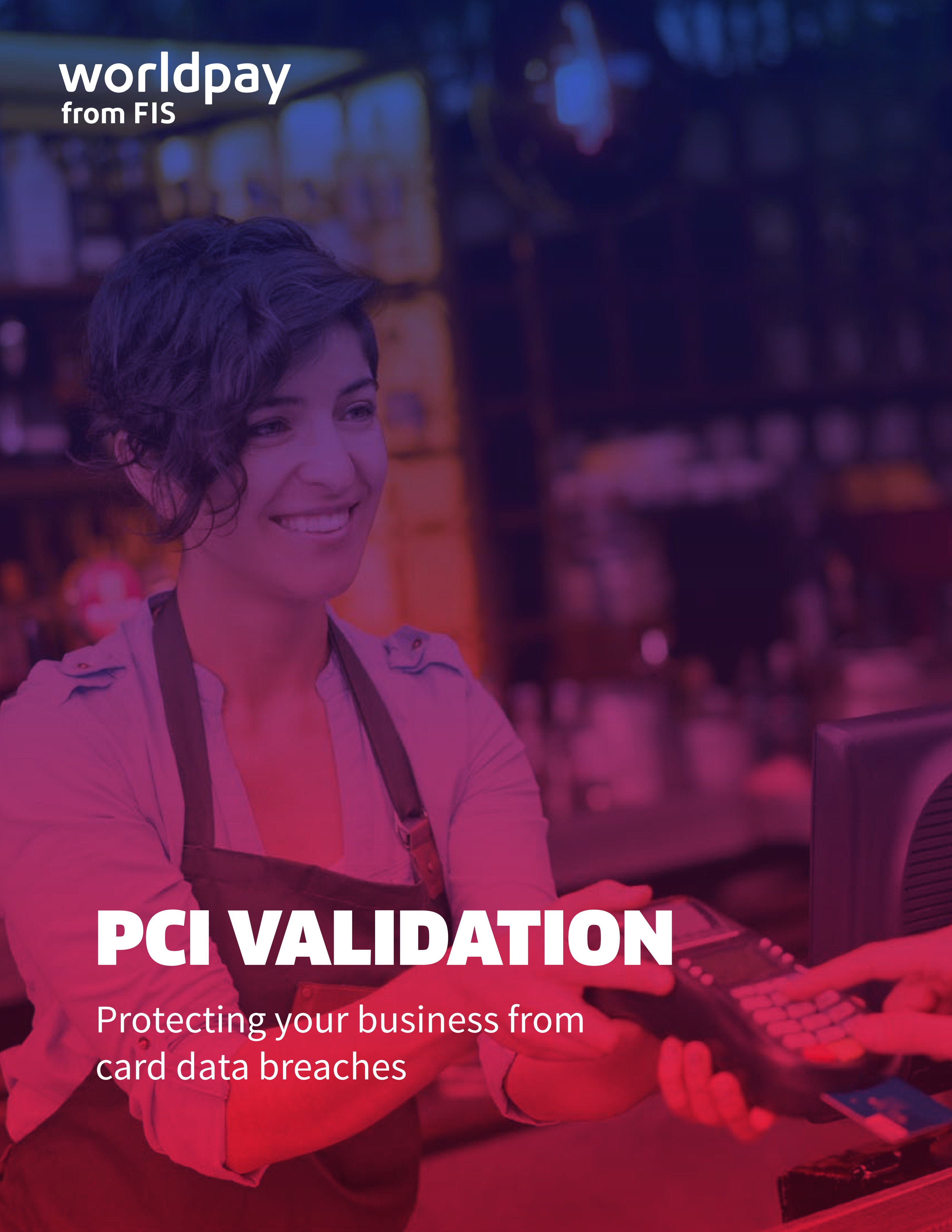

worldpay
from FIS

PCI VALIDATION

Protecting your business from card data breaches

What is the PCI Data Security Standard?

The Payment Card Industry Data Security Standard (PCI DSS) is an evolving framework designed to protect cardholder data. This multifaceted security standard outlines the minimum requirements that must be in place for security management, policies, procedures, network architecture, software design and other critical protective measures.

Who must comply?

If you process, store or transmit cardholder data, you must comply with all aspects of the standard at all times. If you don't comply, you could lose your ability to accept credit cards. We can help.

Using the PCI Data Security Standard as the framework, we have developed the PCI Program as your roadmap to protection and PCI DSS validation.

Data breaches are costly

Not only must you comply with the PCI DSS, but you are ultimately responsible for damages or liability that may result from a data security breach or non-compliance with PCI DSS.

Merchants who suffer security breaches and/or an account data compromise may be subject to the following costs:

- Forensic investigation
- Fines from the card associations
- Operational and fraud loss expenses incurred by card issuing banks
- Litigation
- Brand and Reputation Damage
- Government-Levied Fines

It could happen to you

The majority of all card data security breach cases occur at small retail locations. How?

- Insecure remote access
- Default or weak passwords/credentials
- Improper storage of paper receipts, and reports, and other documents containing cardholder data
- Improper care when handling a customer's credit card
- Improper storage of card information on computer systems in an unsecured fashion
- Improper storage of hand written credit card information
- Improper or nonfunctioning firewalls between a physical dial terminal and another device that may be connected to the Internet
- Utilizing software that is not PCI compliant and is improperly storing cardholder data in an unsecured fashion

Protecting you, your customers, and your data

While larger businesses may have more resources than smaller businesses to deal with the repercussions of a breach, they are not immune to data theft. The challenge to protect payment card data impacts merchants both large and small, and it's constantly changing.

That's why we offer unparallel guidance, backed by a dedicated PCI Specialty Team to help you be more secure and stay continually up-to-date on the latest in card data security. We've partnered with best in class leaders in the industry, to help simplify the process so you can achieve and maintain your compliance year after year.

PCI program

Full compliance with the PCI Data Security Standard is considered by many in the industry to be one of the best ways to protect your systems from unauthorized intrusion. To make it easier for you to comply with the PCI DSS, we have developed a comprehensive security program to help you protect your business and give you peace of mind.

What do you receive in the program?

Access to an online PCI certificate validation tool that allows you to complete your Self-Assessment Questionnaire (SAQ) and track:

- Your PCI certificate number
- Your certificate renewal date

A Self-Assessment Questionnaire is a list of questions developed by the PCI DSS Council to mirror the PCI DSS. There are currently 8 questionnaires covering different types of merchant's processing arrangements. Additional questionnaires may be added to cover new payment solutions such as P2PE and mobile technologies. The online tool will be modified as needed to cover such scenarios. The current questionnaires are:

SAQ A	For card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This does not apply to face-to-face merchants.
SAQ A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic cardholder data storage.
SAQ B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial out terminal merchants with no electronic cardholder data storage.
SAQ B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.
SAQ C-VT	Merchants using only web-based virtual terminals without an integrated mag-stripe reader, no electronic cardholder data storage.
SAQ C	Merchants with payment application systems or terminals connected to the Internet, no electronic cardholder data storage.
SAQ P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.
SAQ D	Merchants who process credit card transactions electronically and DO STORE cardholder information electronically at their merchant locations. Or those merchants that do not meet the eligibility criteria for the above SAQ types.

Access to remote vulnerability scanning services, which includes the following (for PC/IP only):

- Fully integrated scanning
- User friendly reports and tools
- Online scan support and remediation guidance

Access to pci.worldpay.com, which provides you:

- The ability to log in to the self-service portal to complete their compliance reporting on-line
- Access to a PCI support line, on-line chat support and rich on-line guidance
- Improved experience with a fully guided end-to-end compliance journey
- Task and revalidation reminders
- Information security templates
- Online employee security
- Education and training

Waiver benefit*

If you have successfully validated your compliance with the PCI DSS through the PCI Program, in the event of a verified card data security breach, we will waive up to $50,000 of your liabilities for:

- Costs associated with mandatory Card Brand audits conducted if a breach occurs
- Fines assessed as a result of Card Brand audit findings following a breach
- Costs associated with credit card replacement for compromised card numbers

Additional Valuable Benefits:

- You may utilize a cardholder data security policy template that can be used as a guide for the creation of a policy that fits the specific needs of your location's card processing environment
- A validation certificate you can use to notify all of your customers that you take the security of their credit card information seriously

* Without the Waiver Benefit, you will remain liable for all costs and fines related to a verified suspected or confirmed card data breach! See the Terms and Conditions of the merchant agreement for important information and limitations on the waiver.

It’s easy to complete PCI validation online

1. Go to **pci.worldpay.com** or open the email you received from **notifications@pci.worldpay.com**

2. Sign-in Information:

   If you received an email from **notifications@pci.worldpay.com**, this will contain your credentials to login to **pci.worldpay.com** to start your PCI assessment.

   Alternatively, you may also access the new tool by visiting **pci.worldpay.co**m. Click the ‘First sign-in’ link on this page and input your merchant ID when prompted. You will then need to create an account and confirm your email address to register.

3. If you need help getting started and logging in please call our help desk at **833.534.8422**.

worldpay
from FIS

For more information about the PCI Program, please contact our dedicated PCI Specialty Team by phone at **833.534.8422**

WFIS007 10.19