Traditionally, many merchants have been told that ecommerce technology will reduce risk and streamline PCI DSS compliance validation—but is this really the case?

Read on to learn about PCI DSS 3.0 and the potentially significant change in compliance validation for ecommerce merchants. Among other things, we will cover:

- Common ecommerce processing methods
- Threats and vulnerabilities of ecommerce technologies
- PCI validation requirements for ecommerce processing methods

PCI 3.0
“It’s about making PCI compliance part of your business, not a once-a-year, study-for-the-test kind of thing.”

✓ Clarification
✓ Additional guidance
✓ Evolving requirements

According to Bob Russo, General Manager of the Payment Card Industry Security Standards Council (PCI SSC), PCI DSS 3.0 is “about making PCI compliance part of your business, not a once-a-year, study-for-the-test kind of thing.” Among other things, the new standard is designed to:

• Deliver clarification to commonly misinterpreted standards
• Provide additional guidance and practical implementation explanations
• Address evolving requirements, new technology, and emerging threats
The three Self-Assessment Questionnaire (SAQ) types within the new standard are titled A, A-EP (electronic processing), and D. SAQ A-EP is a new addition to PCI compliance, and lies between A (easy) and D (full PCI standard) in complexity. Take a look at the slide to compare eligibility and requirements of each SAQ.
Before we dive into the ecommerce processing methods, we need to first understand the entities (players) and activities (steps) that make up the purchase process.

**The Players**

1. The Merchant, whose website contains the shopping cart
2. The Customer, who visits the merchant website via Internet
3. The Payment Service Provider (PSP), who receives data and submits payment into system

**The Steps**

1. Create form to collect payment data and send to customer’s computer
2. Customer enters card data and submits form, which sends data forward
3. Form containing card data is received and sent to payment system for authorization
REDIRECTION

• Method of passing users from merchant site to third-party service provider
• Very common form of processing for small merchants
• Traditionally used to minimize scope and remove liability—which may not be the case

Our first ecommerce payment method is the website redirection. In this process, customers are passed from the merchant website to a separate, third-party site to process the card transaction. This form of ecommerce processing is very common for small businesses. Traditionally, merchants have used the redirection to minimize scope and reduce liability; however, as we will soon see, this may not always be the case.
1. Merchant website sends redirect instructions to the customer computer
2. The customer computer requests a payment form
3. The Payment Service Provider (PSP) creates payment form and sends it back to customer computer
4. Customer computer displays payment form and sends card data to PSP
5. PSP receives the card data and sends it to payment system for authorization
REDIRECTION Attack Methods

- Man-in-the-middle attacks
- Hacker gains access to merchant site
- Changes redirection to malicious payment site
- Hacker captures card data
- May or may not put customer back into payment process to complete transaction

Very common, traditional ecommerce attacks. Hacker gains access to website and changes redirection code, sending customers to malicious website. After hacker has captured card data, the customer may or may not be sent to the legitimate payment site to complete the transaction. Often, this attack is discovered when merchants find discrepancies in sales records, which result from customer purchases that never make it to the PSP.
Before we look at the redirection summary, let’s take a moment to talk about risk. Risk is evaluated using the following equation:

Risk = Impact x Frequency

Hackers look for the biggest bang for their buck. Because redirections are typically used by small businesses, rarely do these attacks result in a large number of compromised payment cards. In other words, the impact related to typical redirection breaches is very low. For this reason, the PCI SSC has listed the redirection process as low potential risk, and merchant processing this way are eligible for SAQ A.

It’s important to note that merchants who use a redirection payment method are still liable for their customer’s payment card data. Should a hacker compromise the merchant website and redirect customers to a malicious site (one form of a man-in-the-middle attack), the merchant will most likely be held responsible and subject to the fees, fines, and penalties associated with payment card loss.
The IFRAME, or inline frame, is an ecommerce processing method where an HTML document (child page) is embedded into a separate HTML document (parent page). One of the advantages of IFRAMEs is that it allows the merchant site to maintain website consistency and branding while outsourcing the payment card data collection to a third-party.
1. Merchant website creates a parent payment page
2. The customer computer requests a child page, which contains the payment form
3. PSP creates and sends form to customer computer
4. Customer computer displays payment form and sends card data to PSP
5. PSP receives the card data and sends it to payment system for authorization
The above image illustrates how the IFRAME works. On the left, you see the parent page. This page is delivered from the merchant website. The middle image shows the child page. This child page contains the payment form and is delivered from the PSP. On the right, you can see how the pages are presented to the customer. From the customer perspective, it looks just like a single page on the merchant website.
The IFRAME attack is very similar to the redirection attack, in which the hacker gains access to the merchant site and changes the payment pathway. In this case, the hacker changes the redirection code so that the site requests a child page (and payment form) from a malicious website. Once the hacker captures the payment data, the customer may or may not be forwarded onto the legitimate payment site.
Again, like redirection, this is a much less frequent attack as criminals target higher-volume businesses. As such, this is a low risk processing method and requires completion of SAQ A.
The direct post, also known as ‘browser post’ or ‘silent order post’, is different than our first two ecommerce processing methods in that the payment form originates from the merchant website instead of the PSP. This allows the merchant more control over the payment process, but also relies on the merchant’s internal security controls to protect the transaction.
1. Merchant website creates the payment form
2. Customer computer displays payment form and sends card data to PSP
3. PSP receives the card data and sends it to payment system for authorization
DIRECT POST Attack Methods

• Hackers gain access to the website and alter the program that creates payment form
• Malicious code is entered to send payment card data to hacker as well as PSP
• Hacker collects data while legitimate purchases take place
• Very difficult attack to detect

Once again, the attack begins when the hacker gains access to the merchant site. From here, the hacker inserts code to not only send sensitive payment data to the PSP, but to the hacker as well, which allows the hacker to collect card data while legitimate transactions take place. Because there is no disruption of the payment pathway, these attacks can be very difficult to detect.
As used more frequently by larger merchants, this ecommerce payment method is considered to have moderate risk. To counter the additional risk, merchants that use a direct post must validate compliance to SAQ A-EP, which not only includes 139 questions, but also additional security controls like internal/external scanning and penetration testing.
With the JavaScript ecommerce payment method, the payment page originates from the merchant website. In this case, the customer computer is executing code, which comes from the PSP.
1. Merchant website creates the payment page
2. Payment page on customer computer requests JavaScript
3. PSP creates JavaScript and sends back
4. Customer computer uses JavaScript to create payment form within payment page, which customer completes and returns to PSP
5. PSP receives the card data and sends it to payment system for authorization
Just like the previously mentioned attacks, the JavaScript attack begins when a hacker gains access to the merchant website and alters code. Now, when the page requests the JavaScript from the PSP, it also requests malicious code from the hacker as well. This is a very difficult attack to detect, as neither the customer or merchant will notice additional script running in background of the form.

- Hacker gains access to merchant website and alters script
- Page requests JavaScript from not only PSP, but from malicious hacker page as well
- Customer will not notice additional script running in background of the form
- Hackers capture payment card data
- Very difficult attack to detect
Like the direct post, JavaScript is a moderate-risk ecommerce processing method, and as such, merchants processing in this manner are eligible for SAQ A-EP.
The API, also known as a ‘merchant gateway’, is unique from our other ecommerce processing methods in that the merchant controls nearly the entire payment process. By controlling the payment process, merchants have access to much more information to use for customer profiles, consumer trends, and marketing analysis.
1. Merchant website creates the payment page
2. Customer computer displays payment form, which customer completes and returns to merchant website
3. Merchant website sends card data to PSP
4. PSP receives the card data and sends it to payment system for authorization
The API attack begins when, you guessed it, criminals gain access to the merchant website. Hackers alter code to store card data on merchant systems during the transaction. Once the sensitive card data is saved on the merchant system, the hacker will retrieve the card data by periodically accessing the system through remote access. Some hackers have even set up email clients on the compromised system to batch themselves payment card data at the end of the day.
As we said earlier, hackers are always looking for the biggest bang for their buck. With ecommerce processing, this tends to be merchants that use an API. Because of the large impact and high frequency of these breaches, API presents a high-risk level for ecommerce businesses. These merchants are eligible for SAQ-D, which is validation to the entire PCI DSS standard. Internal/external scanning and penetration tests are just of the few additional security controls that are required of these merchants.
How Do You Protect Against Attacks?

• Comply with the PCI DSS
• File integrity monitoring
• Log monitoring
• Automatic log review
• Change management process

First things first, you need to comply with the PCI DSS. Keep in mind that PCI compliance is the minimum-required data security. To truly protect your business and customers, you may need to go above and beyond the standard.

As you can probably tell by now, security of the merchant website is critical to protecting ecommerce transactions. Security controls like file integrity monitoring, log monitoring, and automatic log reviews help you quickly identify when someone has manipulated your website. Implement a strong change management process so your staff has a clear process in place to maintain security once website updates have taken place.
PCI Validation Requirements

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>No of Visa Transactions Annually</th>
<th>Redirect</th>
<th>IFRAME</th>
<th>Direct Post</th>
<th>JavaScript</th>
<th>XML</th>
<th>Anything else</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Over 6 million</td>
<td>RoC^A</td>
<td>RoC^A</td>
<td>RoC^A-EP</td>
<td>RoC^A-EP</td>
<td>RoC</td>
<td>RoC</td>
</tr>
<tr>
<td>2</td>
<td>1–6 million</td>
<td>SAQ A</td>
<td>SAQ A</td>
<td>SAQ A-EP</td>
<td>SAQ A-EP</td>
<td>SAQ D</td>
<td>SAQ D</td>
</tr>
<tr>
<td>3</td>
<td>20,000–1 million</td>
<td>SAQ A</td>
<td>SAQ A</td>
<td>SAQ A-EP</td>
<td>SAQ A-EP</td>
<td>SAQ D</td>
<td>SAQ D</td>
</tr>
<tr>
<td>4</td>
<td>Under 20,000</td>
<td>SAQ A</td>
<td>SAQ A</td>
<td>SAQ A-EP</td>
<td>SAQ A-EP</td>
<td>SAQ D</td>
<td>SAQ D</td>
</tr>
</tbody>
</table>

RoC^A – Partial Report on Compliance validating the scope, eligibility and requirements listed in SAQ A

*chart taken from Processing e-commerce payments, VISA, 2014

This chart, taken from Visa’s Processing e-commerce payments, details validation requirements by merchant level.
Here are some of the key takeaways from this guide:

1. It should be painfully obvious by now that the merchant’s website security heavily influences the transaction risk. If the merchant website is breached, there is nothing the PSP can do to protect the data.
2. PCI DSS 3.0 makes it very clear that the merchant holds responsibility to protect ecommerce transactions that originate from their website.
3. Regardless of the ecommerce processing method, the same basic security controls can protect ecommerce payments.
Questions?

Need some help? Give us a call:

- **Acquirers & ISOs**
  - partners@securitymetrics.com
  - 801.995.6860

- **Merchants & Service Providers**
  - sales@securitymetrics.com
  - 801.705.5656

Still have questions or need help? Use the listed contact information to get the assistance you need today!
About SecurityMetrics

SecurityMetrics protects electronic commerce and payments leaders, global acquirers, and their retail customers from security breaches and data theft. The company is a leading provider and innovator in merchant data security, and as an Approved Scanning Vendor and Qualified Security Assessor, has helped over 1 million organizations manage PCI DSS compliance and/or secure their network infrastructure, data communication, and other information assets. Among other things, SecurityMetrics offers PCI level 4 compliance programs, PCI audits, mobile device vulnerability scanning, penetration testing, and forensic analysis. Founded in October 2000, SecurityMetrics is a privately held company headquartered in Orem, Utah, USA.