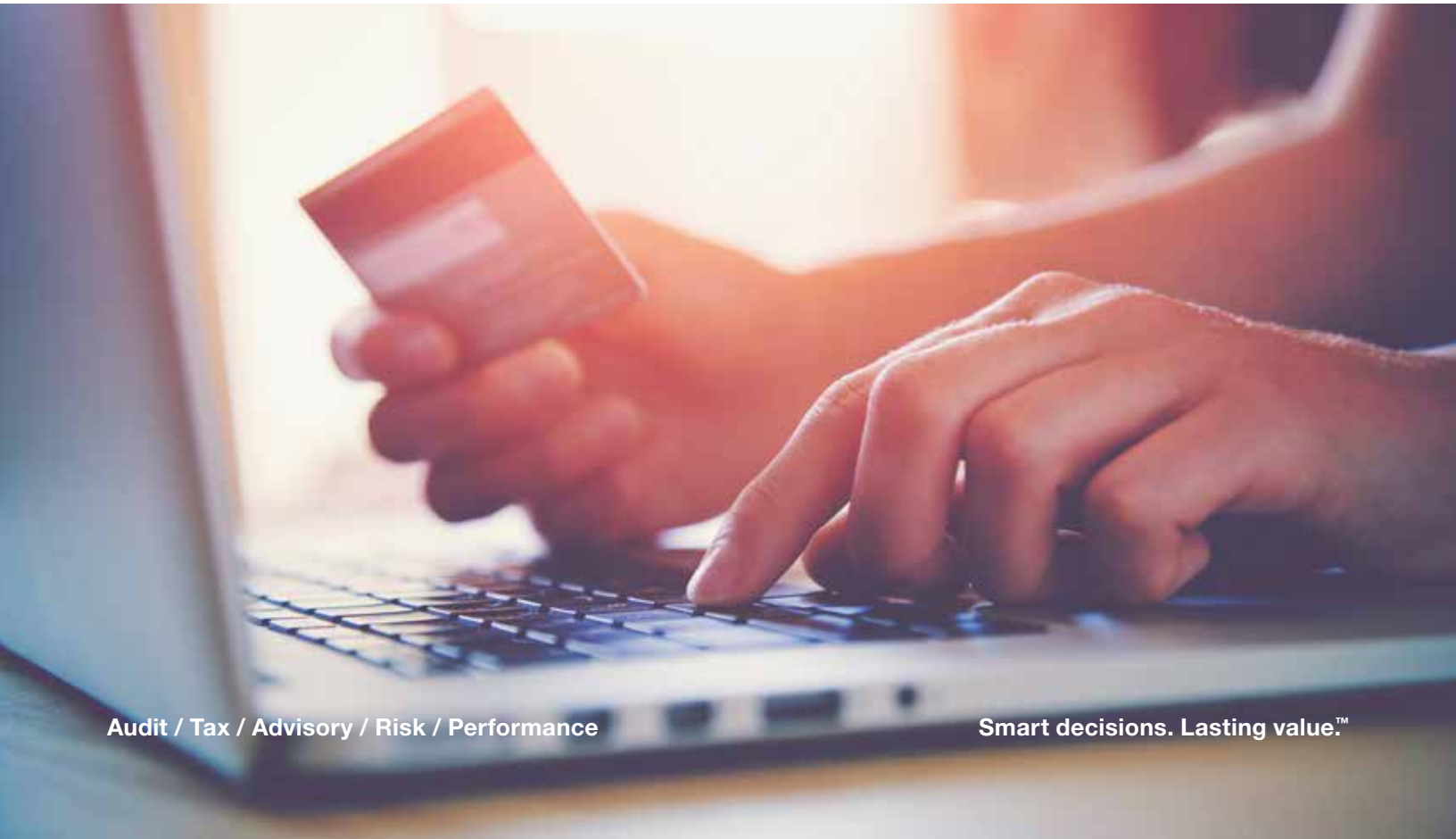
Crowe

February 2018

Maintaining PCI Compliance Through Innovation

An article by Angela K. Hipsher-Williams, CISA, QSA, and Jonathan J. Sharpe, CISA, QSA



The ascendance of online retailers and mobile ordering has created a hypercompetitive environment for purveyors of consumer products and services. Customers today expect a frictionless, “endless aisle” ordering experience, where any item they can think of is instantly orderable, if not instantly accessible.

Customers’ demand for instant gratification is not limited to the online environment. Traditional retailers and restaurants are thus being forced to innovate in a variety of ways to try to replicate the online customer experience. Particularly ripe for innovation is the process of ordering and paying for goods and services, but payment innovations come with a number of pitfalls when it comes to payment card industry (PCI) compliance.

PCI Compliance Stricter Than Ever

While new payment solutions offer flexibility and convenience for patrons, these innovations have security and compliance implications for merchants and customers alike. Recent large-scale payment card breaches have laid bare some of the risks, and in response, PCI compliance requirements have become stricter than ever.

Organizations must fully evaluate the implications of implementing new payment technologies, weighing convenience against cybersecurity risk. Devoting adequate resources to data security and protecting the confidentiality of customer payment card numbers are essential.

Changing the Scope of PCI Compliance Review

With a traditional point-of-sale (POS) transaction – in which a customer swipes or manually enters card information into a POS device or card reader – the card number goes through an organization's network as an unencrypted, 16-digit number. All locations and flows of cardholder data on an organization's network are considered "in scope" for PCI compliance review and must be reviewed against PCI requirements.

A number of emerging payment methods either expand or reduce the scope of PCI compliance. For retailers and restaurants, any time payment information is accepted in a new way, changes in scope must be assessed. Organizations implementing a new payment method should consider these questions:

- How do the benefits to customer experience weigh against the impact on security of the larger payment process, and do the benefits justify the risks?
- Does the organization have dedicated internal resources who understand the different payment methods and options for addressing security threats inherent in each?
- What is the data flow of card information over the internal network and how is it transmitted over the internet?
- Is the development of the application happening in-house or through an external vendor, and what are the PCI implications of each?
- What are the broader PCI implications of scope and applicable requirements of the new payment method?

Emerging Payment Methods

Point-to-Point Encryption Readers

Among the payment methods discussed in this article, the one with the clearest security and compliance benefits is point-to-point encryption (P2PE). P2PE relates to card-present transactions and can shrink the scope of PCI compliance review, reducing review time and overhead of the annual assessments.

With P2PE readers, payment card information is encrypted the moment it is received from the customer's swipe (of cards using a magnetic stripe) or dip (chip cards), meaning card numbers are immediately converted into an indecipherable code. The code is then sent to the payment processor, where it is decrypted and then sent on to the issuing bank. Merchants do not have access to the keys to encrypting and decrypting data, and because of that, the PCI council views the path it takes on an organization's network after encryption as out of scope.

By reducing the contact the retailer or restaurant has with card information, P2PE solutions reduce the number of systems that need to be reviewed for compliance, and also greatly reduce applicable PCI requirements from more than 300 subrequirements down to just 24. This can save organizations time and money on their overall compliance efforts while also improving customer data security.

Retailers using P2PE cannot be complacent, however, and must remain vigilant about PCI compliance. Many P2PE products and solutions are PCI compliant, but they can be implemented in a noncompliant fashion. For example, retailers can inadvertently bypass the benefits of the P2PE technology if they do not control the payment application they're using to make sure every transaction is entered properly (e.g., card information entered into the text field in the app instead of through the PIN pad will not be properly encrypted).

To Reduce Risk:

Retailers should follow vendor P2PE implementation guidelines explicitly to make sure they can reap the benefits of the product. Additionally, retailers and restaurants should ensure their business processes include cardholder data only being entered into the card reader itself for P2PE solutions.

Mobile Point of Sale

Mobile POS technology unshackles the point of sale from the old-school, fixed register at the front of the store. For larger merchants, this allows sales associates to sell products or research inventory from anywhere in the store. Merchants also can use mobile POS devices to collect payments from customers – a common application for smaller merchants.

Any hardware used for a mobile POS transaction must meet PCI compliance requirements. Merchants need to consider a range of security issues, from how the device is connecting to the internet, to who has access to the device and the information it holds, to inventory management of the physical device itself.

If the device is connected to a wireless signal in the store, someone who compromises the network potentially could capture the POS traffic. In addition, stores should consider access restrictions – or the lack thereof – in place for associates. Associates with unneeded access levels to the payment application or operating system may have the ability to capture card data from the store's mobile device and exfiltrate it via email or USB drive.

To Reduce Risk:

Merchants need to consider whether anyone in the store conceivably could compromise the mobile POS technology, as well as what capability malicious actors would have to make unauthorized use of card data. Merchants should then make sure that access rights are restricted appropriately across the organization at both the application and operating system level.

Pay-Ahead and Mobile Ordering

With pay-ahead and mobile ordering, customers can order something before they go to a store or restaurant and pick it up without having to wait while the order is fulfilled and processed.

As these advance transactions all are done on the internet, merchants and restaurants need to understand the technology and, in particular, the sequencing of customer data ownership – namely, understanding who has responsibility for customers' sensitive personal information, which can help organizations evaluate where the security implications lie.

An additional pitfall for merchants with pay-ahead and mobile ordering is the false assumption that any outside vendors managing a part of the process have security covered. The following section addresses risks associated with third-party vendors.

To Reduce Risk:

Merchants need to be sure they understand if and at which points they are storing or transmitting card information in their own environment as opposed to in that of an outside vendor.

Outsourced E-Commerce for Payments

In the case of outsourced e-commerce, merchants or restaurants hire an outside vendor to manage their e-commerce transactions. Too often, from a security and PCI compliance perspective, an IT department thinks that if e-commerce has been outsourced, there is no risk to its own organization. For example, a common arrangement is for a merchant to host the marketing side of its website but redirect customers to a third-party vendor for actual purchases. In this case, the customer is entering payment card information through the third-party vendor's site, and the merchant may thus falsely presume the security and PCI compliance responsibilities of that card number are not its responsibility.

There have been attacks, however, in which hijackers have redirected customers from the shopping cart on the merchant's site to a look-alike site where customers were directed to enter their payment card information. Not understanding how an outsourced e-commerce data flow works can have major security implications, and merchants often are held accountable for such instances of fraud or noncompliance by acquirers/processors and customers.

<u>To Reduce Risk:</u>

Merchants must thoroughly vet outside vendors that are managing parts of the payment process. They also should maintain internal staff who thoroughly understand the technology and where security and PCI compliance accountability lies throughout the payment process data flow. This commonly is overlooked when an organization's website redirects from its page to a third-party vendor payment page at the time of checkout. In these scenarios, the merchant still is responsible for security and applicable PCI compliance; it must ensure it is validating the PCI compliance of the third-party vendor being used to facilitate the payment process on its behalf.

Subscription Services (Recurring Payments)

Subscription services involve periodic payments from customers without customer interaction – meaning card information needs to be stored and accessed on a recurring basis. In most cases, monthly subscription services require access to the card number in order to make that recurring charge.

Storing card numbers poses security risks, because if hackers breach the network and access the servers where that information is stored, they could seize the payment card information.

To Reduce Risk:

Subscription services involve the retention of large amounts of sensitive data, which needs to be accounted for and protected. Merchants storing the actual payment card information for recurring use should consider using token providers, which assign a "token," or a number that is a reference to a card number, for the transmission of payment information through the merchant and bank systems.

Near-Field Communication Payments

Near-field communication (NFC) payments are a form of contactless payments that enable two devices to communicate wirelessly with each other when they are in close proximity. Consumers make NFC payments most often by using a mobile device on which they have saved payment card information.

Typically using tokenization and virtual card numbers as security measures to limit access to payment card information, NFC payment systems offer security to consumers that exceeds security available when using a card alone. However, retailers accepting NFC payment methods still may have more access to information than they realize. In turn, retailers and restaurants face the same PCI compliance implications for any payment card data that is transmitted through their network as part of the payment process.

To Reduce Risk:

Retailers should take steps to make sure their systems are configured properly for NFC payments. Moreover, retailers need to be sure they understand the data flows for NFC payments, as this form of payment may become more prevalent down the road.

Be Informed About Data Locations and Flows to Maintain Compliance

From equipping store associates with mobile devices to enable them to check inventory for customers on the spot, to offering payment methods that mimic the seamlessness of online ordering, retailers and restaurants today are particularly focused on speeding up the process of ordering and paying for goods and services.

Merchants must be aware of the PCI compliance requirements resulting from any change in the payment methods they offer, and they should remain vigilant about the locations and flows of information throughout their payment systems.

Learn More

Angie Hipsher-Williams
Principal
+1 317 208 2430
angie.hipsher@crowe.com

Jonathan Sharpe
+1 317 208 2433
jonathan.sharpe@crowe.com

crowe.com

Text created in and current as of February 2018; Cover and artwork updated in May 2018.

DI-18200-032A