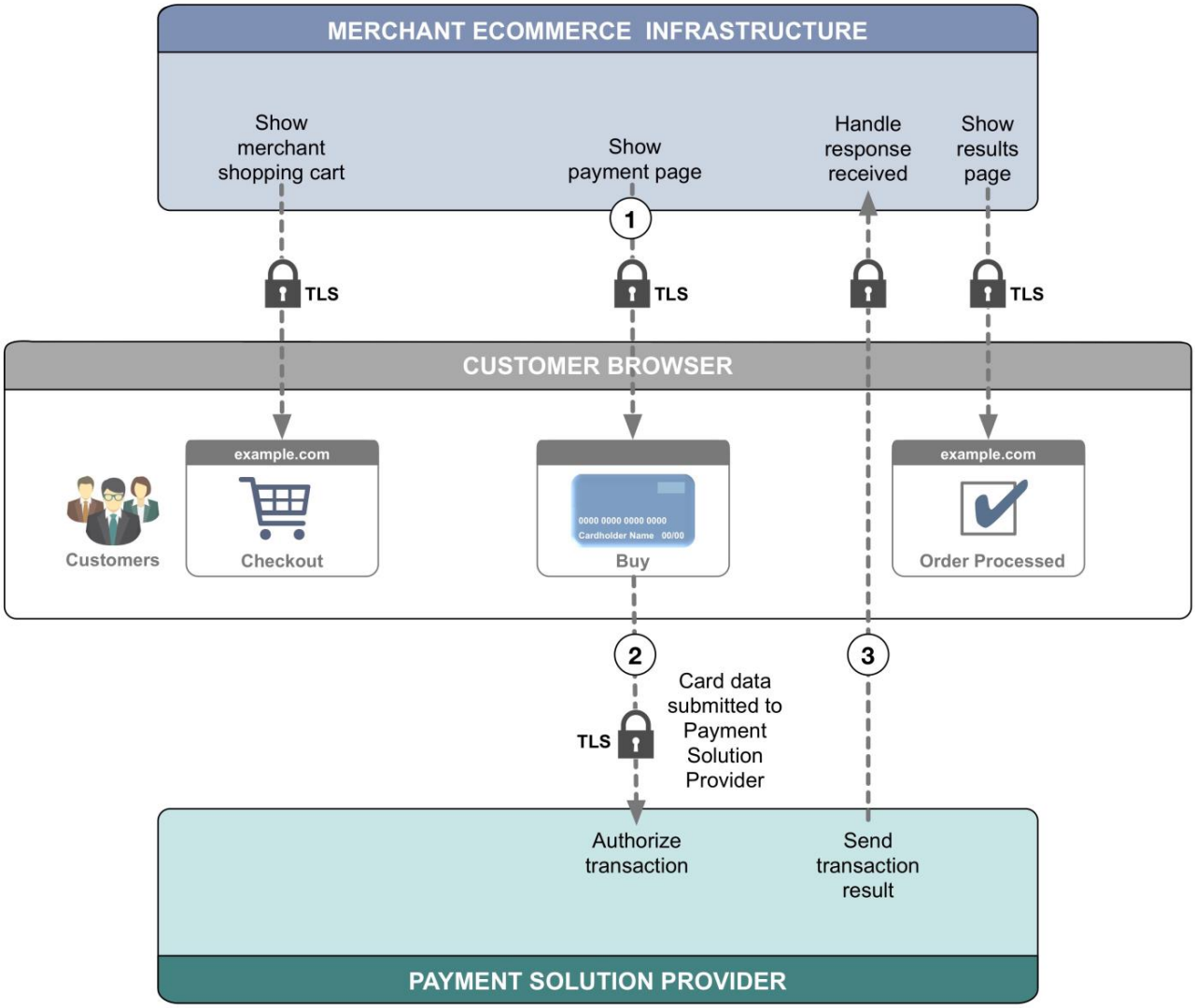

Figure 3 – An Example Direct Post Payment Flow

2.3.3 Merchant Impact

As account data is not stored, processed, or transmitted on the merchant's e-commerce systems, a subset of security controls is required to protect the web server and, in particular, the payment form due to the merchant's control over the manner in which cardholder data is collected and transmitted to the PSP. Because of this, there is an associated security effort, such as network and firewall security, secure software development, vulnerability scanning/penetration testing, and vulnerability and patch management. For a full list of requirements, please see the applicable SAQ.

Merchants using a Direct Post e-commerce implementation may be eligible for PCI SAQ A-EP, providing they meet the eligibility criteria of that SAQ. Merchants should consult with their acquirer (merchant bank) or with the payment brands directly to determine whether they are required to validate their PCI DSS compliance and which reporting method they should use. SAQ A-EP for PCI DSS v3.2 currently includes 191 requirements.

2.3.4 Recommendations

This architecture may be suitable for e-commerce implementations where the merchant prefers more control over the website look and feel and is comfortable with the additional responsibility for securing its website. The organization's appetite for payment-card data risk and PCI DSS scope may require avoidance of a fully merchant managed solution.

The Direct Post Method has a higher security responsibility for and higher risk of merchant system compromise than the URL redirect or iFrame methods, as the merchant's web server controls the payment form, which is often a target for criminals. More PCI DSS requirements apply to the Direct Post Method than the URL redirect and iFrame methods.

Increased security is required to protect the website and its code, raising operational and audit costs for the merchant; however, this needs to be balanced against the design and use benefits of merchant-created forms. It is recommended additional security controls above those required by PCI DSS be implemented.

2.4 JavaScript Form

2.4.1 What is a JavaScript Form?

Similar to the Direct Post Method, the JavaScript payment page originates from the merchant's website and requests the customer's browser execute JavaScript code from the PSP to create the payment form. Entered cardholder data is then sent directly to the PSP in the same way as the Direct Post Method.

Also similar to the Direct Post Method, a JavaScript form is generally used by larger merchants that require more control over their payment form look and feel and are able to understand and implement the extra PCI DSS security controls that are required to protect their systems.

2.4.2 The JavaScript Form process

1. Merchant website creates the payment page.
2. Payment page on the customer's browser requests JavaScript from the PSP.
3. The PSP creates JavaScript and sends to customer's browser.
4. The customer's browser uses JavaScript to create the payment form within the payment page.
5. The customer completes payment by entering payment details into the form, which is sent directly to the PSP.
6. The PSP receives cardholder data and sends to payment system for authorization.

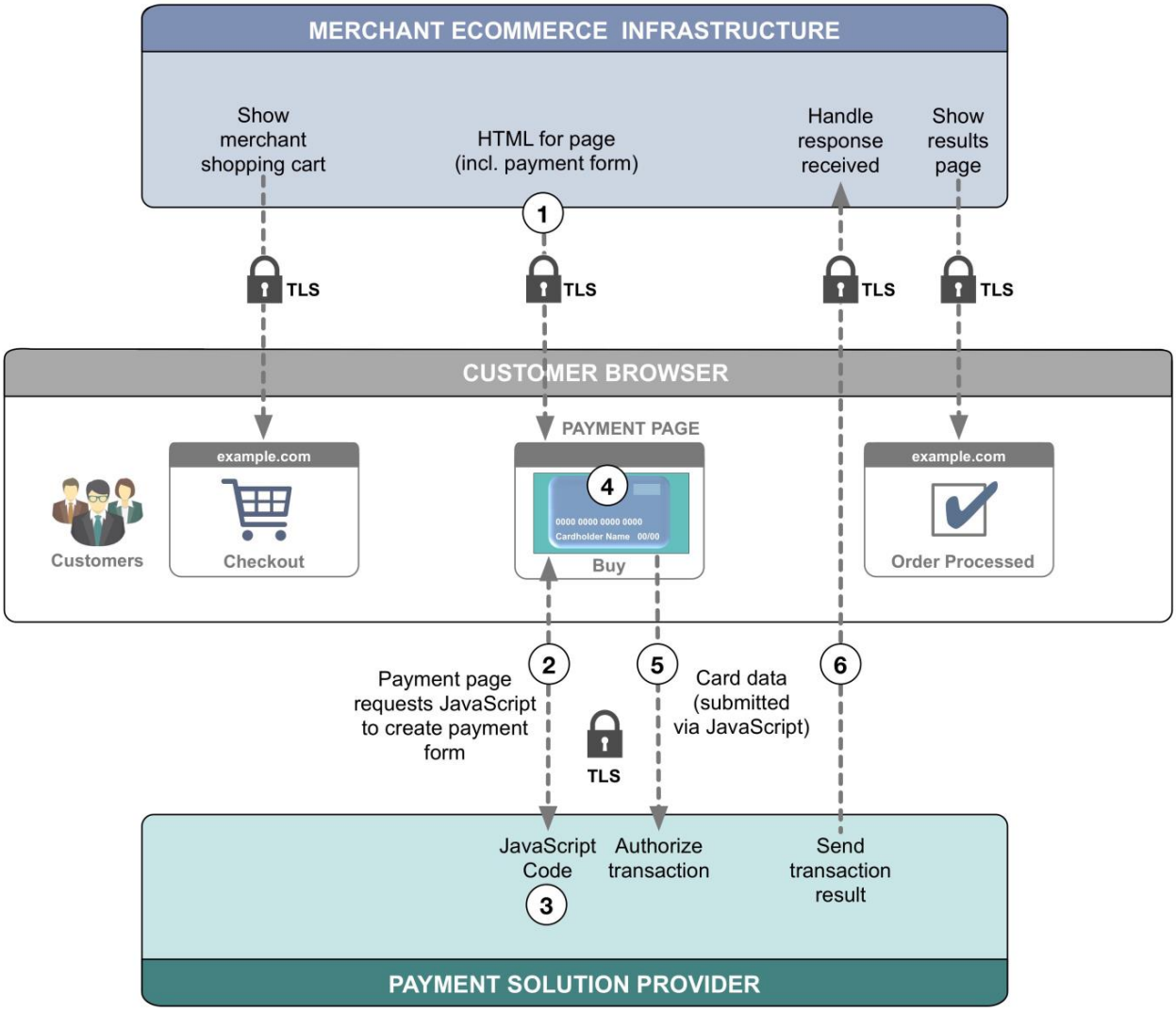

Figure 4 – An Example JavaScript Form Payment Flow

2.4.3 Merchant Impact

As the merchant controls the manner in which cardholder data is collected and transmitted to the PSP, the same PCI DSS controls apply as with the Direct Post Method described above (Section 2.3).

Merchants using a JavaScript e-commerce implementation may be eligible for PCI SAQ A-EP, providing they meet the eligibility criteria of that SAQ. Merchants should consult with their acquirer (merchant bank) or with the payment brands directly to determine whether they are required to validate their PCI DSS compliance and which reporting method they should use. SAQ A-EP for PCI DSS v3.2 currently includes 191 requirements.

2.4.4 Recommendations

All recommendations for the Direct Post Method also apply to the JavaScript Form payment method. The decision to choose one method over the other may be an architectural decision overall. With Direct Post, the merchant will lose control over the session momentarily, whereas with JavaScript, the merchant can maintain some level of control over the session by watching for a timeout and seamlessly delivering an error message to the customer. The decision also depends on the PSP and how the PSP has built what the merchant is using. The merchant should discuss with its PSP.

2.5 The Application Programming Interface (API)

Merchant e-commerce systems that receive or store cardholder card data (even temporarily) require greater security controls than the previously discussed methods.

In the payment methods discussed earlier in this document, risks are minimized due to payment service providers receiving cardholder data directly from the customer, reducing security responsibility for merchant systems.

The merchant system's handling of cardholder data in the API method may require that the entire set of PCI DSS controls be applied to the merchant's in-scope systems, people, and processes.

2.5.1 What is an API?

In this context, an application-programming interface (API) is a method of system-to-system data transmission wherein the merchant principally controls the progress of the payment transaction. Customer cardholder data is sent from the customer browser back to the merchant website before being sent to the PSP. Data sent to the PSP may be sent in different formats such as XML, JSON, or name/value pairs.

The payment page and form are hosted and supplied by the merchant website with all cardholder data processed by the merchant web server (and possibly other system components) before being sent to the payment solution provider.

2.5.2 The API Process

1. Merchant creates payment page.
2. Customer's browser displays the payment form.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 17

3. The customer enters cardholder data into the payment form and the data is sent to merchant web server.
4. The merchant web server transmits cardholder data to the PSP.
5. The PSP receives cardholder data and sends it to the payment system for authorization.

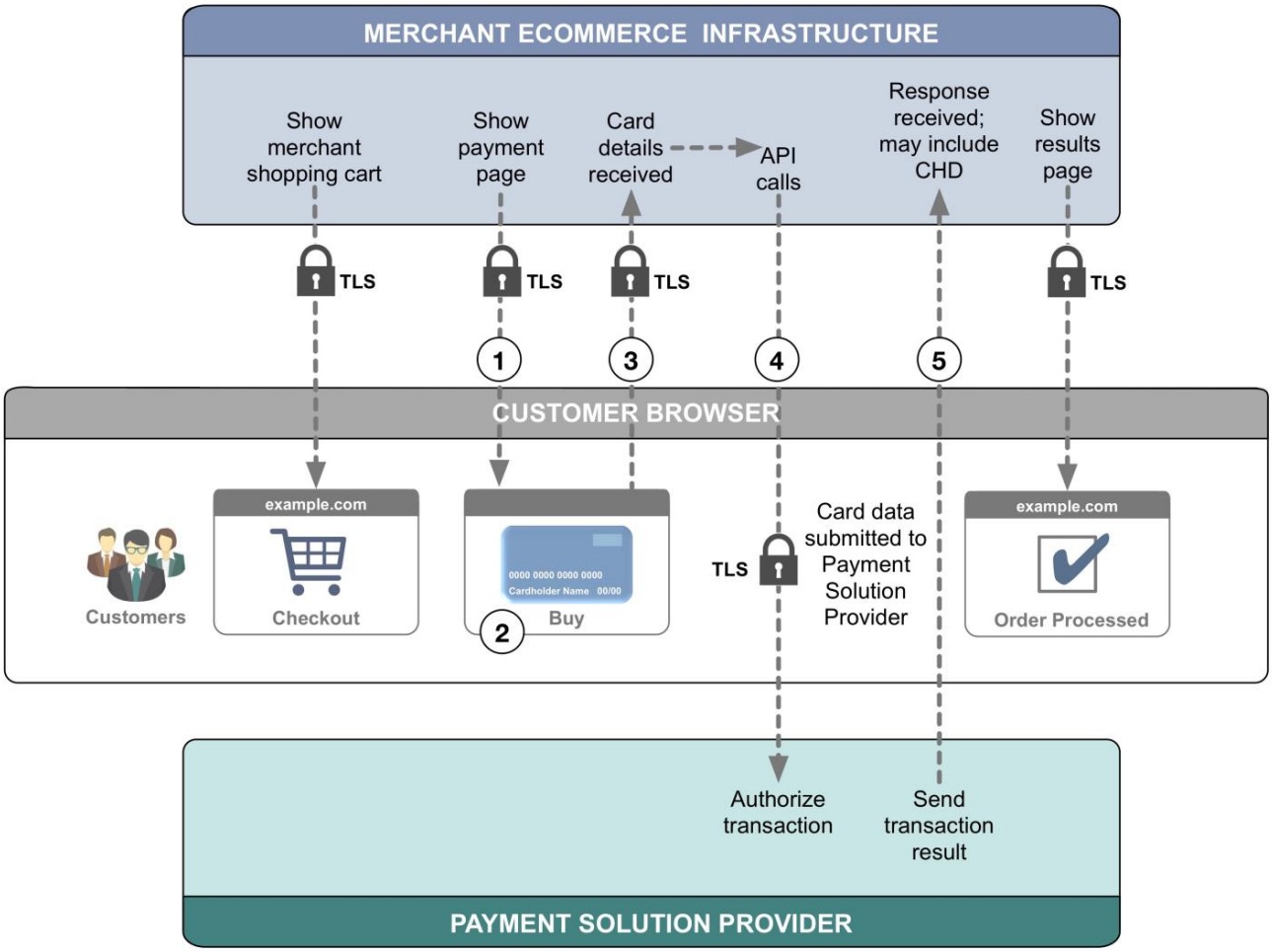

Figure 5 – An Example API Payment Flow

2.5.3 Merchant Impact

This architecture carries a high risk for merchants as their systems will receive and transmit, and may also store and process, cardholder data. Hackers target websites using this payment method because there is a greater chance of larger amounts of valuable cardholder data being available, and the attack can be easier due to varying levels of security controls among merchants. Due to the higher risk of compromise to merchant systems, the level of security responsibly for the merchant is high.

Merchants using the API e-commerce payment method may be eligible for SAQ D, providing they meet the eligibility criteria of that SAQ. Merchants should consult with their acquirer (merchant bank) or with the payment brands directly to determine whether they are required to validate their PCI DSS compliance and which reporting method they should use. SAQ D for Merchants for PCI DSS v3.2 currently includes 250 questions.

2.5.4 Recommendations

For smaller merchants, this may not be a cost-effective e-commerce payment route due to the associated level of security responsibly. The API method is generally used by larger organizations with specific processing needs, or organizations that wish to retain cardholder data.

The applicable controls to secure all systems, people, and processes within an organization for PCI DSS compliance should not be underestimated.

Merchants are advised not to store, process, or transmit cardholder within their own systems unless the nature of their payment acceptance is not compatible with any of the other models described previously.

Note: *Some merchants may reduce the number of applicable requirements by leveraging tokenization to eliminate payment card data storage. See Section 2.11.3, "Tokenization" for more information.*

2.6 Wholly Outsourced E-commerce Solutions

Many e-commerce solutions exist that provide most or the entire merchant's online shopping functionality and experience. These solutions provide more than just transaction processing capability, often including customer-facing features such as product search, cart capability, checkout, and account management; and back-office features such as product management, customer relationship management, order management, and appearance customizations.

A hosted shopping cart is an e-commerce system that is hosted entirely on the service provider's technological infrastructure. The e-commerce is not seamlessly integrated into the merchant's website and the consumer is often directed off-site to select product and complete checkout.

The use of such a solution can alleviate many but not all of the merchant's PCI DSS responsibilities. All merchants have a responsibility to implement policies and procedures that govern safe handling of cardholder data even if they never expect to encounter credit cards. Furthermore, it is the responsibility of the merchant to vet the service provider and monitor its compliance to PCI DSS. See SAQ A for more information on assessing compliance for merchants who use these solutions.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 19

2.7 Advantages and Disadvantages of E-commerce Methods

	URL Redirect	iFrame	Direct Post	Java Script	API
Is generally easier to ensure cardholder data is secured, compared to the other e-commerce techniques.	🟢	🟢	🟡	🟡	🔴
No cardholder data is stored, processed, or transmitted by the merchant.	🟢	🟢	🟢	🟢	🔴
TLS certificate is provided by the PSP for secure transmission of CHD.	🟢	🟢	🟢	🟢	🔴
Merchant does not need to purchase TLS certificate just so the customer “sees the lock” in the address bar.	🟢	🔴	🔴	🔴	🔴
Customers remain on the merchant website throughout the payment process.	🔴	🟢	🟢	🟢	🟢
Ability to use Web 2.0 UX capabilities to improve customer experience.	🔴	🔴	🔴	🟢	🟢
Same “look and feel” as core website.	🔴	🟡	🟢	🟡	🟢
Complete control and visibility over the customer payment process.	🔴	🔴	🟢	🟢	🟢
Supports highly specialized processing requirements.	🔴	🔴	🟡	🟡	🟢
The merchant has extensive control over customer’s end-to-end experience.	🔴	🔴	🟢	🟡	🟢
Customizable payment page that matches the website design.	🔴	🟡	🟢	🟡	🟢
URL remains consistent, preserving branding and reducing customer suspicion.	🔴	🟢	🟢	🟢	🟢
Merchant is less dependent on third party for critical payment function.	🔴	🔴	🔴	🔴	🟢
Vulnerabilities on merchant web server do not impact security of cardholder data.	🟢	🟢	🔴	🔴	🔴
Lower risk and reduced PCI DSS security requirements to protect the web server and code compared to other methods.	🟢	🟢	🟡	🟡	🔴
Lower cost to comply with applicable PCI DSS requirements.	🟢	🟢	🟡	🟡	🔴
Merchant has greatest flexibility to store, process, and transmit cardholder data if needed per business requirements.	🔴	🔴	🔴	🔴	🟢

Legend:

- 🟢 Advantage
- 🟡 Neutral
- 🔴 Disadvantage

2.8 PCI DSS Validation Requirements

Merchants should consult their acquirers or the payment brands directly to determine any PCI DSS validation requirements and reporting methods that may apply to them. For example, the acquirer or payment brands determine whether the merchant:

- May be required to complete an onsite assessment documented via a PCI DSS Report on Compliance (ROC) or
- Is eligible to complete a self-assessment documented via one of the PCI DSS Self-Assessment Questionnaires (SAQs).

Merchants eligible to self-assess their PCI DSS compliance should work with their acquirers or payment brands to determine which SAQ type is appropriate, based on the e-commerce implementation method used. The table below summarizes the relevant PCI DSS documentation for merchants that may be required to submit a ROC, as well as for those that may be eligible to self-assess via an SAQ. The corresponding number of PCI DSS requirements is included for each reporting method.

PCI DSS Documentation Requirements by E-commerce Method

E-commerce Method	SAQ Type for eligible merchants	Guidance for merchants who are required to submit a Report on Compliance (ROC)	Number of Questions under PCI-DSS v3.2 (Not including any relevant appendices)	Ease
Wholly Outsourced e-Commerce	SAQ A	Merchants may be required to submit a Report on Compliance (ROC) but may be able to use SAQ A as a reference to identify applicable PCI DSS requirements for that environment, providing the environment fully meets all eligibility criteria defined in that SAQ.	22	
Redirect	SAQ A			
iFrame	SAQ A			
Direct Post	SAQ A-EP	Merchants may be required to submit a Report on Compliance (ROC) but may be able to use SAQ A-EP as a reference to identify applicable PCI DSS requirements for that environment, providing the environment fully meets all eligibility criteria defined in that SAQ.	191	
JavaScript	SAQ A-EP			
API	SAQ D	Some requirements of SAQ D or ROC may be marked “not applicable” if they do not apply to the specific e-commerce channel. Consult with QSA or acquirer for further guidance.	250	
Other	SAQ D			

2.9 The Intersection between E-commerce and Other Payment Channels

2.9.1 E-commerce Transactions

E-commerce is the use of the Internet to facilitate online transactions for the sale and payment of goods and services. E-commerce is a card-not-present (CNP) payment channel and includes:

- E-commerce websites accessible from any web browser, including "mobile-device friendly" versions accessible via the browser on smart phones, tablets, and other consumer mobile devices
- "App" versions of the merchant's e-commerce website, i.e., apps downloadable to the consumer's mobile device that have online payment functionality (consumer mobile payments)

The merchant may be involved in initiating or triggering the transaction; however, it is always the cardholder who enters the payment information (i.e., cardholder data) on a device that is not controlled or provided by the merchant. For example, the merchant may instigate the sales process (i.e., invoicing) by sending the cardholder an e-mail message with a unique payment URL for them to complete the credit card transaction via the Internet. Alternatively, for example, the merchant may retain payment card details initially submitted by the cardholder for an e-commerce payment in order to initiate ongoing recurring transactions, such as subscriptions. Depending on how the card details are stored and recurring transactions processed, these recurring payments may also be considered e-commerce.

Some merchants have introduced e-commerce payments into what are traditionally card-present environments—for example, quick-service restaurants. While present on the merchant premises, the consumer initiates a card payment using their own mobile device via the "mobile-friendly" merchant website or app.

2.9.2 Non E-commerce Transactions

Payment channels and methods that could be confused with but are not e-commerce include:

- Merchant payment acceptance using a COTS (commercial off-the-shelf) mobile device:
  - With a card reader (connected to the mobile device via cable to the radio jack, or using Bluetooth):
    - Card data is captured through dip or swipe of the payment card.
  - Without a card reader, merchant-initiated:
    - Merchant manually enters the consumer's payment card details into the mobile device's web browser (e.g., via its online order management website or a third-party virtual terminal).
    - Merchant manually enters the consumer's payment card details into an app on the mobile device, providing virtual terminal functionality.
- Merchant-initiated payments using a web browser:
  - Merchant manually enters the consumer's payment card details into web browser—e.g., via its online order management website or a third-party virtual terminal.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 22

- Consumer-initiated payments using a web browser on the merchant's payment kiosk on the merchant's premises or merchant-provided payment device (such as tablets for payment at a restaurant table):
  - Consumer manually enters their payment card details into the web browser on the merchant's payment kiosk or through the provided payment device.

These non-e-commerce methods may be used/offered in card-present (CP) or card-not-present (CNP) scenarios. A merchant should implement appropriate PCI DSS controls to ensure the security of the devices and facilities offered to the public, in addition to securing its e-commerce website (or app).

2.10 E-commerce Scoping Considerations

When a merchant is scoping its cardholder data environment and determining where PCI DSS controls need to be applied, it must ensure the online capture and retention of cardholder data is considered as well as the method used to process and authorize the payment. Typically, for CNP e-commerce transactions, payment card authorization is real-time as the e-commerce site has connectivity to a payment gateway or payment service provider. However, the merchant's site may only capture the consumer's payment card data with no subsequent authorization—for example, if card details are submitted purely to "guarantee" the order (e.g., a hotel or car rental reservation). In such cases, there is no consumer expectation that the payment account will be charged at the time of booking. The consumer payment for the services rendered is usually face-to-face (card-present)—at check-in or on collection of the rental vehicle, for example.

In some scenarios, e-commerce websites not connected to a payment gateway or payment service provider offer the consumer other order/booking options in addition to the submission of card details to "guarantee" an order. For example, merchants in the hotel or car rental sectors may offer:

1. **Advanced Purchase:** Card details are provided with the order; the cardholder's expectation is that the merchant will take the full value of the order/booking up-front.

2. **Deposit Booking:** Card details are provided with the order; the cardholder's expectation is that the merchant will take a deposit amount (percentage of the order/booking value) up-front.

   These order/booking options usually set the consumer expectation that the card details supplied will be charged at the time of the order/sale. Both options 1 and 2 should be considered e-commerce transactions since they are online CNP transactions where card data is submitted by the consumer with an expectation of real-time authorization of the agreed amount. However, if the e-commerce site has no connectivity to a payment gateway or payment service provider, the merchant processes the consumer's payment "offline"—for example, as a re-key submitted manually using a payment terminal or via a virtual terminal. As these payment card transactions are not flagged as e-commerce, be aware that this may be a breach of payment brand rules for the processing of e-commerce transactions. Merchants should contact their acquiring bank or the applicable payment brand to determine whether offline authorization of e-commerce card payments is permitted.

As mentioned above, when a merchant is scoping its e-commerce payment channel for compliance assessment, it is necessary to consider of all card data flows and all aspects of payment card processing that may affect its scope, not just the e-commerce website itself.

2.10.1 Scoping E-commerce in Isolation

A merchant considering its e-commerce payment channel in isolation from its other payment card handling activities may conclude that the scope of assessment is as shown in the blue area below, because the e-commerce website is set up to redirect the consumer to a PSP payment page.

The merchant may decide that SAQ A is applicable for this channel:

- All processing of cardholder data is entirely outsourced to PCI DSS compliant third-party service providers (SP).
- All SPs handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant.
- All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS compliant SP.
- Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a SP to handle all these functions.
- Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically. This information must be stored in accordance with the applicable PCI DSS requirements.

As a reminder, merchants may be eligible for SAQ A, providing they meet the eligibility criteria of that SAQ. Merchants should consult with their acquirer (merchant bank) or with the payment brands directly to determine whether they are required to validate their PCI DSS compliance and which reporting method they should use.

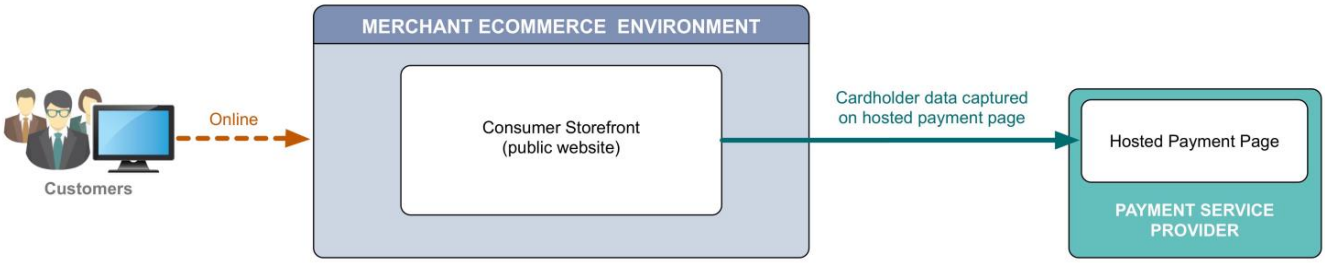

Figure 6 – E-commerce in Isolation

2.10.2 Scoping E-commerce in Conjunction with all Card Data Flows and Payment Channels

However, in reality, a merchant's e-commerce payment channel and website may not be operating in isolation from other payment card handling activities. The merchant may operate other payment channels and there may be other cardholder data flows related to or supporting the e-commerce payment channel that need to be taken into consideration when scoping the merchant's PCI DSS environment.

The diagram below illustrates some of other payment methods and cardholder data flows that may be present:

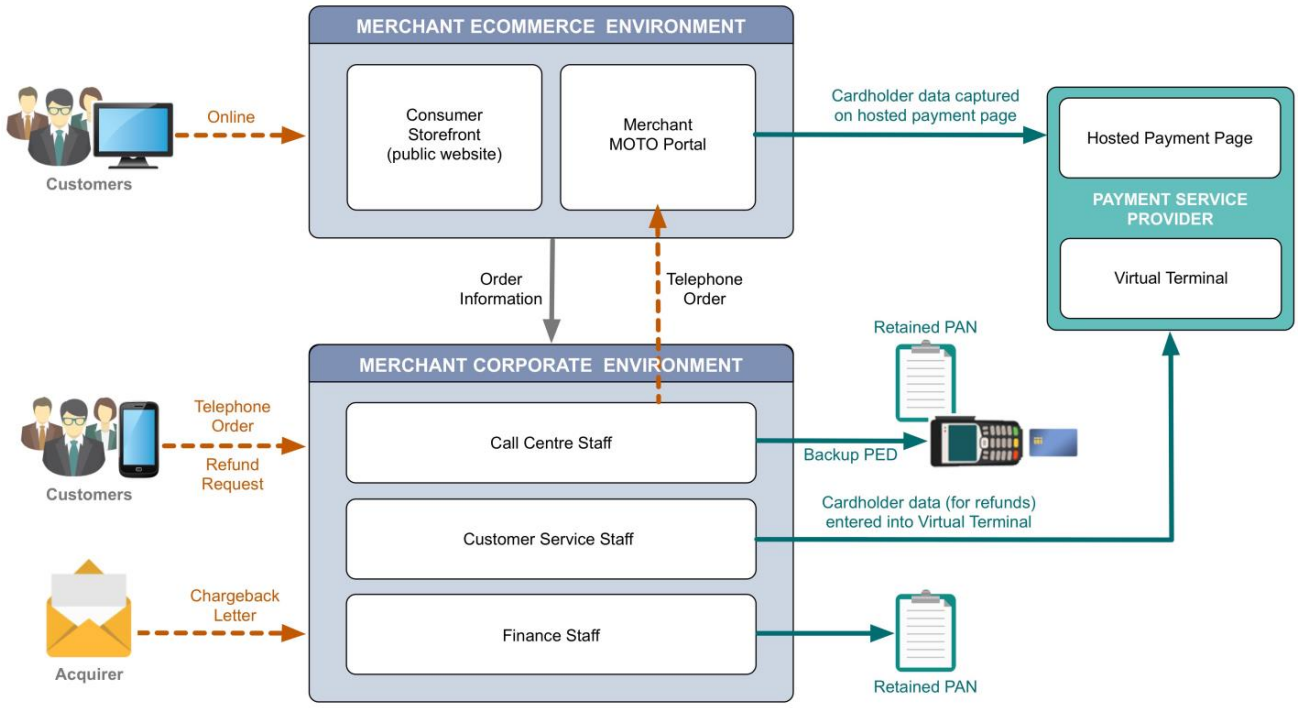

Figure 7 – E-commerce in Conjunction with all Card Data Flows and Payment Channels

By considering all payment methods and cardholder data flows, the merchant may find that despite the fact that the e-commerce website is set up to redirect the consumer to a hosted payment page, it is not eligible for SAQ A. For example, because of the following payment card handling activities, other PCI DSS requirements may be applicable:

- **Telephone orders:**
  - The merchant's call center staff provide support for consumers having difficulty ordering online. The call center can take orders and payments for these consumers. In this example the call center uses a mail order/telephone order (MOTO) portal (web application) supported from the same e-commerce infrastructure as the consumer storefront. (See PCI SSC FAQ

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 25

1439 for more information.) The MOTO portal is also configured to redirect to the PSP's hosted payment page. The merchant will need to consider the scope implications of taking payments on corporate PCs, through a VoIP telephone system (transmitting CHD), and whether they are recording the calls. In all cases, they may be capturing cardholder data and sensitive authentication data.

  - Call center staff also have a back-up payment terminal for use when the website is out of service. The merchant will need to consider how is this connected, and whether the receipts contain the full card number.

- **Refund requests:**
  - The merchant's customer service team process refunds for online orders. In this example, they manually rekey the customer card details into the PSP's virtual terminal. The merchant should consider whether there is an alternative method that allows it to refund a transaction without re-entering the cardholder data; if not it will need to consider the scope implications as with the call center.
- **Retrieval requests and chargebacks:**
  - The merchant's finance team may receive retrieval requests and chargeback letters from its acquirer. Typically, these contain the full card number. The merchant will need to consider how these letters are handled. Are the letters retained in hard or soft copy? Are the letters scanned or e-mailed? Scanned chargeback letters containing the full card number (instead of only the last four digits or a replacement token) would be considered electronic storage of cardholder data, negating eligibility for any SAQ other than D. The acquirer may offer alternative methods for the merchant to eliminate handling of full card numbers, such as an acquirer extranet chargeback notification service.

From these examples, we can see that although the merchant has outsourced the handling of e-commerce payment card data to the PSP, merchant PCI DSS compliance assessment using only the SAQ A is no longer appropriate as is does not cover all of its payment card handling activities.

2.11 Additional Considerations

It is one thing to look for the best or most innovative e-commerce technology on the market; however, this does not guarantee that the customer's card data will be protected. Many businesses are searching for SPs to provide various security features along with the "seamless" payment processing solution offered in order to make the most informed decision. In this section, we will discuss the features that merchants may also want to consider when selecting the most appropriate e-commerce implementation for their CHD processing environment while not compromising on the integrity of the solution's security features.

2.11.1 Anti-Fraud Considerations

As a standard business practice, companies must implement and consistently manage some level of an adequate governance program. This would include the execution of compliance, training, and audit programs in order to protect a company's assets—the most important being the consumer and the

consumer's data. Consequently, many aspects of an entity's governance program can be outsourced to minimize scope and exposure. If a company decides to manage its own anti-fraud program with respect to CHD and has CHD in the clear (instead of a replacement token), this may mean that its scope has been expanded to include its corporate structure. Therefore, companies must determine whether and how they will conduct their own anti-fraud programs. Some service providers manage the overall processing, transmitting, and/or storage of cardholder data along with anti-fraud tools and analytics as a value-added service.

Anti-Fraud Measures

As a CNP channel, e-commerce does not have access to the cardholder's PIN or signature for verification of the cardholder. Instead, e-commerce payments rely on the merchant capturing the card security code (the three-digit number printed on the card signature panel or four-digit number on the front of an American Express card). A cardholder verification method to confirm that the consumer has the card in-hand and is not using a stolen account number is requesting the card security code for e-commerce payments; it provides some merchant protection.

E-commerce payments can use additional, stronger cardholder verification methods including address verification, which checks the address provided by the consumer against the billing information on file with the card issuer. Other methods provide additional cardholder verification using a customer's pre-defined password like 3-D Secure or other payment brand or issuer payer authentication methods. 3-D Secure is not available if a merchant processes the consumer e-commerce payment "offline." Address verification is no guarantee against fraud because criminals frequently sell address and other cardholder information together with card account information.

3-D Secure is a protocol designed to be an additional security layer for online payment card transactions, enabling consumers to authenticate their card directly with their card issuer when shopping online. 3-D Secure is offered under different names by each of the payment brands.

2.11.2 Payment Service Provider Best Practices to Detect Suspicious Activity

It is the expressed intent of the PCI SSC to address matters of account data security, preventing valuable cardholder data and sensitive authentication data from being stolen. In doing so, the PCI DSS identifies security controls that must be in place to ensure that card data is sufficiently protected. In addition, Requirement 12.8.5 requires merchants to maintain a clear understanding of which controls the service provider will meet on their behalf. This can be achieved by consulting the service provider's AOC and/or responsibility matrix.

Concepts such as detection and prevention of fraud (the use of account data that has already been stolen elsewhere) are out of scope for PCI DSS. Nonetheless, fraud and data security are tightly linked. Increased adoption of fraud-detection and prevention methods will ultimately improve the effectiveness of data security efforts, as widespread industry use of such tools devalues cardholder data in the eyes of fraudsters who can no longer easily abuse stolen information online. Transaction monitoring and alerting services provided by PSPs for fraudulent transactions may also be used to track security incidents.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 27

Furthermore, fraud indicators may themselves be symptomatic of compromised systems or man-in-the-middle attacks. The most common such indicator of intercepted data is transactions that suddenly originate from an unrecognized source or spoofed IP (for API transactions), or IPs that are not representative of the customer base (for redirect or Direct Post transactions). Other transaction changes—such as changes to customer information that may prevent customer alerts, accessing customer login credentials, undermining geography verification, or redirecting shipping information—may also be an indication of a hacker attempting to subvert security controls. Dips in expected transaction volume might indicate that the normal process has been altered to allow the attacker to intercept transaction information. Similarly, a spike in transaction volume may represent an attempt to flush batches of intercepted transactions in order to avoid detection (as merchants tend to notice if sales were to stop altogether).

For these reasons, the table of common security and fraud controls below has been included that supplement existing guidance. This information may be especially relevant to merchants who are evaluating the use of a service provider to provide secure e-commerce payment processing solutions through APIs, redirects, and Direct Posts (see Section 2).

Common Security and Fraud Control Services

Service	Description
Instant Merchant Notification	A feedback loop from the PSP to the merchant ensures that the merchant is immediately informed of transactions, and can raise alerts when suspicious activity is observed that is not otherwise detected. Where this notification is passed programmatically to a merchant API endpoint (e.g., “postback”), the PSP should provide a mechanism to ensure that the destination is not changed by a malicious user or that the postback does not contain account data.
Authentication	It is recommended that PSPs support the use of a limited-use token that can be retrieved or generated. This method may be used to authenticate the source of the transaction.
Data Verification	PSPs may support the use of cryptographic hashes to verify that important data passed from the merchant to the PSP remains unaltered in the hand-off (e.g., shipping information). Verification failures should be logged to alert merchants to possible man-in-the-middle attacks.
Address Verification Service (AVS)	AVS is a system supported by the card brands, where numeric address information from the street address and postal code are passed to the issuing bank for verification. This control may be very effective for preventing fraud or redirected shipping information from a man-in-the-middle.
CVV2 Verification	CVV2 verification is the recommended cardholder verification method for card-not-present merchants. Card data stolen from card-present merchants should not contain this value, and thus should be unusable online if proper verification is performed. Note that CVV2 is considered sensitive authentication data (SAD) and should never be stored by the PSP after authorization.
Transaction Amount Floors/Limits	Blocking or reviewing transactions that fall outside minimum and maximum transactions amounts can prevent carding, where fraudsters attempt to identify which of their stolen cards are still active.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 28

Service	Description
Transaction Volume Floors/Limits	Blocking or reviewing transactions that fall below or exceed expected transaction count thresholds is a common way to alert merchants of abnormal activity associated with compromise or fraud. Granular configurations often exist to measure similar transactions within a short time frames (e.g., transactions per second, transactions per hour) based on common source, type, or other attribute. These features are often called "velocity controls."
Brute Force / Trial-and-error Detection	Duplicate transactions with altered information (different source IP, different expiration date, or different CVV2) should be cause for suspicion. These may indicate attempts to bypass other fraud tests or verify stolen card data that may be incomplete or expired.
E-mail Verification	Some PSPs may offer verification services to confirm whether an ISP e-mail account originates from the IP of the ISP itself or whether fraudsters commonly use that e-mail domain. This test is insufficient to identify fraud but may be used in fraud scoring.
Geographic Verification	Common geography verifications include comparing the provided physical address with the geographic region associated with the source IP, or the area code of the provided phone number.
IP Blacklisting	Manual blocking of IPs and IP ranges allows the merchant to prevent abuse from known sources. Some PSPs offer access to known sources of suspicious activity, such as proxies or regions known for malicious activity.
IP Whitelisting	For merchants who send transactions to the PSP via API, an IP whitelist is crucial to confirm that the transactions originate from the trusted system(s), and not from a man-in-the-middle attacker.
HTTP Header Verification	For merchants who use redirect (including iFrame), Direct Post, or JavaScript methods to pass customer data from the browser to the service provider, the PSP may monitor the incoming HTTP headers to ensure that the customer originated from the expected e-commerce site or is using a common browser. Some browsers will hide this information for privacy reasons so it cannot be relied upon with full accuracy, but an increase in missing referrer information or non-standard browsers can be an indication of fraud or compromise.
Identity Verification	While somewhat more expensive than other verification methods, confirming the identity of the customer against third-party sources such as credit files or public records can reduce fraud. Verification may also include checking the validity of address information against postal system databases or validating phone numbers through text or voice confirmation.
Prohibited Data	Blocking specific cardholder name, credit card BINs, card types, e-mail domains, phone numbers, addresses, etc. may be useful for merchants that need to block transactions manually based on known customer characteristics or history of abuse. PSPs may also offer access to databases with known abuse data.
Other Proprietary Filters	Some fraud detection may occur based on algorithms or heuristic transaction evaluation that is based on proprietary methods. While the approach itself may not be disclosed to the merchant, these services can vary in their effectiveness at identifying fraud.

PSPs should also implement multiple transaction security and fraud controls to provide merchants with options to configure and respond to suspicious activity:

Additional Unusual Activity Detection Options

Action Type	Description
Scoring	Many of the tests above cannot be acted on alone, as they may do not constitute a clear indication fraud or security compromise. In addition, excessive false positive alerts tend to lead to monitoring complacency. Scoring systems generally assign risk to each marker or transaction and raise alerts or take automated action only when a designated threshold is met within a single transaction, or between multiple transactions.
Alert	An e-mail alert or other notification may be sent to the merchant for any transaction that fails one or more tests, allowing for human review or verification of the transaction and prompt escalation for fraud or security incident response.
Reject	It is recommended merchants reject transactions that are clearly fraudulent or exceed merchant risk tolerance; however, legitimate sales could also be rejected. Rejections should always be accompanied by alerts or reporting to ensure spikes in rejected transactions over time are cause for review.

These services are not required for PCI DSS compliance, but complement any e-commerce merchant's security program and should be considered as a part of the merchant's risk analysis and incident response plan.

2.11.3 Tokenization

Tokenization at a high level allows businesses to avoid having to access or store CHD. Tokenization allows for the replacement of the payment card number with a token (referred to as an acquiring token—for more information see FAQ 1384) that may be used post-authorization but only by the merchant to whom the token is issued. If a merchant's environment were breached, the tokens would be useless for purchases at any other merchant, CP or CNP; hence, there is no incentive for criminals to steal tokens.

Keep in mind that the initiation of a transaction begins with actual CHD, which is still transmitted along a secure network to the tokenization provider's secure vault. Subsequently, a token is then derived and sent to the merchant who can then use the token internally without concern of having CHD transmitted throughout its network. Depending on the service provider offering, merchants may or may not be provided with encryption "keys" which would allow them to request access to the sensitive information stored within the provider's vault if a business need were to arise. Processes and systems used by the merchant to handle that de-tokenized payment card data would then be subject to PCI DSS requirements. This is something to consider in the event of addressing a chargeback. Typically, the final four digits of a card number are sufficient for managing chargebacks and refunds. Merchants still face some challenges. Regardless, potential solutions exist that may help even though the merchants receive payments originating from various card brands and organizations.

2.11.4 Encryption and Temporary Storage

Encryption is a vital aspect for protecting a merchant's cardholder data environment, including e-commerce implementations. Encryption of CHD does not remove it from scope of the PCI DSS. Merchants must carefully consider the capabilities of the e-commerce solution to ensure that strong cryptography is used to secure CHD. This includes data in transit and in storage (even temporarily) and must be able to maintain and monitor the security of encrypted CHD in accordance to PCI DSS.

Encrypted Transmission

Per PCI DSS Requirement 4.1, cardholder data must be encrypted across open, public networks. Businesses must question potential SPs with respect to their adherence to this PCI DSS requirement. As noted further in PCI DSS Appendix A2 regarding SSL, "all service providers must provide a secure service offering"—this includes acquirers, processors, and gateways as well. If a service provider is not able to verify that a merchant has indeed adhered to this mandate and is not able to supply a remediation plan to support its activities towards meeting this requirement, the merchant should consider selecting a different SP. It is also recommended that merchants ensure their systems are using a secure protocol and, if applicable, the service provider can support that protocol.

Encrypted Storage

Many merchants who opt to utilize an e-commerce solution may not consider the potential for the e-commerce solution to store CHD in some manner. Even if the merchant has received a fully outsourced e-commerce solution, unless specifically noted as a service option, the merchant should ask the potential SP for specifications regarding the manner in which CHD is handled from acceptance to transmission. Many e-commerce solutions may store CHD and sensitive authentication data (SAD) prior to authorization, and that data must be secured in compliance with applicable PCI DSS requirements. This may become a larger issue if the same data remains on the SP's servers post-authorization, as it is prohibited to store SAD post-authorization. Questions a merchant may want to ask its service provider include the following:

- Does the solution ever receive CHD or is a redirect or payment iFrame used for the payment process?
- Is CHD ever stored temporarily in memory or on disk before it is transmitted for processing? If so, what efforts are made to remove the data properly? Is this data encrypted while at rest?
- If SAD (for example, CVV2) is collected for authorization, is the data securely removed once the solution gives up trying to authorize the transaction? What is the defined retention period for CHD and what is the process for securely deleting this data?
- What cryptographic architecture is used to secure the stored CHD? (After 30 June 2018, SPs are required to document this as noted in PCI DSS Requirement 3.5.1.)

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 31

2.11.5 Cardholder Data Caching Avoidance Mechanisms

E-commerce solutions should be developed in a manner that minimizes the risk of caching CHD in intermediate consumer systems.

Web forms should disable autocomplete for fields accepting payment details, as this may cause the web browser to store a copy of those details after submission.

Merchants may consider the use of “password-type” fields for sensitive information. The fields have the benefit of masking input as it is typed, defending against shoulder-surfing attacks; however, this may also increase the incidence of errors during the payment process as the cardholder makes typing mistakes.

Form submission should use “POST” methods rather than “GET” methods, as described in the HTTP specification. In addition to being semantically correct, it is common for browsers, proxies, and web servers to cache or log the contents of GET variables or query strings, which may result in clear-text CHD being stored in numerous locations for a single payment. These systems are generally not designed to store POST variables, as these often contain other sensitive data (such as passwords).

Note that in some implementations, the use of POST is infeasible. This is common in the case of payment processors providing support for legacy browsers, as the same-origin policy (SOP) prevents a website hosted on one domain (e.g., the merchant) from using POST to send data to another domain (e.g., the payment processor). Cross-Origin Resource Sharing (CORS) was designed to allow domains to communicate with each other in a controlled manner and bypass this restriction, but is not supported by some older browsers. In these cases, merchants and service providers should aim to support POST wherever possible, supporting GET only where strictly necessary, and never by sending the data in a URL query string. Use of older browsers may also create difficulty meeting applicable PCI DSS requirements.

2.11.6 Third-Party Content in Payment Forms

Payment forms should be developed to avoid the inclusion of any third-party content, or to restrict any third-party content to only that which has been thoroughly vetted and is trusted.

Any third-party content (images, scripts, or other content) included on a payment form is an opportunity for an attacker to silently steal CHD.

Third-party content may include analytics, testing packages, content optimization, fraud detection, or any other service. In some cases, service providers providing logos (e.g. “security seals”) deliver these as scripts. Scripts included in a merchant website in this fashion run with the same permission as the merchant’s website, so in this way the merchant is not protected by the SOP.

The net result of this is that these scripts can modify any element on the page, including monitoring all keyboard input and copying the contents of the page or payment forms to other servers. Effectively, any script running on a website has complete control over that website. If payment websites include content from third parties, a compromise of the third party will result in an attacker gaining control over the payment website.

Although this is a relatively obvious attack vector, similar problems can be caused by elements other than scripts. Attacks have at various points in history been executed from images, style sheets (CSS), and other HTML elements using browser content-type sniffing. Merchants developing e-commerce solutions should assume that any third-party element might be unsafe.

Merchants and service providers can use a Content Security Policy (CSP) to limit the inclusion or behavior of some third-party elements, but this is not a fail-safe.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 33

3 Public Key Certificate Selection

3.1 Brief History on SSL and TLS

There has been a good deal of confusion about SSL vs. TLS since early 2015, and this section is intended to address the points of confusion. Per the PCI SSC *Migrating from SSL and Early TLS:* "SSL/TLS encrypts a channel between two endpoints (for example, between a web browser and web server) to provide privacy and reliability of data transmitted over the communications channel." Because of the deprecation of SSL and early TLS, both protocols no longer "…meet the security needs of entities implementing strong cryptography to protect payment data over public or untrusted communications channels." SSL/TLS is also used to describe digital certificates that provide a level of authentication between the browser and the web server. These certificates are used to deliver both encryption *and* authentication.

In other words, having a certificate on a website provides for the encryption of data being transmitted from the browser to the web server (so the data cannot be intercepted over the Internet by an eavesdropper), and the certificate authenticates the web server (so the sender knows that the CHD or other data the browser is sending to the web server is actually going to the right web server, and not a phisher or a cyber-thief). This is true for both SSL and TLS certificates, which are often referred to as "certs," "SSL certs," and "TLS certs."

Nevertheless, when talking about the security protocol that is used between the browser and the web server for encryption of data, "SSL" and "TLS" have different meanings. Appendix A2 to PCI DSS 3.2 provides guidelines for replacing TLS 1.0 and any version of the SSL protocol (e.g., SSL 1.0, SSL 2.0, or SSL 3.0) with a secure alternative, such as TLS 1.1 or higher (TLS 1.2 recommended). To check the protocol used on a given website, see the discussion about tools in Section 3.4, "Tools for Monitoring and Managing E-commerce Implementations."

3.2 Selecting the Certification Authority

Certification Authorities (CAs) and their resellers provide SSL/TLS certificates. Some things to consider in selecting a CA (and things which a merchant might want to consider adding to an RFI/RFP) include looking for documentation and/or evidence that:

a) Security is core to the CA's business.

b) It has a history of upstanding reputation, reliability/uptime, and trustworthiness.

c) It provides 24/7/365 customer support that is readily available—for example, by e-mail, phone, and chat.

d) It provides industry-standard authentication practices.

e) It separates authentication, support, and sales processes.

f) It provides a cloud-based console for certificate management.

g) It provides highly reliable Certificate Revocation Listing and Online Certificate Status Protocol services.

h) It has a history of WebTrust audit compliance.

i) It provides warrantees for services.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 34

3.3 Selecting the Appropriate Type of Public Key Certificates

SSL/TLS certificates have many features, technologies, and characteristics, many of which change over time. Some things for a merchant to consider in specifying its needs (and to consider adding to an RFI/RFP) include:

a) Authentication method (Refer to Section 4.1, "Certificate types (DV, OV, EV) and associated risks.")

b) Core SSL/TLS certificate capabilities/features:

   i. Authentication methods (DV, OV, EV)
   ii. Support for Subject Alternative Name (SAN), wildcards, Internationalized Domain Name (IDN)
   iii. Validity period
   iv. 128/256-bit encryption
   v. Support for multiple currently-approved (by NIST or PCI) encryption algorithms
   vi. Support for multiple key lengths based on currently-approved (by NIST or PCI) encryption ciphers
   vii. Breadth of browser support
   viii. Re-issuance of certificates

c) Optional/added-value capabilities/features of a CA:

   i. Trust seal(s) provided by CA as an additional form of "signaling" to the user that its website has been authenticated and is encrypted, as well as to increase conversions and to decrease shopping-cart abandonment. CA's seal-related infrastructure/services should be subject to the industry-standard security controls—e.g., delivered via HTTPS and tested for no vulnerabilities.
   ii. Scanning for malware or vulnerabilities ***Note:*** *these scans do not take the place of a PCI-approved ASV scan, which comes with an "Attestation of Scan Compliance."*
   iii. Certificate management: console, discovery, renewal
   iv. Third-party certificate management—inventory, certificate characteristics, violation of corporate policy (e.g., weak algorithms, expiration too long), identification of certificate misuse, etc.

d) Pricing:

   i. Brand-related pricing
   ii. Authentication method-related pricing
   iii. Volume discount-related pricing
   iv. Validity period-related pricing
   v. Support level-related pricing

3.4 Tools for Monitoring and Managing E-commerce Implementations

While there are free tools available to monitor and manage an e-commerce implementation of TLS certificates, these tools may not work for every organization. For those who are looking for tools or services with different functionality or need to address organizations with larger, more complex, environments, consider commercially available services and tools with features such as these:".:

- Check the certificate (common name, key size/type, certificate transparency, validity period).
    - These checks ensure the common name syntax is correct, the key size meets the minimum length requirements, the type is valid (e.g., RSA or ECC), the certificate transparency timestamp is included, and the validity period does not exceed the maximum allowed.
- Check the certificate chain, intermediate CA, and root CA.
    - These checks verify that the certificate has a proper chain, and that the chain is to a known intermediate and public root.
- Check for supported ciphers and protocols, and any vulnerabilities.
    - These checks verify that the cryptographic cyphers and protocols are of the allowed type.
- Check for OpenSSL vulnerabilities
- Check for server vulnerabilities

It is recommended that merchants schedule periodic tests to ensure the quality of the TLS certificate implementation and to also schedule tests after changes to certificates, web servers, load balancers/application delivery controllers, network changes and any other major change.

4 Encryption and Digital Certificates

As discussed in Section 3, digital certificates provide a level of authentication between the browser and the web server. These certificates are also used to deliver encryption of data transmissions between the browser and the web server. Because certificates can provide both authentication and encryption, merchants need to understand those services and how the different types of certificates deliver those services.

4.1 Certificate Types (DV, OV, EV) and Associated Risks

This is where authentication comes in. Authentication means, "How do I know the true identity of the merchant to which I am sending my data"? The CAs (certificate authorities) providing TLS certificates are providing three different ways of authenticating servers: domain validated (DV), organization validated (OV) and extended validation (EV) certificates. DV has the lowest cost, OV is in the middle, and EV has the highest cost.

One may argue that secure e-commerce is possible only when there is a high level of trust in the transaction. How is that level of trust defined, what are the proper security criteria, and are there different types of e-commerce which merit different conditions of trust? The following paragraphs discuss certificate types and how they may be used to identify, evaluate, and authorize parties to a transaction. Please note while all certificate types may be able to meet the PCI DSS requirements for encryption of transmissions over public networks, certain certificates may not always be appropriate for a particular circumstance.

For example, one type of certificate may be practical in the context of a typical business-to-consumer (B2C) e-commerce transaction (i.e., a website accessed by a person with a browser or mobile device), but may not apply for machine-to-machine (e.g., B2B) or an automated API-based transaction where a human is not involved. In the latter, the digital certificate is there to provide only encryption, not authentication.

Only recommendations on the use of digital certificates are being presented; it will be up to the merchant to determine ultimately, which type of certificate best meets its needs.

Historical Perspective

In the early days of the Internet, the only type of SSL certificate available was an OV certificate. With this type of certificate, the CA would validate certain business information along with the domain name to ensure not only the chain of trust but also that the entity "is who it says it is." For example, to purchase a website certificate for *example.com*, Example Inc. would send the CA some information from the web server along with proof that it was a real company. In addition, the person requesting the certificate was verified to be an employee of the company. The CA would validate this data (this could take 2-5 business days) and then issue the certificate to the organization for the website.

This worked fine for many years but some organizations complained about the time involved to verify business details and wondered whether someone could come up with a quicker solution that still provided the necessary encryption. In the early 2000s, a new type of certificate, called DV, appeared on the market. This certificate was issued very rapidly because it required only that the applicant evidence its ability to use a domain name; there was no validation or verification of any other business information. For example, if someone purchased the domain *www.example.com,* they could obtain a DV SSL certificate for that domain

simply by applying to a CA and responding to an e-mail sent by that CA to an address such as webmaster@example.com. Once the CA received the response, the certificate would be immediately issued. Only the domain name was put into the certificate—not the organization, its address, or any other information—because the CA had access to none of that information. The organization could then set up a website for www.example.com and begin accepting credit cards securely. Consumers would see the padlock in the browser, indicating that all traffic was encrypted to/from the server via SSL/TLS. The obvious problem here was that there was not any mechanism to independently verify and validate that www.example.com was actually a legitimate business—and not someone committing fraud.

In response to complaints from various parties, as well as to strengthen the authentication processes and Internet data-in-transit security, CAs and browsers formed an industry association called the "CA/Browser Forum" in 2006 to address matters such as this. Early participants of this forum included Microsoft, Symantec, Comodo, Entrust, and Mozilla. The first contribution from this industry group was specifications for the EV certificate. In this case, the CA performs enhanced vetting of the applicant to increase the level of confidence in the legitimacy of the business. The browser display is enhanced, and a user can readily discern the difference via visual indicators—usually a green lock or address bar, which indicates that the website is using an EV certificate. This makes it much easier for the consumer to know that the identity of the website has been thoroughly verified. All browsers show the organization name to the left or right of the URL. Enhanced vetting makes EV certificates much harder to obtain, in part because phishers and cyber-criminals do not want to share information about their real identities.

"In a study of phishing sites using HTTPS between March 2014 and June 2015, Netcraft found that more than 77% of the SSL/TLS certificates used were domain validated (DV)," according to Robert Duncan of Netcraft. Current statistics on the certificates used by phishing sites blocked by Netcraft can be found at http://toolbar.netcraft.com/stats/certificate_authorities.

Recommendations

For a relatively small additional cost (compared to a DV certificate), a legitimate business conducting e-commerce could purchase an OV or EV certificate. This would prove to the consumer the business was validated by the CA and has provided address and other independently verified contact information in the certificate that the consumer could use in case of questions or problems. In addition, EV certificates provide another benefit: a visual cue (the green bar) in the browser tells the consumer the business has gone through the effort to obtain this enhanced certificate, the information has been verified by the CA, and there is a higher probability that online trust can be established. The table below summarizes the various certificate levels.

TLS Certificate Level Summaries

Certificate type	HTTPS encrypted?	Padlock displayed?	Domain validated?	Address validated?	Identity validation	Green address bar?
DV	Yes	Yes	Yes	No	None	No
OV	Yes	Yes	Yes	Yes	Good	No
EV	Yes	Yes	Yes	Yes	Strong	Yes

Following are best practices associated with the table above:

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 38

- **DV:** The lowest level of authentication, for situations only where trust and credibility have low risk, e.g., B2B or machine-to-machine type of communication where a consumer is not directly involved. DV certs are acceptable when used between entities that have a formal business relationship and contract in place (which authenticates and documents the relationship between the entities), and the DV cert's role is that of encrypting data-in-motion between the parties.
- **OV:** A more secure step where the CA vets the business before issuance of the certificate, recommended for public-facing websites dealing with less sensitive information.
- **EV:** The highest level of authentication of the business by the CA, recommended for websites handling CHD, PII, and other sensitive data.
- It is recommended the certificates (certs) be configured to use the highest level of security available regardless of the type of certificate used.

4.2 TLS 1.2 Configurations

4.2.1 Importance of Modern Encryption for E-commerce

PCI DSS Requirement 3 broadly delves into the protection methods for safeguarding stored CHD. In particular, Requirements 3.5 and 3.6 speak to the requirement to secure cryptographic keys and replace them when their integrity is weakened. In order to assure an orderly transition when a class of keys becomes weakened or an algorithm is no longer considered a strong cryptographic function, it is important that organizations enable support for modern encryption methods with high integrity well ahead of older algorithms being deprecated or disallowed. As an example, organizations deploying TLS need to be aware that different versions and configurations of TLS vary in the level of integrity provided, and simply deploying TLS does not protect against deprecation. The PCI SSC published *Migrating from SSL and Early TLS* to help organizations understand how to go about deprecation planning. Additional guidance and/or recommendations regarding modern TLS configurations can be found in NIST Special Publication 800-52 Revision 1, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations." (This publication provides a general TLS overview, recommended minimum server/cryptographic/TLS extensions requirements, and general operational considerations. As with all special publications, it is recommended that organizations periodically follow up with the source to determine whether any document revisions have been issued.)

Organizations deploying TLS should ensure that they are using best practices for modern TLS. These may include:

- Using and supporting only TLS 1.2, to ensure that modern encryption methods can be utilized for protecting data.
- Separating authentication and key-agreement protocols to use different cryptographic keys, serving to reduce the impact of unauthorized key usage or key disclosure.

- Choosing key sizes and hash functions for digital signature generation and key agreement rated as acceptable by NIST Special Publication 800-57 Part 1 Revision 4, "Recommendation for Key Management" to assure integrity of the transaction.
- Ensuring clients utilize current TLS options and ensuring servers select current TLS options when negotiating with clients.

By adopting these practices now, organizations conducting e-commerce can help maintain trust by assuring continued protection of customer data and avoid compatibility challenges as older encryption algorithms weaken.

4.2.2 Certificate Transparency

Certificate Transparency (CT) is a Google-initiated framework (defined at www.certificate-transparency.org) and is a new technique for further protecting the SSL/TLS ecosystem. At a high level, it requires CAs to submit information about each SSL/TLS certificate being issued to multiple CT log files. These log files can be viewed publicly, along with the domain name of the web server.

The main advantage to CT is that an enterprise could monitor the CT log files and discover issuances of SSL/TLS certificates in its name that were not approved. For example, a company like Example Inc. might have a policy that "we only work with a particular CA, and any SSL/TLS certificate for https://*.example.com must be issued solely by that CA." Example Inc. could then monitor the CT log files and learn that an SSL/TLS certificate for https://phishingserver.example.com was issued by a CA other than its approved CA, and take steps to have that SSL/TLS certificate revoked.

A number of companies, in multiple sectors (banking and financial services, e-commerce, payment processing, content-delivery services, etc.) have expressed objections to the public availability of their web servers' domain names being, and have chosen to opt out of using CT. If the company chooses to opt out, Google Chrome today makes the EV cert look like a non-EV cert (no green bar). A new CT spec is being reviewed and once it is approved and is deployed, customers who choose the "privacy feature" will be able to "redact" some portion of the fully qualified domain names in their CN and SubjectAltNames, but the domain name will still appear in the CT log file (so phishingserver.example.com will appear as example.com).

4.3 Merchant Questions on Certificate Types and TLS Migration Options

This is an initial set of questions or concerns that a merchant might have, followed by some helpful guidance:

- ***I am a small business so surely no one is going to attack me if I continue to use SSL and early TLS.***

  Unfortunately, small businesses are just as susceptible to attack as larger organizations. Hackers use computer programs that systematically perform exhaustive searches for targets that are misconfigured or contain exploitable vulnerabilities. Hackers and their computers do not care how big or small an organization is that is utilizing a vulnerable system. We tend not to hear about small merchant

breaches because the businesses are not well known and the breaches too numerous. It is just a matter of time before any vulnerable system is exploited.

The cost of a breach, even for a business storing a small number of credit cards, will far outweigh the cost it will take to migrate to TLS 1.2. For the small business that has outsourced all or part of its payment processing to a PCI DSS compliant SP, the service provider will mandate the migration to TLS 1.1 and/or TLS 1.2. The merchant will be required to adhere to the SP's timeline for migration to ensure connection protocols for payment transactions continue to function.

- ***My SP tells me that it supports later versions of TLS—is that all I need to do to meet the PCI DSS requirements on TLS?***

  While support for the later versions of TLS (1.1 and 1.2) is good, the retention of support for the TLS 1.0 and any version of SSL still introduces a potential weakness in the environment unless appropriate compensating controls are implemented and maintained. In terms of PCI DSS compliance, then, SPs must support the use of later versions of TLS (currently 1.1 and 1.2) and must only support later versions of TLS for new implementations. Service providers can still offer SSL and TLS v1.0 up to 30 June 2018 for existing services, provided the SP has implemented appropriate risk-mitigation controls.

- ***How can I find out what SSL/TLS protocols and versions I support?***

  Although there are companies that provide testing services, one way of finding out whether your website supports a particular version of SSL or TLS is to use a computer browser to connect to the site and actually establish a secure connection. If you can connect using https, not http, and you can see the locked padlock, you have successfully established a secure connection. ***Note:*** *Only TLS 1.1 or 1.2 connections are considered strong cryptography and supported secure encryption protocols. Each type of browser provides options that enable you to select specific versions of both SSL and TLS, so by a process of elimination you can quickly establish what is actually supported.*

- ***As a merchant, many of my customers, either because of policy or because of in-house systems incompatibility, do not have the latest software. Therefore, this may limit the versions of TLS that are available for them to implement. What can I do to be compliant without losing my customers?***

  The best solution is to (1) develop a TLS mitigation plan to disable all early versions of TLS and migrate to TLS 1.2; (2) until the migration is complete, the merchant must address the vulnerabilities associated with the use of insecure protocols through risk-mitigating compensating controls. The PCI Information Supplement, *Migrating from SSL and Early TLS,* provides guidance on developing the migration plan and implementing risk-mitigating controls, including control recommendations for small merchant environments.

  Organizations that are unable to discontinue use of solutions that do not support the latest version of TLS must perform an ASV scan quarterly to verify that compensating controls continue to effectively mitigate known and newly discovered vulnerabilities associated with the insecure protocols. Merchants should contact their acquirer to discuss business requirements, limitations of current solutions, and compensating controls in place or planned to address risk to the merchant environment.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 41

- ***I am a small business and will need to upgrade my systems to support the latest versions of TLS at great expense. What can I do to remain secure until I can upgrade?***

  Until the migration to TLS 1.1/1.2 is complete, a small business must address the vulnerabilities associated with the use of insecure protocols. The PCI SSC Information Supplement, *Migrating from SSL and Early TLS,* provides guidance on implementing risk-mitigating controls, including recommendations for small merchant environments. Merchants should also talk to their acquiring bank or payment card brand to determine whether there are any other requirements that must be met.

- ***If I stop taking card payments and only accept payments through alternative methods, do I still need to do anything about SSL/TLS?***

  Engaging with e-commerce SPs to handle all or part of the payment processing will most likely reduce the PCI scope and costs associated with PCI compliance for the merchant; however, it does not relieve the merchant of the ultimate responsibility to meet at PCI DSS requirements including any related to SSL/TLS security:

  - The mobile wallet pay technologies utilize protocols already in place with most swipe and EMV payment terminals. In fact, these implementations, including transactions utilizing the older magnetic swipe terminals, are more secure than regular card-present transactions. This is because tokenization and biometrics on the user device provide a unique, surrogate value that is a substitute for the payment card information (see Section 2.11.3, "Tokenization"). The payment card information is not available to the merchant or the acquirer, and it cannot be reversed engineered to reveal the CHD. This has the benefit of reducing the scope of the cardholder data environment (CDE). Merchants utilizing payment terminals to enable Apple Pay and Samsung Pay transactions that can be verified as not being susceptible to all known exploits for SSL and early TLS may continue using these protocols as a security control. Merchants should contact their acquirer to ensure terminals are PCI validated.

- ***Can I create my own SSL certificates or must I buy them from a commercial CA to be compliant?***

  When the owner of the web server creates SSL/TLS certificates, they are called "self-signed certificates." There are two very significant problems created by doing this:

  - **Lack of recognition by browsers**: The browsers do not know about self-signed certificates, and users will receive "scary dialogs" that a particular website is not trustworthy. This alone should guide legitimate e-commerce merchants to use commercially available SSL/TLS certificates.
  - **Lack of independent verification:** If the only form of authenticating a website is the owner saying, "trust me because I am who I say I am," then the merchant knows nothing about that site (or its owner). This is what phishers and cyber-thieves want: lack of insight into who operates the web server that is purporting to be legitimate.

  The SSL certificate demonstrates to your customers that your site is a safe place to conduct e-commerce transactions. In effect, easily verifiable certificates show that your site is to be trustworthy. While self-certification is operationally allowable and technically feasible, a third-party certificate

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 42

authority adopting universally accepted standards and practices can more effectively and clearly demonstrate the safety and security of your site. Hence self-certification in e-commerce is not recommended.

- ***—Are "SSL Certificates" still OK to use? All the technology, marketing, and instructional literature I see references "SSL Certificates". What is the difference between an SSL 3.0 certificate and a digital certificate?***

  Most digital certificates are advertised as "SSL Certificates" even if they are not using the SSL protocol. These may be acceptable to use only if they are actually using TLS 1.1 or higher as the security protocol.

  Also, most offers for "free SSL certificates" refer to domain-validated (DV) certificates, which were covered in Section 4.1, "Certificate Types (DV, OV, EV) and Associated Risks." DV certs are not recommended for e-commerce transactions. For e-commerce transactions, use OV or EV authenticated SSL/TLS certificates.

5 Guidelines to Determine the Security of E-commerce Solutions

There are many considerations for determining the security of an e-commerce solution. It is recommended that a merchant determine roles and responsibilities—for both itself and any third party it chooses to engage for services—for meeting for PCI DSS requirements, as well as due diligence to confirm the third party's status regarding PCI DSS compliance. The following sections provide more detail on these guidelines.

Note: *The PCI SSC Information Supplement,* Third-Party Security Assurance, *provides much more in-depth information on validation than is outlined below. These guidelines and questions are meant as a companion to that publication. The publication* Payment Protection Resources for Small Merchants: Questions to Ask Your Vendors *can also provide clarification and additional questions a merchant should ask its e-commerce solution provider.*

5.1 E-commerce Solution Validation

Merchants should be prepared to ask a number of questions of any prospective e-commerce SP, about how the SP may or may not be compliant against the various PCI standards (PCI DSS, PA-DSS).

5.1.1 PA-DSS Validated Software and Services

A PA-DSS validated shopping cart may be one of the tools used for e-commerce. This may include situations where the SP is responsible for the installation, maintenance, and development of the e-commerce platform, including the shopping-cart functionality. In this case, the question should be asked whether the shopping cart has been validated per and can be verified by looking for the software on the PA-DSS Validated Applications listing. Additional questions/assurance should be obtained to ensure the PA-DSS application was installed as per the implementation guide (IG). Expiration dates of the PA-DSS application should be recorded, and updated documentation should be obtained to ensure the PA-DSS application remains on the List of Validated Payment Applications.

5.1.2 Service Provider Validation

As per PCI DSS Requirement 12.8.3, the merchant should develop a process to engage service providers. This engagement process should consider validation level of the service provider. While the DSS itself does not set validation levels, the card brands may set guidance on the level of validation required for compliance, for both merchants and service providers. Merchants should look at whether any SP should meet the same level of validation as the merchant must, which may require inquiries to the card brands or acquiring banks. If additional requirements must be met, this may influence the selection of a SP.

Additional factors that may influence this decision include the merchant's appetite for risk, additional internal pressures driving the level of acceptable assurance, and any needs of the merchant's customers. Ultimately, the merchant is responsible for its PCI DSS compliance, which may be impacted by the SP PCI DSS compliance status, and must therefore exercise careful due diligence.

Where service providers have not undertaken their own PCI DSS assessment, the merchant should make sufficient enquiries to understand the security controls the service provider has in place and perform a

risk assessment as to whether or not those controls meet PCI DSS requirements. The outcome of these inquiries should be taken into account before signing any contracts.

5.1.3 Other Validation or Assessments

PCI DSS is not the only set of standards that exist for e-commerce and security purposes. If your industry or business requires additional guidelines for a solution, care should be taken to ensure that any provider chosen meets these requirements as well. However, it is important to keep in mind that meeting other security compliance guidelines and security certifications does not guarantee PCI DSS guidelines are met.

PCI DSS does not require service providers to undergo a self-assessment or QSA-led PCI DSS assessment. This is an acquirer or payment brand determination. There are multiple reasons why it may be advantageous for a service provider to undergo such a PCI DSS assessment.

5.2 Validation Documentation

PCI DSS compliant service providers should have PCI SSC documentation (for example, the Attestation of Compliance or AOC) to support their compliance status. Although service providers can redact sensitive information from this document, the intent is that the document provides enough detail about the scope of assessment within the AOC such that a merchant can determine whether the assessment covered the services being provided it. It is recommended the signatories and dates be carefully checked to ensure the AOC is credible. If enough assurance is not possible from the AOC, additional details may be requested of the service provider. Other types of documentation may be requested and accepted by the merchant. See Section 3.2.2 of the PCI SSC Information Supplement, *Third-Party Security Assurance*.

Where PA-DSS applications support services provided, the applications in use and any expiry dates can be confirmed though the PCI SSC website's List of Validated Applications.

It is recommended the supplied documents be checked to ensure they cover a valid version of the PCI DSS, when the documents are dated, and cover the services provided. Best practice is to record the dates on these documents so revalidation can be checked on the anniversary dates.

In addition to the PCI DSS documentation to support the service provider validation, the service provider may be asked to provide supporting documentation to help the merchant work on Requirement 12.8.5, which requires the merchant to identify which PCI DSS requirements are managed by the entity, the service provider, or both. (See the "Sample PCI DSS Responsibility Matrix" in Appendix B of the *Third-Party Security Assurance* Information Supplement.[2])

[2] *PCI SSC Information Supplement: Third-Party Security Assurance*

5.3 PCI DSS Requirement Ownership

As an e-commerce solution is evaluated, it is important to understand what requirements from the DSS that the solution meets on behalf of the merchant. There are several aspects to this a merchant may want to consider:

- The PCI DSS scope of the solution, the requirements covered by the service provider, the joint services, and use of compensating controls should be covered in the service provider's AOC.
- Per PCI DSS Requirement 12.8.5, the merchant needs to understand any requirements it is responsible for meeting.
- The merchant is responsible for understanding how both internal and external ASV scans and penetration tests are conducted, who will maintain copies of test results, whether the service provider will assist the merchant in remediating any failed tests, and whether the merchant will have access to copies of the test results to meet its obligations for PCI DSS Requirements 11.2 and 11.3.
- It is highly recommended a merchant understands whether the service provider will have access to its account data or its cardholder data environment, and what risk that may involve the merchant.
- The merchant should be aware of nested service provider arrangements—i.e., a service provider outsourcing to another service provider—and should be aware of how those relationships affect the services being provided to the merchant.[2]
- Merchant and service provider should both understand and have documented who is responsible for what, exactly what requirements each must meet, and how they will meet any joint requirements.

5.3.1 Legal and Contract Considerations

Legal and contractual questions should be raised when selecting a service provider as well. The Third-Party Security Assurance document[3] expounds on questions and guidelines a merchant may use. Additionally, any consultation on contracts or requirements may raise the following additional questions:

- What information disclosure can be given as part of an audit or investigation that is not normally disclosed or is redacted due to security concerns?
- What support, feedback, or general inquiry SLAs are defined as part of the service agreement? Does this include support or assistance in case of an audit or PFI investigation?
- How are evolving guidelines handled?

[3] *PCI SSC Information Supplement: Third-Party Security Assurance*

6 Case Studies for E-commerce Solutions

6.1 Case Study One: Fully Outsourced Redirect

Case Introduction

ABC Retailer is a typical brick-and-mortar designer clothing retailer. Over the past five years, ABC has expanded to more than 20 retail outlets, offering designer clothing at discount prices. Recently, ABC expanded into the e-commerce market, offering customers a feature-rich website that allows them to pay for goods online with either click-and-collect or delivery options available.

Merchants often want to simplify their security and PCI DSS assessment efforts. For purposes of this case study, simplification is achieved using a redirect to a service provider's (SP) payment page or by utilizing an embedded payment form within an iFrame on the merchant's website.

Description of Environment

ABC has outsourced its e-commerce website to a third-party company called PCIWeb Hosting Co. PCIWeb Hosting Co. is responsible for the installation, management, and maintenance of the web-hosting platform and for all development work for the ABC website. A firewall is deployed between the Internet and the ABC website, which is running on a virtual private server (VPS) within its own isolated virtual network. The web server is deployed with a LAMP (Linux, Apache, MySQL, PHP) stack, running Magento as the content management system (CMS) driving the ABC e-commerce site.

A URL redirect is utilized to redirect users to ABC's payment service provider (PSP), XYZ PSP Co., for all cardholder data submissions.

Payment Flow

The following diagram depicts the customer journey and cardholder data flow for ABC's URL Redirect e-commerce implementation.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 47

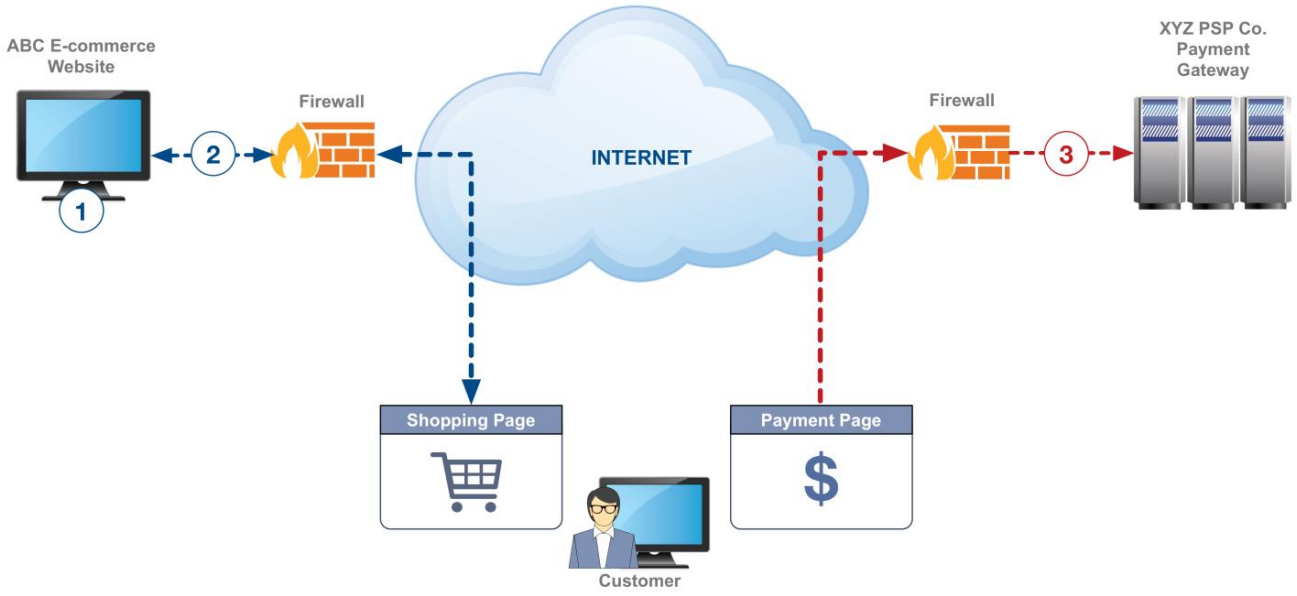

Figure 8 – Fully Outsourced Redirect Payment Flow

1. The user browses ABC's website to build a shopping cart. This website is hosted by PCIWeb Hosting Co., which is a third-party hosting company.
2. The ABC website issues a redirect to the XYZ PSP Co. payment page, which is displayed within the customer's web browser.
3. The customer enters all CHD into this PSP's payment page, which is submitted directly to the PSP, who is then responsible for handling the payment functions.

No CHD is submitted to the merchant; therefore, the merchant has no cardholder data environment. ABC may be eligible to validate PCI DSS compliance via self-assessment, SAQ A, which is applicable to outsourced e-commerce environments using redirection mechanisms to redirect customers to a PCI DSS compliant payment service provider. For merchants with such implementations that are required to validate PCI DSS compliance via an onsite assessment and a Report on Compliance (ROC), SAQ A can be used as a reference for applicable PCI DSS requirements. SAQ A for PCI DSS version 3.2 includes additional PCI DSS requirements to address ongoing threats to merchant web servers that redirect customers to third parties for payment processing.

6.2 Case Study Two: Fully Outsourced iFrame

Case Introduction

ShoesInc Retailer is a pure e-commerce retailer selling designer shoes throughout multiple countries. The product range offered by ShoesInc includes sports, casual, and dress shoes across a range of child and adult sizes. Customers of ShoesInc often return to its website to make subsequent purchases. In a bid to make this process simpler, ShoesInc allows customers to save their card details; however, the customer still needs to submit the card verification value (CVV2/CVC2/CAV2/CID) each time as part of the payment process. This information is captured and stored at the PSP.

Merchants often want to simplify their security and PCI DSS assessment efforts. For purposes of this case study, simplification is achieved using an embedded payment form within an iFrame on the merchant's website.

Description of Environment

The hosting and website is fully managed and maintained by ShoesInc staff. A firewall is deployed between the Internet and the ShoesInc website, which is running in a demilitarized zone (DMZ) within ShoesInc's offices. On the internal network, an ERP system is used to manage stock within the warehouse. The web server is deployed on a Windows 2012 operating system running on Microsoft IIS. The ERP software has a front-end web service component running on the DMZ web server that links to the internal ERP.

A payment page iFrame is rendered within the customer browser to accept cardholder data. This payment page iFrame is received from ShoesInc's Payment Service Provider, XYZ PSP Co. All CHD is submitted from the customer's web browser to the PSP.

Payment Flow

The following diagram depicts the customer journey and cardholder data flow for ShoesInc's iFrame e-commerce implementation.

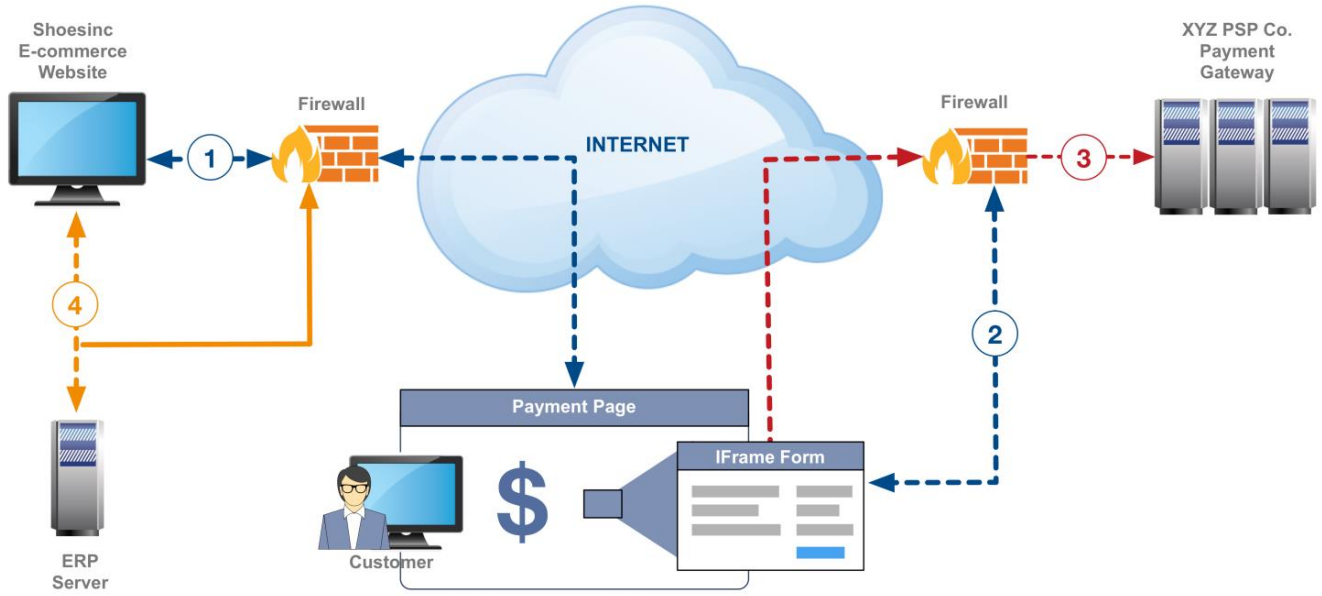

Figure 9 – Fully Outsourced iFrame Payment Flow

1. The cardholder browses ShoesInc's website, filling a shopping basket before reaching the payment page.
2. ShoesInc's shopping cart embeds an iFrame with a payment form (received, in its entirety, from the PSP web server) to the customer's web browser.
3. The customer enters all CHD into this embedded iFrame, which is submitted directly to the XYZ PSP Co., who is then responsible for handling the payment functions.
4. This link shows communication between the website and the ERP Server.

No CHD is submitted to the merchant; therefore, the merchant has no cardholder data environment. ShoesInc may be eligible to validate PCI DSS compliance via self-assessment, SAQ A, which is applicable to outsourced e-commerce environments using iFrames to redirect customers to a PCI DSS compliant payment service provider. For merchants with such implementations that are required to validate PCI DSS compliance via an onsite assessment and a Report on Compliance (ROC), SAQ A can be used as a reference for applicable PCI DSS requirements. SAQ A for PCI DSS version 3.2 includes additional PCI DSS requirements to address ongoing threats to merchant web servers that redirect customers to third parties for payment processing.

6.3 Case Study Three: Partially Outsourced (JavaScript-Generated Form)

Case Introduction

AutoRental is a brick and mortar/e-commerce retailer offering car and van rentals to customers across North America, South America, Europe, Asia, and Australia. Due to AutoRental's global reach, multiple payment providers are used dependent upon the customer's country of origin. To help integrate this into the payment process and to allow the payment journey to be fully customizable, AutoRental has made the decision to implement the payment flow using a JavaScript payment form, retrieved from the payment provider.

Description of Environment

The hosting and e-commerce platform (website) is fully managed and maintained by an outsourced company called PCIData Hosting. A firewall is deployed between the Internet and the AutoRental website. The AutoRental website is housed within an AutoRental demilitarized zone (DMZ) with a Microsoft SQL Server 2015 server housed within an AutoRental internal zone. The website is running on a Windows 2012 Server, using Microsoft Internet Information Services (IIS) and Microsoft ASP (Active Server Pages). The AutoRental DMZ and internal zone are both isolated networks for just AutoRental's use.

A payment page is generated by the website using a JavaScript payment form served from AutoRental's PSP, XYZ PSP Co. All CHD is entered into the payment form, which is built by the website using the PSP's JavaScript payment form. With the JavaScript payment form, the AutoRental's website is responsible for building the payment page, albeit with JavaScript code downloaded from the PSP. The cardholder data for payment is sent from the customer's web browser to the PSP.

Payment Flow

The following diagram depicts the customer journey and cardholder data flow for AutoRental's JavaScript Created Form implementation with a payment service provider for its e-commerce platform.

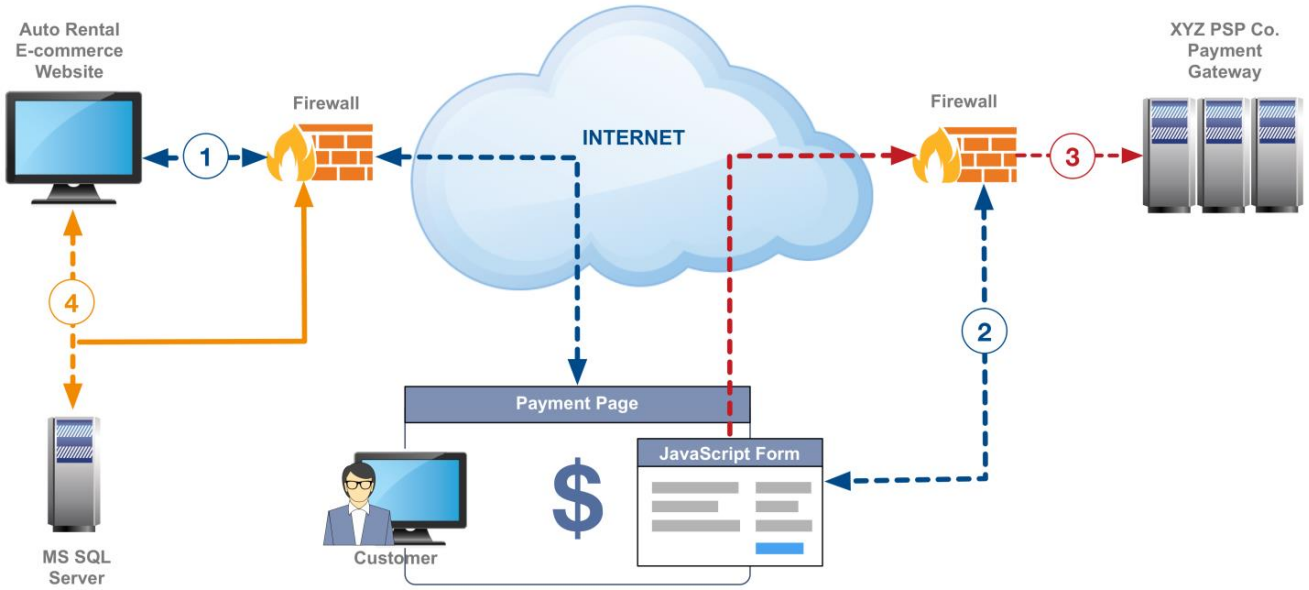

Figure 10 – Partially Outsourced (JavaScript-Generated Form) Payment Flow

1. The cardholder browses AutoRental's website, filling a shopping basket before reaching the payment page.
2. The creation of AutoRental's payment page includes building a payment form through JavaScript (received from the PSP web server) in the customer's web browser.
3. The customer enters all CHD into this JavaScript-generated payment form, which is submitted directly to the XYZ PSP Co., who is then responsible for handling the payment functions.
4. This link shows communication between the website and the Microsoft SQL Server.

Although no CHD is submitted to the AutoRental website, the payment page and form are generated per instructions from the AutoRental website. This is different from Case Study Two because here the merchant's website produces some or all of the web page that is used to accept payment data and then passes it directly to the third-party payment processor. In this implementation, the customer never leaves the merchant's website. For merchants eligible to validate PCI DSS compliance via self-assessment, SAQ A-EP is applicable to outsourced e-commerce environments. Merchants are responsible for some or all elements in the payment page used to collect cardholder data and then pass it to a PCI DSS compliant payment service provider. For merchants with such implementations that are required to validate PCI DSS compliance via an onsite assessment and a Report on Compliance (ROC), SAQ A-EP can be used as a reference for applicable PCI DSS requirements.

6.4 Case Study Four: Merchant Managed (API)

Case Introduction

LensInc is an e-commerce retailer offering affordable monthly prescription lenses. Due to LensInc being a pure e-commerce business with high transaction volumes, the payment functions integrate with an API to provide failover of payment service providers (PSP), should a payment transaction fail a secondary PSP can be tried.

Description of Environment

The hosting and e-commerce platform (website) is fully managed and maintained by LensInc staff within BigGuy Cloud Solution to provide a highly resilient infrastructure capable of dynamically increasing service capacity when required. BigGuy security groups are used to provide firewalling features along with BWS WAF (Web Application Firewalling) services to provide public-facing web application defenses. BigGuy Relational Database Services (BigGuy RDS) is used as the backend database for the web server on an internal network zone. The front-end web server utilizes Apache web server running PHP within a demilitarized zone (DMZ).

A payment page and payment form are generated by the LensInc website. CHD is submitted to the LensInc web server, where it is then submitted to one of the PSPs for authorization and settlement through an API call to the PSP. Encrypted CHD is stored in LensInc's backend database to provide easy checkout options where customers only need to provide the card verification value (CVV2/CVC2/CAV2/CID).

Payment Flow

The following diagram depicts the customer journey and cardholder data flow for an organization using an API implementation with a payment service provider for its e-commerce platform.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 53

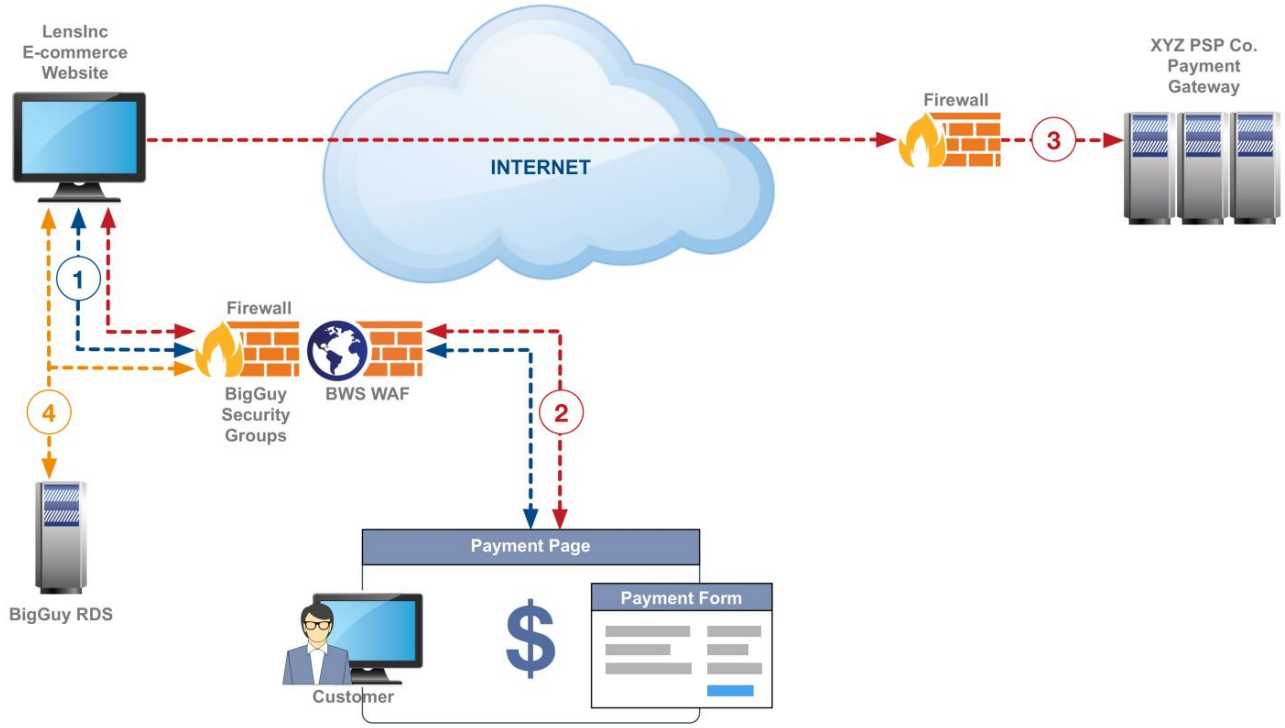

Figure 11 – Merchant-managed (API) Payment Flow

1. The user browses LensInc's website, filling a shopping basket and browsing to the payment page, issued by LensInc's website.
2. The customer enters all CHD into the LensInc generated payment form, which is submitted directly to the LensInc web server.
3. The LensInc web server stores the CHD (PAN Only) before submitting the information (including the card verification value) to the Level 1 Compliant Payment Service Provider, XYZ PSP Co., through an API.

This link shows communication between the website and the BigGuy RDS server, where CHD is stored (encrypted CHD storage, no sensitive authentication data).

For merchants eligible to validate PCI DSS compliance via self-assessment, SAQ D is applicable in this scenario. The payment brands or the merchant's acquirer may determine the merchant must complete a Report on Compliance (ROC) instead of SAQ D.

7 Best Practices

In addition to meeting the PCI DSS requirements applicable to a specific merchant e-commerce implementation, e-commerce merchants should consider implementing the additional PCI DSS requirements and some or all of the security best practices noted in this section.

7.1 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 (PCI DSS Requirement 1.1.3). Periodic review will ensure accuracy as changes to the environment may occur. Data-discovery software may help a merchant find any unencrypted PANs in the environment.

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 that store, process, or transmit cardholder data.
- Illustrate how cardholder data is processed, such as how CHD is managed within a web application's functionality, and page along with how 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) and payments processed solely within third-party environments.

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

Eliminate any cardholder data that is not needed per PCI DSS Requirement 3.1. Consolidate necessary cardholder data in known and manageable locations and isolate all cardholder data away from non-cardholder environments. These steps 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. As a reminder, sensitive authentication data (SAD) cannot be stored after authorization, even if encrypted.

7.3 Evaluate Risks Associated with the Selected E-commerce Technology

Merchants should evaluate thoroughly and carefully 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, is partially outsourced to a third party, 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 per PCI DSS Requirement 12.2.

7.4 Service Provider Remote Access to Merchant Environment

In a shared-environment e-commerce implementation, the service provider may require access to the merchant's systems to perform maintenance or other changes. It is recommended a merchant understand how and when a service provider will access its systems. Both the service provider and the merchant must meet PCI DSS Requirement 8.3, which requires multi-factor authentication for remote access into the merchant's cardholder data environment. In addition, the merchant is advised to be familiar with PCI DSS Requirement 8.1.5, which relates to a service provider's IDs on the merchant's systems. The service provider ID should be turned on when needed and turned off as soon as access is no longer needed. This limits service-provider access to the systems to only those times the merchant knows about. This also closes the door for a malicious individual to hack in using a service provider's credential if the access is always on.

7.5 ASV Scanning of E-commerce 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. ASV scans check for common vulnerabilities within the system and provide a report of those vulnerabilities. The following best practices apply to merchants using third-party hosting-commerce solutions:

- 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 its own and provide evidence of compliant scans to the merchant; or
    - The hosting provider can undergo an ASV scan as part of each of its merchants' ASV scans.
- Determine whether the service provider will provide scan reports and whether the service provider will assist with any vulnerability corrections/remediation.

Ultimately, it is the merchant's responsibility to ensure its hosted environment receives a passing result on a quarterly basis from appropriately scoped ASV scans.

7.6 Penetration Testing of E-commerce Environments

PCI DSS Requirement 11.3 for external and internal penetration testing applies to e-commerce environments as well. As with ASV scans, a merchant may not have control over the penetration testing process. The following best practices apply to merchants using third-party e-commerce solutions:

- Ensure the service provider is conducting the annually required penetration tests per PCI DSS Requirement 11.3.
- Understand and be notified when the test will be performed to ensure minimal downtime for customers.
- Understand whether the service provider will assist with any remediation necessary to correct findings or whether the merchant is fully responsible for correction.

- Ensure the service provider provides enough information on the systems to be tested to cover those services and systems provided to the merchant.
- Additional information on penetration testing can be found on the PCI SSC website document library.

7.7 Best Practices for Securing e-Commerce

- Use TLS 1.1 or higher when transmitting cardholder data internally (for example, at cardholder data ingress and egress points) throughout the network per PCI DSS Requirement 4.1.
- Due to the dynamic nature of e-commerce environments and frequent changes to websites and web applications, consider implementing a web application firewall (WAF) per PCI DSS Requirement 6.6 or additional intrusion-detection technologies per PCI DSS Requirement 11.4.
- It is also recommended that firewall rules be configured to ensure unwanted traffic does not access (both ingress and egress) the network per PCI DSS Requirement 1.2. It is important to understand the type and nature of any firewalls installed in a service provider environment that controls access to services or environments provided to the merchant.
- Follow PA-DSS when internally developing and implementing payment applications/shopping carts to help ensure that the application will follow good coding practices and support PCI DSS compliance per PCI DSS Requirement 6.3 and PA-DSS Requirement 5.
- 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 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 securely and in a manner that supports PCI DSS compliance.
- Regularly review any links (such as URLs, iFrames, APIs etc.), from the merchant’s website to the payment gateway to confirm the links have not been altered to redirect to unauthorized locations.
- Per PCI DSS Requirement 5, it is recommended the merchant check with its service provider to ensure anti-virus/anti-malware software is running on the systems provided to the merchant. If the service provider is not running AV software on the merchant’s behalf, it is recommended the merchant understand why and implement a solution of its own for those systems. It is also recommended a merchant have AV software running on the systems it manages.
- PCI DSS Requirement 10 details that a change-detection solution be in place. Typically, existing logging and monitoring tools can be configured to comply with PCI DSS requirements but it is worth explicitly asking the service provider whether a change-detection solution is in place.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 57

- Merchants are advised to ask their service providers about the intrusion-detection/prevention systems and file-integrity monitoring in place according to PCI DSS Requirement 11.4 and 11.5. They are also advised to ensure their own systems are being monitored for intrusions.

7.8 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 per PCI DSS Requirement 12.6 and the appropriate action to take in the event of a suspected breach per PCI DSS Requirement 12.10.4.
- Train technical staff to manage properly security including firewalls, digital certificates, and encryption. (PCI DSS Requirement 12.6.1)
- 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.

7.9 Other Recommendations

- Assign a specific team member(s) to monitor and report on all security alerts issued by the card brands and other security websites to stay current on emerging threats. (PCI DSS Requirement 12.5.2)
- Consider implementing an additional firewall between the application server and the database server to reduce further risks from the Internet-connected web server. (PCI DSS Requirement 1.3)
- Limit displays of PAN to the minimum necessary for the consumer to complete their purchase. For example, once the PAN is verified, don't display full PAN back to the consumer in the order summary or receipt. (PCI DSS Requirement 3.4)
- Even though it is not a PCI DSS requirement, network segmentation is an important subject to discuss with the service provider. Segmentation may help reduce PCI DSS scope if implemented properly. A merchant is advised to ensure it understands any segmentation controls a service provider has implemented.

7.10 Best Practices for Consumer Awareness

Provide awareness for consumers to protect their payment card data when making online purchases—for example:

- Do not 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.
- Do not make purchases when connected to an unsecured wireless network (for example, using your laptop computer with a public Wi-Fi connection), unless you have a personal firewall on your computer.
- Be aware of "shoulder-surfing" when 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, the little “padlock icon” at the top or bottom of the web browser, a green address bar, or a security seal before entering your payment card data.
- Use strong passwords that cannot be easily guessed (for example, do not use your date of birth or your name as a password).
- Keep your passwords private. For example, do not write them on a piece of paper attached to your computer (especially if you are in a public place), and do not save them in a file on a computer that is shared with others.

7.11 Resources

Organizations should familiarize themselves with industry-accepted best practices and guidelines for securing e-commerce environments. There is 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:

7.11.1 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 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, e-books, 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 Applications,* and *Cornucopia E-commerce Website 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.*

7.11.2 PCI SSC Resources

The PCI Security Standards 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 Guidance: Small Merchant Guidance*** – Four documents that provide additional guidance and payment protection resources for small businesses. This family of documents includes *Guide to Safe Payments, Common Payment Systems, Questions to ask Your Vendors,* and *Glossary of Payment and Information Security Terms.*
- ***PCI DSS Guidance: Third-Party Security Assurance*** – Provides additional guidance for meeting PCI DSS Requirement 12.8 and 12.9 to ensure payment data and systems entrusted to third parties are maintained in a secure and compliant manner.
- ***PCI DSS Guidance: Penetration Testing Guidance*** – 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.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 60

- ***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 provides guidance and requirements for ASVs who perform these scans.
- ***PCI DSS and 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 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).

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 61

Acknowledgments

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

Accenture
Accretive Solutions Operating Corp.
Advam Pty Ltd
Agio, LLC
Allstate Insurance
Amazon Web Services, Inc.
Amazon.com
Australian Payments Clearing Association (APCA)
Avis Budget Group Inc.
BBPOS
BDO USA, LLC
Bluefin Payment Systems
Board of Trustees of the University of Arkansas
BT PLC.
Canadian Tire Financial Services
CardConnect
Coalfire Systems
College Entrance Examination Board
Comsec
Corporate Solutions Company
Costco Wholesale
Crowe Horwath LLP
Crutchfield Corp.
CyberSource
Datatrans AG
Deloitte
Demandware, Inc.
DSW Inc.
Elavon Merchant Services
Electronic Transactions Association
Emirates/Dnata
Ernst & Young LLP
Expedia Inc.
Games Workshop Ltd
Global Blue SA
Global Payments Direct Inc.
Heartland Payment Systems
Henry Ford Health System
Hewlett Packard Enterprise Company
HSBC
Information Risk Management (IRM)
Innovative Controls Systems
Kaiser Foundation Health Plan Inc.
Kaizen Data Security Group Inc.
KYTE Consultants, Ltd.
L.L. Bean, Inc.
The Liquor Control Board of Ontario
Liverpool Victoria Friendly Society
Market America Inc.
Metlife Group, Inc.
NCC Services
Nettitude Ltd.
NIC Inc.
North Carolina State University
NTT DATA INTELLILINK Corporation
Oracle Corporation
PAN-Nordic Card Association
Parkingsoft, LLC
Patterson Companies, Inc.
PayU S.A.
Philips Electronics North America Corporation
The Regents of the University of California
RSA
RSM US LLP
SavvyPCI
Sec-1 Ltd.
SERVIRED
Shaw Cable Systems
Soft Space

Stratica International PTY LTD
Symantec Corporation
Synopsys
Sysxnet Limited DBA Sysnet Global Solutions
Tech Lock, Inc.
TrustedSec, LLC
TUI Travel PLC
U.S. Payments
UL Transaction Security
University of Oklahoma
Vantiv
Verifone
Verizon
Verizon Wireless
VerSprite
Vodat International Limited
WorldPay
Xerox

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 63

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Created in 2006 by the founding payment card brands American Express, Discover Services, JCB International, MasterCard, and Visa Inc., the Council has more than 700 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

Intuit Inc. / IQX Corp.
Exhibit 1024
Page 64