The Cost of Compliance

The Payment Card Industry Data Security Standard (PCI DSS) aims to protect sensitive cardholder data throughout the life cycle of ecommerce transactions. The standard puts heavy scrutiny on merchants, Acquirers and Independent Sales Organizations (ISOs) managing and operating merchant portfolios to ensure that credit card processing is safe and secure and generally requires significant internal policy development, training, monitoring and risk response. PCI compliance is mandated and can be costly both in time and resources and merchants that are compliant can still be at risk of a data breach.

This has become painfully obvious to merchants in the wake of mega retail breaches like Target, Neiman Marcus and Home Depot and it raises an important question: How can I provide safe, secure and compliant payment processing without breaking the bank? This white paper outlines steps that merchants can take to get out ahead of stringent PCI scrutiny while reducing PCI scope, cost and effort and boost consumer confidence and profits.

How can I provide safe, secure and compliant payment processing without breaking the bank?

Safe and Secure Payment Processing

Compliant payment processing protects merchants from costly breaches but also boosts customer confidence and minimizes reputational damage. But merchants that are compliant are still at risk of data breach. That is why maintaining additional layers of security across the entire payment life cycle is essential. While PCI compliance is mandated, security-optimized transaction processing is not. CNP merchants should be prudent in insulating their payment processing operation beyond the requirements of PCI with adequate **data protection, tokenization and end-to-end encryption**. Secure transaction processing requires vendor-specific payment protocols that reach from the point of origin, through the network, to the originating point upon reception of authorization.

Protecting Data: an Overview

PCI compliance is only one step in protecting data. CNP merchants should be sure that they and their chosen payment processor are PCI certified, and take additional steps to guard against data and security problems.

The best way to understand your real gateway requirements is through reporting and analytics. When selecting a payment gateway and considering the various payment processing types, make sure to demand robust reporting and data analytics features. Reporting provides line-of-sight into recent changes to business priorities and helps you develop custom strategies to address the shifting economics of the business or to prepare for upcoming events. There are a number of reporting metrics and analytical functions you should consider when choosing a gateway:

- **Encryption** CNP merchants should encrypt data being sent across public networks, including phone lines, FTP and email.
- **Merchant partner data protection** Merchants are responsible (and liable) for cardholder data accessed by business partners and should ensure that any marketing affiliates, fulfillment[1] houses or other vendors are adequately protecting cardholder data.
- **Limited access to cardholder data** Business processes and operations will sometimes require that other departments have access to cardholder data; CNP merchants should restrict access to sensitive data to only those departments that need it and should enlist the help of their payment processor to set up role-based data access.
- **Secure data storage** Online merchants should never store customer card data on their servers or on a system outside of the firewall. Additionally, information stored internally should be encrypted or not stored at all and tokenized.
- **Transaction routing analytics** When using multiple processors, analytics provides the visibility and monitoring necessary to avoid traffic problems and proactively uncover network vulnerabilities that can often be hidden under layers of routing redundancy.

Spotlight: Tokenization

An effective part of end-to-end secure processing is tokenization. Tokenization replaces sensitive user data with a reversible benign substitute.[2] As an augmentation to PCI compliance, tokenization simplifies validation by reducing the number of components for which PCI requirements apply, though this solution does not eliminate the need to maintain PCI compliance.[3] There are different implementations of tokenization, from de-tokenization methods to deployment models and technologies. The importance lies in protecting the process and maintaining strong security controls to ensure the effectiveness of the tokenization process and continued compliance.

The main benefit to tokenization is the protection offered to consumers, as their information is guarded from being released to hackers. Additionally, tokenization offers merchants coverage against potential damages not only to their business, but also to their reputation. As evidenced by the recent major retail breach, when retailers fail to protect themselves, they become liable to each and every person whose information has been compromised.

Tokenization does have some drawbacks. It is an all or nothing approach to security, and cannot be implemented in pieces, unlike other solutions. With tokenization, several other aspects of security have to be in place to guarantee a safe environment for data. It is not a magic wand ensuring security; it works in conjunction with a comprehensive security policy.

E2E ENCRYPTION

End-to-end (E2E) encryption works hand-in-hand with tokenization to ensure complete security of cardholder data, from point-of-sale throughout the entire transaction lifecycle.[4] By encrypting the data at the point of capture and maintaining encryption throughout, the card number is never stored unencrypted by the merchant.

Typically, merchants store customer cardholder data before it moves into the payment process, putting it at risk if a breach were to occur. With E2E encryption, the card number is separated from sales information and replaced with a token, and the transaction is processed independent from the merchant via controls in the front-end and back-end processes. This protects sensitive information from would-be thieves, who cannot commit fraud with the meaningless token information.

Why PCI DSS is Important to Merchants

The PCI DSS is "a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information."[5] This standard was created by VISA® to provide merchants with consistent data security protocol.

PCI DSS compliance can have great benefits for merchants, including increased customer confidence that the merchant is adequately protecting sensitive card information. The PCI DSS is comprised of twelve security requirements – each consisting of numerous tasks and steps to complete – to protect cardholder data.The table below outlines the goals of the PCI DSS as well as the requirements to fulfill those goals; however this is just a tip of the iceberg. Many of these requirements are broken into sub-requirements and there are additional tenants that merchants may adhere to, depending on their classification.

Understanding the Cost of Compliance

GOALS	PCI DSS REQUIREMENTS
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to cardholder data
	11. Regularly test security
Maintain an information security policy	12. Maintain a policy that addresses information security

Compliance is not a one-time occurrence: it is ongoing. For that reason, there are four levels of compliance and associated costs for CNP merchants to consider.[6] The cost of compliance includes the infrastructure and technology costs associated with closing the gaps identified in the merchant's current business model. Annual costs refer to the costs to maintain PCI compliance from year to year.

There are various levels of PCI, and merchants need to determine which level they fall under and the subsequent audits required to be compliant. There may also be some fluctuation in requirements as some lower levels with a higher number of transactions may require additional checks and audits to be compliant. These audits cost money and each level experiences a different financial burden, but merchants should take into consideration the time, resources and staffing costs associated with each level's requirements as well. The table below outlines each level, the criteria associated with each level, the compliance requirements and annual cost.

The Shift From Plastic to Digital and Implications to Security

LEVEL	MERCHANT CRITERIA	COMPLIANCE REQUIREMENT	ANNUAL COST
Level 1	**VISA®, MasterCard & Discover** Any merchant that processes greater than 6 million credit card transactions per year via any acceptance channel.[7] **American Express** 2.5 million or more American Express Card transactions per year.[8]	Annual PCI data security assessment conducted onsite by a third party vendor in addition to quarterly network scans.[9]	**Initial scope** - $250,000 **Becoming compliant** - $550,000 - $1,000,000 Annual PCI cost - $250,000
Level 2	**VISA®, MasterCard & Discover** Any merchant processes 1 to 6 million transactions regardless of channel.[10] **American Express** 50,000 to 2.5 million American Express Card transactions per year.[11]	Self-assessment conducted annually by a third party vendor in addition to quarterly network scans.[12]	**Initial scope** - $125,000 **Becoming compliant** - $260,000 - $500,000 Annual PCI Cost - $100,000
Level 3	**VISA®, MasterCard & Discover** Any merchant who processes 20,000 to 1 million online transactions per year, regardless of channel.[13] **American Express** Less than 50,000 American Express Card transactions per year.[14]	Annual PCI data security assessment conducted onsite by a third party vendor in addition to quarterly network scans.[15]	**Initial scope** - $50,000 **Becoming compliant** - $75,000 - $90,000 Annual PCI cost - $35,000
Level 4	**VISA, MasterCard & Discover** Less than 20,000 e-commerce transactions or 1 million total transactions via any channel.[16]	Self-assessment conducted annually by a third party vendor in addition to annual network scans[17]	**Initial scope** - $50,000 **Becoming compliant** - $75,000 - $90,000 Annual PCI cost - $35,000

The landscape of payments is quickly evolving and new payment options and technologies are emerging rapidly. In light of the noteworthy breaches, security is top of mind for consumers who are increasingly making payments online and via mobile. These events have resulted in obstacles for emerging payment technologies looking to get consumer buy-in. In a recent Thrive Analytics study, consumers ranked security concerns as the top barrier to using a digital wallet.[18] But they also present opportunities; many of the breaches occurring are taking place at the store level, so a window has opened for emerging payments to step in and demonstrate that they offer superior security, giving skittish consumers peace of mind. Recently, companies have recognized this opportunity and are capitalizing on security concerns to increase adoption.[19]

A recent Thrive Analytics study, consumers ranked security concerns as the top barrier to using a digital wallet.[18]

VISA CHECKOUT

Visa is one of those companies. Seeing the market opportunity, Visa recently released Visa Checkout, a checkout solution that eliminates the need for entering in a 16-digit card number during the checkout process. Instead, the user enters one username and password combination, simplifying the process and offering a streamlined – and secure – payment process.[20] Recently, Visa announced it is partnering with several top acquirers and e-commerce platforms and has increased its reach by another 4 million online merchants.[21]

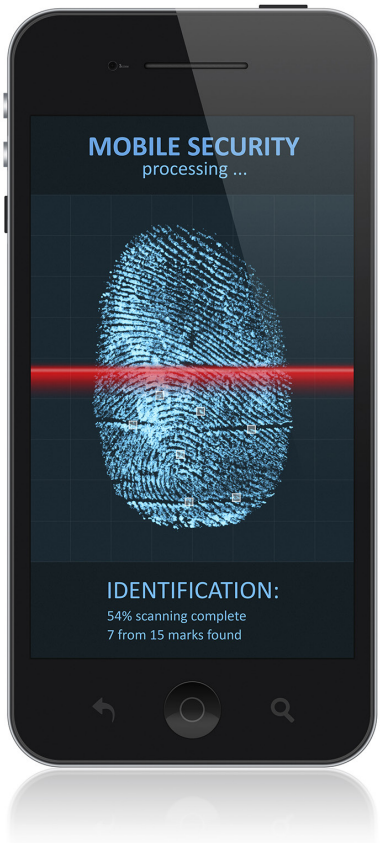
In addition to allowing consumers to complete payment with just a few clicks, it offers a number of security features that make it an attractive payment choice for security-minded shoppers.

Visa Checkout uses advanced tools to ensure the safety of sensitive data, including device fingerprinting and Visa Dynamic Network Analytics scoring, both of which authenticate customers before they make a purchase.[22] Additionally, its tokenization service supports token creation for all payment cards, not just Visa-branded ones.[23] Tokens are created and stored across any number of devices, including mobile, cloud-based mobile apps and e-commerce applications; and their use can be limited to specific devices, merchants or purchase types.[24]

MASTERCARD® CONTACTLESS

MasterCard also offers an alternative payment option to consumers. Its contactless payment platform enables shoppers to “Tap&go™” – or tap their device or contactless card on a contactless enabled reader when checking out. This provides convenience by streamlining the payment process and the device or card never leaves the customer’s hands. Also, the customer doesn’t sign for purchases under $50.[25]

MasterCard is also partnering with Apple on their newest payment technology, Apple Pay, allowing users to pay with a single touch via their iPhone and using their MasterCard information. The solution also has a mobile application – MasterCard Nearby™ – that directs users to the nearest location where they can use their mobile device to pay.[26]



By combining TouchID on the phone with tokenization, a strong bond is created between the payment and the mobile device, significantly raising the security of the transaction.[28]

APPLE PAY

Apple has also put skin in the emerging payments game with the recent launch of Apple Pay, a technology that combines tokenization with user identification via various features on the iPhone to allow consumers to make secure payments. This type of security combination is extremely innovative and has never been done before.[27] By combining TouchID on the phone with tokenization, a strong bond is created between the payment and the mobile device, significantly raising the security of the transaction.[28] The level of this security is reflected in the lower card-present rates that have been extended to Apple.[29] The consistency of the security is unmatched – Apple controls both the hardware and software aspects – which affords it the ability to support verification aspects like biometrics and geolocation.[30] Apples innovation allows consumers to pay securely without sacrificing convenience – consumers simply hold their phone to a contactless reader while placing a finger on TouchID.[31]

Apple Pay assigns a unique Device Account Number so users don't have to use their actual credit card. This Device Account Number is encrypted and stored securely in a dedicated chip within the iPhone called a Secure Element. When a purchase is made, a transaction-specific dynamic security code is issued and used along with the Device Account Number to process the payment, meaning the actual payment card number is never stored on Apple servers, shared with the merchant or transmitted with payment.[32]

These benefits position Apple to succeed both with consumers and merchants, who are looking to get back into good graces with distrusting shoppers. Additionally, the liability provision of EMV will encourage merchant adoption of the updated POS systems, which are NFC enabled to accept payments from iPhones and Apple Watches.[33] Apple never saves transaction information, so consumers payments are always private and can't be traced back to you.[34] Finally, a lost or stolen device can be protected by putting the device in Lost Mode, blocking access to the contents of your phone or completely deleting them if the users wishes.[35]

WHAT ARE THE IMPACTS OF THESE EMERGING PAYMENT TECHNOLOGIES ON LIABILITY?

EMV is rolling out in the U.S. and there will be a subsequent liability shift for merchants who do not comply with the new standard. Issuers and merchants using non-EMV compliant devices that opt to process payments made with EMV-compliant cards will assume liability for all resulting fraudulent transactions. *The target date for this shift is October 2015 and is described succinctly by MasterCard: The party, either the issuer or merchant, who does not support EMV, assumes liability for counterfeit card transactions.*[36]

This financial liability provides a strong incentive for merchants to adopt the new POS devices for EMV, which will have the NFC system enabled and allow customers to pay with their iPhone or Apple Watch.[37]

The Bottom Line

The bottom line is that non-compliance is much more expensive than compliance. Fines for non-compliance can range from $5,000 to $100,000 per month at the discretion of the payment brand. This cost is typically passed through the bank and eventually rests on the merchant. Another risk is termination of relationships with your merchant bank in addition to raised transaction fees.[38]

Fines for non-compliance can range from $5,000 to $100,000 per month at the discretion of the payment brand.

If a data security breach takes place, a fine of $50-$90 per cardholder compromised can be imposed, along with an increased risk of civil suit brought by customers.[39] Credit card account providers can also penalize merchants by suspending acceptance. Aside from the dollar amount, brand and reputational damage risk can be costly as well.

Simplifying PCI Compliance Involvement – Choosing Your Gateway

From building and maintaining a secure, cost-effective payment process to better understanding PCI compliance, your gateway provider should be your partner. When selecting a payment gateway, merchants should choose a provider that is flexible and able to adapt as your business evolves. Whatever the size of your business, work with your provider to achieve the right balance of rates and fees.

The total cost of acceptance will vary from merchant to merchant and is dependent on a number of considerations. CNP merchants must weigh cost, benefits and limitations of payment processing options. By following industry standards and best practices along every step of the payment process, businesses have the opportunity to decrease many of these costs and even increase revenue. Payments-related expenses are a cost of doing business, but – when managed properly – can be a driver of increased efficiency, growth and long-term stability and savings.

ABOUT VERIFI'S GLOBAL PAYMENT GATEWAY PLATFORM

Reduce PCI scope using Verifi's Secure Payment Fields and Data Tokenization services

Verifi's PCI Level 1 certified payment gateway is processor agnostic and features flexible user management and controls, multi-currency support for international processing, and customizable reporting. The Gateway provides secure real-time and batch, credit card, ACH and eCheck payment processing for card-not-present (CNP) merchants. It also enables connectivity to all of the major domestic and international acquirer processing networks, enabling global payment acceptance across all major international and domestic payment types and currencies. Our platform enables merchants to:

- Increase data and transaction security
- Simplify your PCI compliance involvement
- Streamline payment integration to banks
- View and analyze transaction activity with rules based filters
- Protect payments and boost profits along the entire transaction lifecycle
    - o One integration that provides access to multiple fraud management tools that can be tested and toggled without additional cost or IT pain
    - o Prevent chargeback problems and added costs with the award-winning Cardholder Dispute Network® (CDRN) to resolve disputes quickly before they become a chargeback
    - o Recover lost billings by up to 20% and retain at-risk customers with guaranteed ROI through Decline Salvage
    - o Save time and recover profits lost to chargebacks by 50% or more

The Payment Gateway's dynamic transaction routing allows you to simplify the management of multiple business lines and merchants accounts through a single, easy to use platform. Through a single integration, merchants have access to a wide variety of fraud prevention and management solutions that can be customized and tested to your desired thresholds. Verifi understands the wide scope and associated costs of PCI compliance, so we streamline transaction processing and reduce PCI exposure associated with storing and transmitting raw payment data via tokenization. This combination of security features and a comprehensive suite of fraud prevention and management solutions offers unmatched protection for each merchant's custom needs and it is all possible through one, simple integration.

ABOUT VERIFI

Since 2005, Verifi has helped merchants protect their payments and boost profits. Offering a wide-range of flexible, configurable fraud prevention and chargeback management tools, Verifi makes it easy to prevent and fight payment disputes, protect the entire transaction lifecycle and increase revenue. Verifi is PCI Level 1 certified and headquartered in Los Angeles, California.

For more information about Verifi, please visit the Verifi website at www.verifi.com.

For More Information

Main Phone: (323) 655-5789 Mon-Fri 8:00 AM – 5:00 PM PST

Main Fax: (323) 655-5537

Email Address: info@verifi.com

Mailing Address: 8391 Beverly Blvd., Box #310, Los Angeles, CA 90048

Citations

1 Chabrow, Eric; “Cyber-Insurance: Not One-Size-Fits-All”. http://www.bankinfosecurity.com. January 10 2013; http://www.bankinfosecurity.com/cyber-insurance-one-size-fits-all-a-5395/op-1.

2 No Author Listed. “Tokenization”. wikipedia.org; No Date Listed; https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.

3 No Author Listed. “Tokenization”. wikipedia.org; No Date Listed; https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.

4 PX; “E2E Encryption + Tokenization Technology”. epx.com; No Date Listed; http://epx.com/epx-e2e-tokenization-technology/

5 No Author Listed; “PCI Security Standards For Merchants; pcisecuritystandards.org; No Date Listed; https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.

6 EPX; “E2E Encryption + Tokenization Technology”. epx.com; No Date Listed; http://epx.com/epx-e2e-tokenization-technology/

7 PCI Compliance Guide; “PCI FAQS”. pcicompliance.org; No Date Listed; http://www.pcicomplianceguide.org/pcifaqs.php#5

8 American Express; “The Data Security Operating Policy”. americanexpress.com; No Date Listed; https://www209.americanexpress.com/merchant/services/en_US/data-security

9 No Author Listed; “PCI Compliance: Basics for Credit Card Security”; braintreepayments.com; No Date Listed; https://www.braintreepayments.com/blog/pci-compliance-basics-for-credit-card-security

10 PCI Compliance Guide; “PCI FAQS”. pcicompliance.org; No Date Listed; http://www.pcicomplianceguide.org/pcifaqs.php#5

11 American Express; “The Data Security Operating Policy”. americanexpress.com; No Date Listed; https://www209.americanexpress.com/merchant/services/en_US/data-security

12 No Author Listed; “PCI Compliance: Basics for Credit Card Security”; braintreepayments.com; No Date Listed; https://www.braintreepayments.com/blog/pci-compliance-basics-for-credit-card-security

13 PCI Compliance Guide; “PCI FAQS”. pcicompliance.org; No Date Listed; http://www.pcicomplianceguide.org/pcifaqs.php#5

14 American Express; “The Data Security Operating Policy”. americanexpress.com; No Date Listed; https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US_11.pdf

15 No Author Listed; “PCI Compliance: Basics for Credit Card Security”; braintreepayments.com; No Date Listed; https://www.braintreepayments.com/blog/pci-compliance-basics-for-credit-card-security

16 PCI Compliance Guide; “PCI FAQS”. pcicompliance.org; No Date Listed; http://www.pcicomplianceguide.org/pcifaqs.php#5

17 No Author Listed; “PCI Compliance: Basics for Credit Card Security”; braintreepayments.com; No Date Listed; https://www.braintreepayments.com/blog/pci-compliance-basics-for-credit-card-security

18 http://www.digitaltransactions.net/news/story/Tokenization-Plays-the-Central-Role-in-Visa_s-New-Cloud-Payment-Suite

19 http://www.digitaltransactions.net/news/story/Tokenization-Plays-the-Central-Role-in-Visa_s-New-Cloud-Payment-Suite

20 https://checkout.visa.com/business/index.jsp

21 http://techcrunch.com/2014/08/28/newly-launched-paypal-alternative-visa-checkout-adds-nearly-a-dozen-more-partners/

22 https://checkout.visa.com/business/index.jsp

23 http://www.digitaltransactions.net/news/story/Tokenization-Plays-the-Central-Role-in-Visa_s-New-Cloud-Payment-Suite

24 http://www.digitaltransactions.net/news/story/Tokenization-Plays-the-Central-Role-in-Visa_s-New-Cloud-Payment-Suite

25 http://www.mastercard.com/us/company/en/whatwedo/paypass.html

26 http://www.mastercard.us/mobilepayments/

27 http://www.zdnet.com/apple-pay-and-security-could-tokenization-be-the-tool-that-curbs-data-breaches-7000033585/

28 http://www.zdnet.com/apple-pay-and-security-could-tokenization-be-the-tool-that-curbs-data-breaches-7000033585/

29 http://www.zdnet.com/apple-pay-and-security-could-tokenization-be-the-tool-that-curbs-data-breaches-7000033585/

30 http://www.zdnet.com/apple-pay-and-security-could-tokenization-be-the-tool-that-curbs-data-breaches-7000033585/

31 https://www.apple.com/iphone-6/apple-pay/

32 https://www.apple.com/iphone-6/apple-pay/

33 http://www.macobserver.com/tmo/article/5-reasons-apple-pay-will-succeed-brilliantly

34 https://checkout.visa.com/business/index.jsp

35 https://checkout.visa.com/business/index.jsp

36 http://www.macobserver.com/tmo/article/5-reasons-apple-pay-will-succeed-brilliantly

37 http://www.macobserver.com/tmo/article/5-reasons-apple-pay-will-succeed-brilliantly

38 No Author Listed; “PCI FAQs”; pcicomplianceguide.org; No Date Listed; http://www.pcicomplianceguide.org/pcifaqs.php#11

39 No Author Listed; “PCI Noncompliant Consequences”; focusonpci.com; No Date Listed;
http://www.focusonpci.com/site/index.php/PCI-101/pci-noncompliant-consequences.html