PCI FAQS AND MYTHS

Presented by BluePay

BluePay

THE IMPORTANCE OF PCI COMPLIANCE

When your business — no matter its size — began accepting credit card payments, it immediately became a potential target for data thieves.

Much more is at risk than your customers' sensitive information, however. If you aren't employing the best industry practices to protect that data, your business could face fines, lose the ability to accept credit and debit card payments, and jeopardize its credibility.

To help protect consumers' credit card information from data thieves, the Payment Card Industry Security Standards Council created data security standards that businesses must follow to be in compliance.

The cost of noncompliance can be staggering. The bank that processes your payments could be fined $5,000 to $100,000 per month by the credit card companies — amounts likely to be passed along to you — until the business is following the requirements. Your bank also could raise the fees it charges to process your business's transactions, or stop handling them altogether. (Check your account agreement with the bank.) Your business also might have to cover the cost if the bank has to issue new cards to customers whose data has been compromised — and who could become former customers if there has been a data breach. Finally, your business also may be liable for losses due to fraud and other financial losses.

BluePay

TABLE OF CONTENTS

BluePay

FAQ 1:

WHAT ARE THE PCI COMPLIANCE LEVELS AND HOW ARE THEY DETERMINED?

There are four levels of PCI compliance as determined by Visa and MasterCard. These levels are based on the transaction volume (including credit, debit and prepaid) over a 12-month period. Merchants that have been affected by a security breach that resulted in compromised card data may be escalated to the next level.

Merchant Level Description

- Any merchant processing more than $6 million Visa and/or MasterCard transactions per year.
- Any merchant processing $1 million to $6 million Visa and/or MasterCard transactions per year.
- Any merchant processing $20,000 to $1 million Visa and/or MasterCard e-commerce transactions per year.
- Any merchant processing less than $20,000 Visa and/or MasterCard e-commerce transactions per year, and all other merchants processing up to $1 million Visa and/or MasterCard transactions per year.

BluePay

FAQ 2:

MY BUSINESS HAS MULTIPLE LOCATIONS; IS EACH LOCATION REQUIRED TO VALIDATE PCI COMPLIANCE?

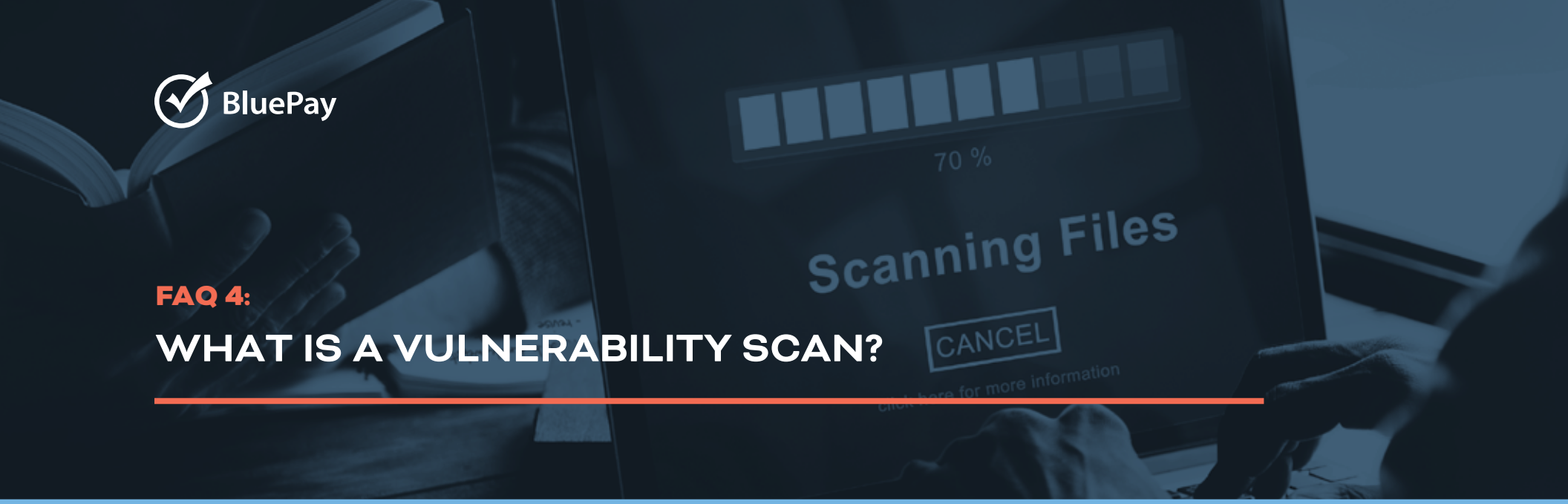
Best practices would be to certify each merchant ID (MID) number individually. Some businesses choose to certify by multiple MID numbers under one entity. However, if multiple locations are certified under one entity and a compromise were to occur, all MID numbers are subject to forensic investigation (versus only the identified MID).

BluePay

FAQ 3:

AM I PCI COMPLIANT IF I HAVE AN SSL CERTIFICATE?

No. An SSL certificate is just one piece of the puzzle to becoming PCI compliant. You must establish strong encryption of the cardholder's data during transmission over open, public networks. In addition, you need to validate that the website operators are a legitimate, legal organization.



BluePay

FAQ 4:

WHAT IS A VULNERABILITY SCAN?

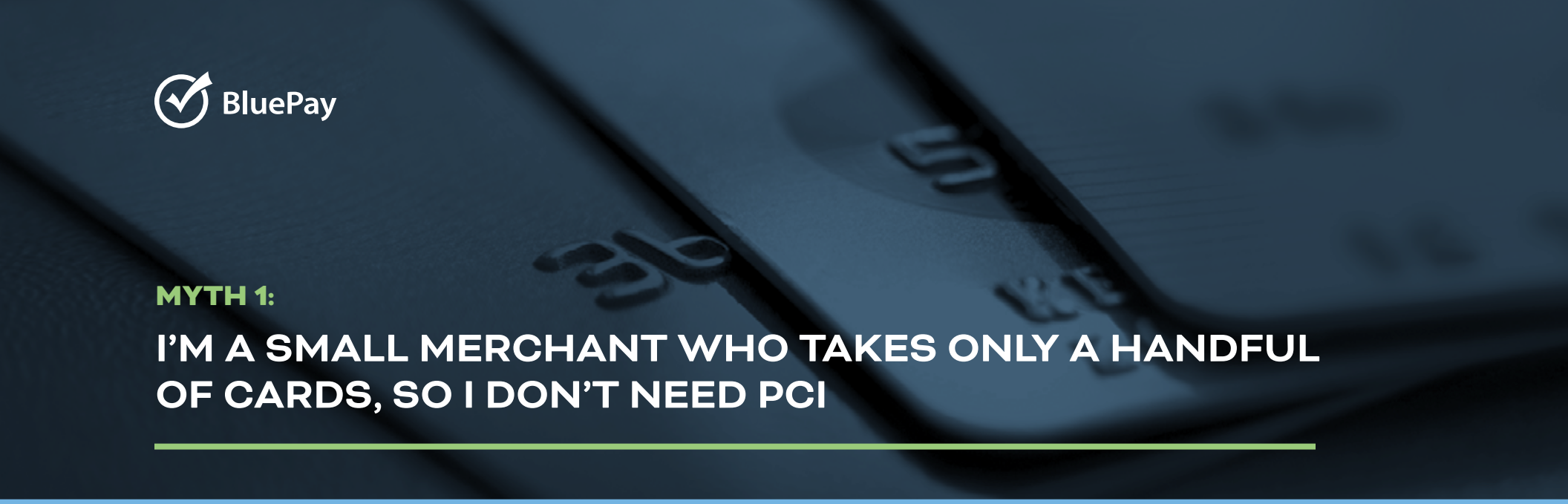
A vulnerability scan is an automated tool that conducts a nonintrusive scan of a merchant or service provider's system to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan pinpoints vulnerabilities in operating systems, services and devices that could be used by hackers to target the company's private network. Approved Scanning Vendors (ASVs), such as ControlScan, do not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks will be performed.

BluePay

FAQ 5:

ARE DEBIT CARD TRANSACTIONS IN SCOPE FOR PCI?

Any debit, credit and prepaid cards branded with one of the five card association/brand logos that participate in the PCI SSC — American Express, Discover, JCB, MasterCard and Visa International — are within scope.



BluePay

MYTH 1:

I'M A SMALL MERCHANT WHO TAKES ONLY A HANDFUL OF CARDS, SO I DON'T NEED PCI

Merchants are divided into four categories based on the number of card transactions handled in a 12-month period, but all must meet PCI requirements regardless of their size-level designation.

Smaller merchants do face fewer validation requirements, however. For a Level 4 merchant (processing fewer than 20,000 e-commerce transactions or up to 1 million transactions overall), an annual self-assessment questionnaire is recommended and a network scan by an approved vendor is to be performed quarterly if applicable, but the requirements of the bank handling the merchant's transactions still must be met for the business to be in compliance.

MYTH 2:

PCI APPLIES ONLY TO E-COMMERCE COMPANIES

Whether your business handles one transaction or hundreds of credit/debit card purchases per day, it is subject to the PCI Data Security Standards regardless of whether the transactions are electronic, in person or by phone. The requirements apply to your business if any customer ever pays you directly using a debit or credit card.

BluePay

MYTH 3:

I CAN WAIT UNTIL MY BUSINESS GROWS

As previously noted, a business of any size that processes a credit or debit card transaction is subject to PCI compliance. If you think your business is too small to attract a hacker, consider this: About 60 percent of cyber attacks in 2015 targeted small and medium-sized businesses, which in general have smaller or less sophisticated IT security staffs and resources than big corporations.

Overall, 42 percent of small businesses surveyed by the National Small Business Association reported experiencing a cyber attack. Among types of attacks, the theft of credit card information was second behind a general computer hack. The firms whose business bank accounts were hit suffered an average of more than $32,000 in losses, and 42 percent of small businesses said it took them more than three days to resolve a cyber attack issue.

BluePay

MYTH 4:

OUTSOURCING CARD PROCESSING MAKES US COMPLIANT

Relying on an outside vendor does not ensure that your business is PCI compliant. Outsourcing could reduce your risk and make it easier to prove that your business is compliant, but much like with paying your taxes to the IRS, relying on an external “expert” does not relieve your accountability.

BluePay

MYTH 5:

PCI COMPLIANCE IS AN IT PROJECT

Any temptation to shift the entire burden of PCI compliance onto the IT staff could prove costly. While IT can set up, run and test programs, compliance is an ongoing task. Rules change and regular assessments are needed, and with so much at stake from financial and reputation standpoints, your entire organization is affected.

BluePay

THIS PRESENTATION IS BROUGHT TO YOU BY BLUEPAY

BluePay, Naperville, IL
(Note: BluePay has multiple offices nationwide and in Canada; corporate headquarters is in Naperville)

www.bluepay.com
866-495-0423 (sales, toll free)
866-739-8324 (U.S. merchant support, toll free)

BluePay is a leading provider of technology-enabled payment processing for merchants and suppliers of any size in the United States and Canada. Through physical POS, online, and mobile interfaces, as well as CRM and ERP software integrations, BluePay processes business-to-consumer and business-to-business payments while providing real-time settlement, reporting, and reconciliation, along with robust security features such as tokenization and point-to-point encryption. BluePay is headquartered in Naperville, Illinois, with offices in Chicago, Maryland, New York and Toronto.