SECURE payments

9 Questions Every MSP Needs to Ask (and Answer) About their Customers' PCI Compliance

All MSPs provide cybersecurity for their customers and most customers assume this includes payment security. The reality is, payment security is often overlooked because MSPs have lacked the visibility and tools to identify and resolve the risks associated with PCI compliance.

Your customers need help! 70% of businesses fail to maintain PCI compliance after 12 months and are penalized with costly fees. And that's just the beginning. With the rapid acceleration of cybercrime, it's only a matter of time before your customers suffer a breach—and you suffer the blame.

Who is addressing payment security for your customers? To mitigate risk to you and your customers, the following criteria should be assessed in each of your customers' payment environments:

01

Has a proper point-to-point encryption solution been implemented to increase security of customer data?

Why is point to point encryption important?

Customers want to know their information is protected however they choose to pay. Point-to-Point Encryption (P2PE) is an in-store protection solution that converts customer card data into meaningless code, making it unusable in the event of a cyberattack and removing the incentive for cyber-crime. Point to point encryption encrypts payment card data from the point of capture, such as when the card is read by a card payment terminal, until it reaches the secure decryption endpoint.

02

Has EMV technology been implemented to accept payments?

Why is EMV chip acceptance important?

EMV, short for Europay, MasterCard, and Visa, is a set of standards governing card authentication technology that utilizes a chip embedded in a credit card rather than a magnetic strip. Credit cards that follow the EMV standard include a chip containing the card's information, in addition to the standard magnetic stripe. EMV card readers require the card to be inserted into a terminal, providing authentication that the card is valid. For retailers, it is incredibly important to understand the requirements that need to be met to ensure that you are not liable for fraud.

03

Does the payment process include tokenization?

Why is tokenization important?

Tokenization protects sensitive data by replacing it with an algorithmically generated number called a token. This token can be securely passed through the internet without exposing real credit card data. Tokenization can work in multiple ways and can drastically reduce the financial impact of a data breach. Tokenization makes achieving and maintaining PCI compliance significantly easier.

04

Does your customer use a payment software integration to the payment processor to strengthen security?

Why is payment software integration important?

A payment integration is a connection between a website or application and a payment processor or payment gateway. This allows credit card payments to be accepted directly from the application or website. An integrated payment solution offers a seamless checkout experience and reduces human error by automating the payment process when compared to manually imputing transaction details.

05

Has a PCI-compliant secure payment gateway been implemented?

Why is a secure payment gateway important?

A payment gateway is a technology that securely captures and encrypts sensitive credit card details from a customer and transmits that data to a payment processor to complete a transaction. If you have a gateway that is PCI compliant and employs payment tokenization safeguards, your business and your customers will be protected. Your gateway should have the highest level of PCI compliance, a tier-1 level. The highest level tells you that your provider goes through annual third-party audits and vigorous precautions to ensure payment security.

06

Has the PCI SAQ been completed on an annual basis to validate the security of cardholder data?

Why is annual PCI SAQ important?

The growing popularity of card-based and online transactions has made it extremely convenient for consumers to conduct transactions. With the growth of cashless transactions, there has been a corresponding increase in fraud, identity theft and other cyber-crimes. To reduce these instances, the PCI Security Standards Council has made it mandatory that every merchant or service provider who stores, processes and/or transmits cardholder data (credit, debit, or prepaid card) needs to be PCI Data Security Standard (DSS) compliant. The annual Self-Assessment Questionnaire (SAQ) is designed as a validation tool used to assess security of cardholder data for merchants.

07

Has the customer satisfied all requirements and is PCI DSS compliant?

Why is PCI DSS compliance important?

PCI DSS is an information security standard that was created to increase controls around cardholder data to reduce credit card fraud. It is important to protect the data of your business, employees and customers. The purpose of PCI DSS is to aid in protecting card data from hackers and thieves. PCI DSS standards help keep your data secure and can prevent costly data breaches which can range from tens to hundreds of thousands of dollars, which could potentially result in the business shutting down for good.

08

Is your customer on the most price advantageous pricing model to save money on processing fees?

Why are credit card fees important?

Credit card processing fees are the fees a merchant pays for credit or debit card sales determined by the card issuer, the card network, and the payment processor. To get the best possible pricing for your credit card processing service, you need to understand the different pricing models that processors use and how they work. Credit card processing companies charge various fees, some you should never have to pay. As a business, having a fundamental knowledge of how credit card processing fees are designed will help you choose a processor with the best rate and lowest fees.

09

Does your customer charge an extra fee to recoup fees to increase margins?

Why is credit card fee recoupment important?

The primary benefit of credit card fee recoupment is the burden of credit card fees is passed on to the purchaser, eliminating the cost to the business while still allowing your customers their choice of payment method. While credit card fee recoupment is becoming more acceptable, it is important to consider your customer. The initial cost savings could end up costing you significantly more overall if your customers do not accept it.

It's not possible for an MSP to be an expert in every area of security. With constant and rapidly accelerating cybercrime that's targeting payment information, your customers are more at risk than ever before. Now, you can easily assess your customers' payment environments and mitigate risk with Secure Payments.

Secure Payments is the channel's only MSP-facing solution for PCI compliance and payment security. With a simple assessment to identify risk and an actionable plan to attain compliance within 60 days, the Secure Payments team provides your MSP with clear visibility and status to all your clients' PCI compliance from a centralized portal with ongoing monitoring. Best of all, you can feel confident your customers are protected with a team of payment experts doing the work on your behalf all while you earn passive revenue.

BROOKFIELD TECHNOLOGY CENTER 203.775.5009 sales@btcamerica.com