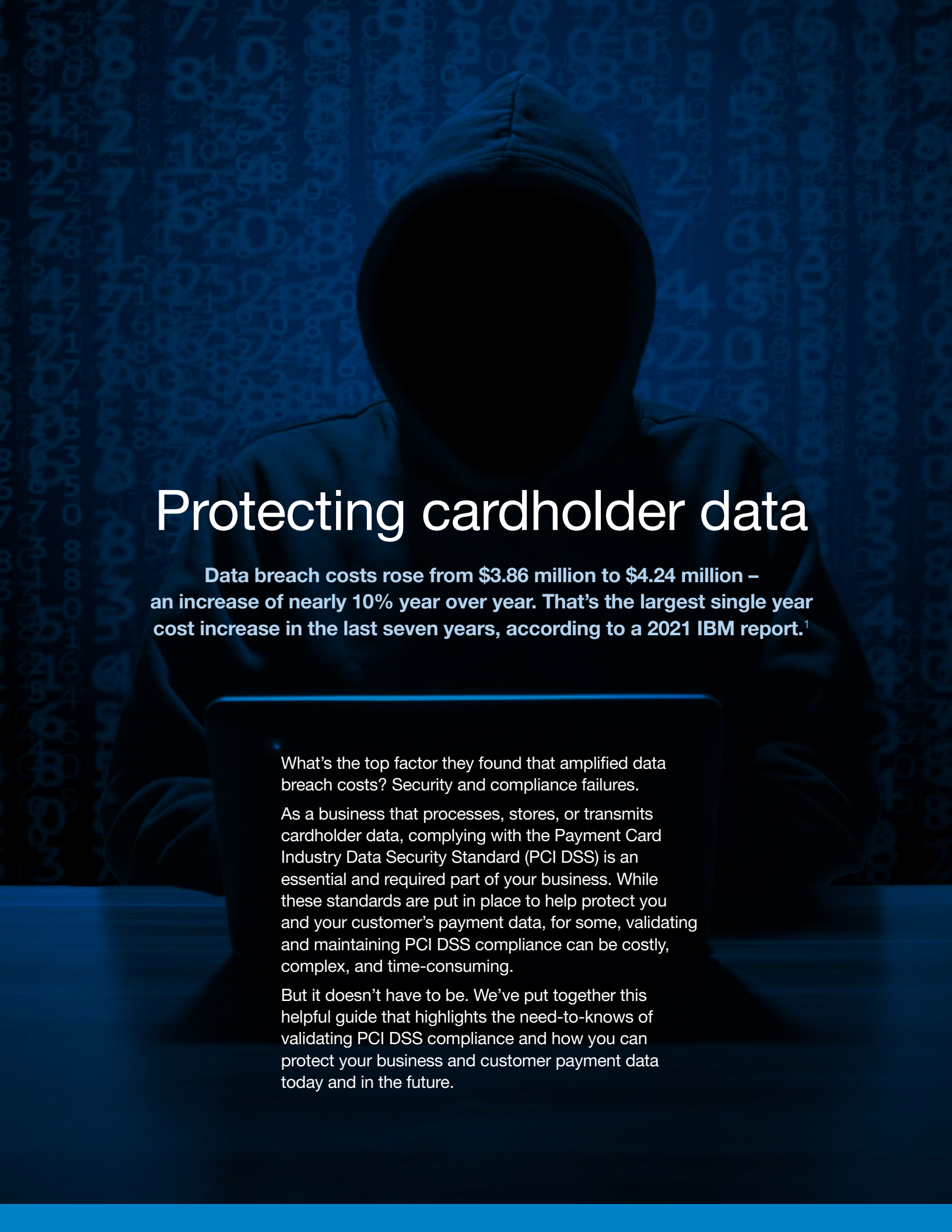
The Need-to-Knows of

PCI DSS Compliance

Elavon®



Protecting cardholder data

Data breach costs rose from $3.86 million to $4.24 million – an increase of nearly 10% year over year. That's the largest single year cost increase in the last seven years, according to a 2021 IBM report.[1]

What's the top factor they found that amplified data breach costs? Security and compliance failures.

As a business that processes, stores, or transmits cardholder data, complying with the Payment Card Industry Data Security Standard (PCI DSS) is an essential and required part of your business. While these standards are put in place to help protect you and your customer's payment data, for some, validating and maintaining PCI DSS compliance can be costly, complex, and time-consuming.

But it doesn't have to be. We've put together this helpful guide that highlights the need-to-knows of validating PCI DSS compliance and how you can protect your business and customer payment data today and in the future.

The basics of PCI DSS

To help businesses of all sizes minimize the risks associated with security and data protection, the payments industry developed the PCI Security Standards Council (PCI SCC) and the Payment Card Industry Data Security Standard (PCI DSS). The council consists of VISA®, Mastercard®, American Express®, Discover® and JCB International – the five major card brands worldwide.

PCI DSS is a global set of security requirements or best practices for payment security. These standards ensure proper security controls are in place across the entire payment ecosystem, including:

- Point-of-sale devices
- Mobile devices, personal computers or servers
- Wireless hotspots
- Web shopping applications
- Paper-based storage systems
- The transmission of cardholder data to service providers
- Remote access connections

Why your business needs to be PCI Compliant

Non-compliance can result in hefty fines and assessments from the payment card brands which require businesses accepting payment cards to annually validate compliance with the PCI DSS standard. Even worse, a data breach event could result in negative brand perception and even the loss of your business.

Levels of compliance

The first step in validating PCI compliance starts with knowing which requirements apply to your business. There are four different PCI compliance levels which are based on the annual number of transactions your business accepts and processes. The best way to determine your compliance level is to consult with your payment processing provider.

The four merchant levels for PCI DSS compliance

Level 1: Merchants processing more than 6 million Visa or Mastercard credit or debit card transactions annually. Report of compliance must be conducted by an authorized Qualified Security Assessor (QSA) and must undergo an internal audit once a year. Additionally, once a quarter, they must submit to a network scan by an Approved Scanning Vendor (ASV).

Level 2: Merchants processing between 1 and 6 million Visa or Mastercard card-present credit or debit card transactions annually. They're required to complete an assessment once a year using a Self-Assessment Questionnaire (SAQ). Additionally, a required quarterly network scan must be provided by an ASV.

Level 3: Merchants processing between 20,000 and 1 million Visa or Mastercard eCommerce transactions annually. They must complete an annual assessment using the relevant SAQ. Additionally, a required an annual network scan must be provided by an ASV.

Level 4: Merchants processing fewer than 20,000 Visa or Mastercard eCommerce transactions annually, or those that process up to 1 million transactions. An annual assessment using the relevant SAQ must be completed, or other alternative validation exercise as defined by the acquirer and a quarterly network scan may also be required from an ASV.

It's important to know which of the PCI compliance levels you fall under as your processor will require different documentation and procedures.

The 12 PCI DSS requirements

Once you have determined your business's level of compliance, there are 12 core requirements grouped into six broader goals that are necessary to validate and achieve PCI compliance. See the chart below for the latest set of security standards, PCI DSS version 3.2.1

These 12 security requirements provide a strong foundation and should be used as a baseline when implementing a security program.

Steps to ensure PCI Compliance

In order validate PCI Compliance, organizations – including payment processors and service providers – must assess their current security infrastructure, fix any identified vulnerabilities, and submit assessment and remediation details as well as compliance reports.

The processes for validating compliance typically follow these steps, according to the PCI Security Standards[2]:

1. **Scope** – determine which system components and networks are in scope for PCI DSS
2. **Assess** – examine the compliance of system components in scope following the testing procedures for each PCI DSS requirement
3. **Report** – assessor and/or entity completes required documentation (e.g. Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls
4. **Attest** – complete the appropriate Attestation of Compliance (AOC)

Goals	PCI DSS Requirements
Build and maintain a secure network and systems	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 cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs 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 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 network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

5. **Submit** – submit the SAQ, ROC, AOC and other requested supporting documentation such as ASV scan reports to the acquirer (for merchants) or to the payment brand/requestor (for service providers)
6. **Remediate** – if required, perform remediation to address requirements that are not in place, and provide an updated report

For more detailed information about the steps, visit the PCI Security Standards Council website.

Selecting a provider

Validating and staying PCI Compliant may seem like an overwhelming venture, however, there are service providers that can help alleviate the complexities of PCI DSS compliance. Many payment processors and gateway providers offer security and PCI compliance assistance solutions to help simplify the process and reduce the cost and labor of annual PCI DSS compliance validation.

When evaluating security and PCI compliance providers, it's important to look for solution offerings that satisfy all of your PCI needs rather than just a portion. Here are a few offerings to look for when selecting a security and PCI compliance provider:

Security software and tools

Look for state-of-the-art security technologies like encryption and tokenization that protect sensitive payment data both "in-transit" and "at rest." Cybersecurity software adds an extra layer of support to protect your devices against malware and cybercriminals. And lastly, many providers will offer online PCI DSS compliance validation tools, including assistance with the PCI Self-Assessment Questionnaire (SAQ) and network vulnerability scanning (if applicable).

Breach Assistance

While every business that processes credit cards must validate with the PCI-DSS on an annual basis, breaches still occur. In the event of a data breach event, a breach assistance program can provide your business with financial assistance and help reimburse financial costs associated with forensic investigations, card replacement costs, fines, fees, or assessments from the payment card networks affected by the breach.

Comprehensive support

Your provider should offer comprehensive and ongoing support when you need it and should be accessible via online help, email, and phone. Since PCI compliance is not a single task but an ongoing process, your provider should reach out to you throughout the year if anything needs to be done to maintain compliance or if your compliance needs to be renewed.

Education

The world of PCI DSS compliance is complex. Look for a provider that offers access to valuable tips, information and best practices that make it easy for you to understand how you can safeguard your business and your customer payment data.

Next steps

Ready to improve your data security and validate your PCI DSS compliance? As your trusted payments partner, Elavon is committed to providing payment security solutions you and your business can rely on. From payment security and fraud mitigation to PCI DSS Compliance Validation, we offer the data security and risk reduction expertise so you can focus on growing your business, increasing your revenue, and building customer trust.

Ready to get started?

For additional information about Elavon and our security and compliance solutions, contact:

John Webb
937-671-1606
john.webb@usbank.com

Elavon

[1] IBM Security: Cost of a Data Breach Report 2021, [2] PCI Security Standards Council