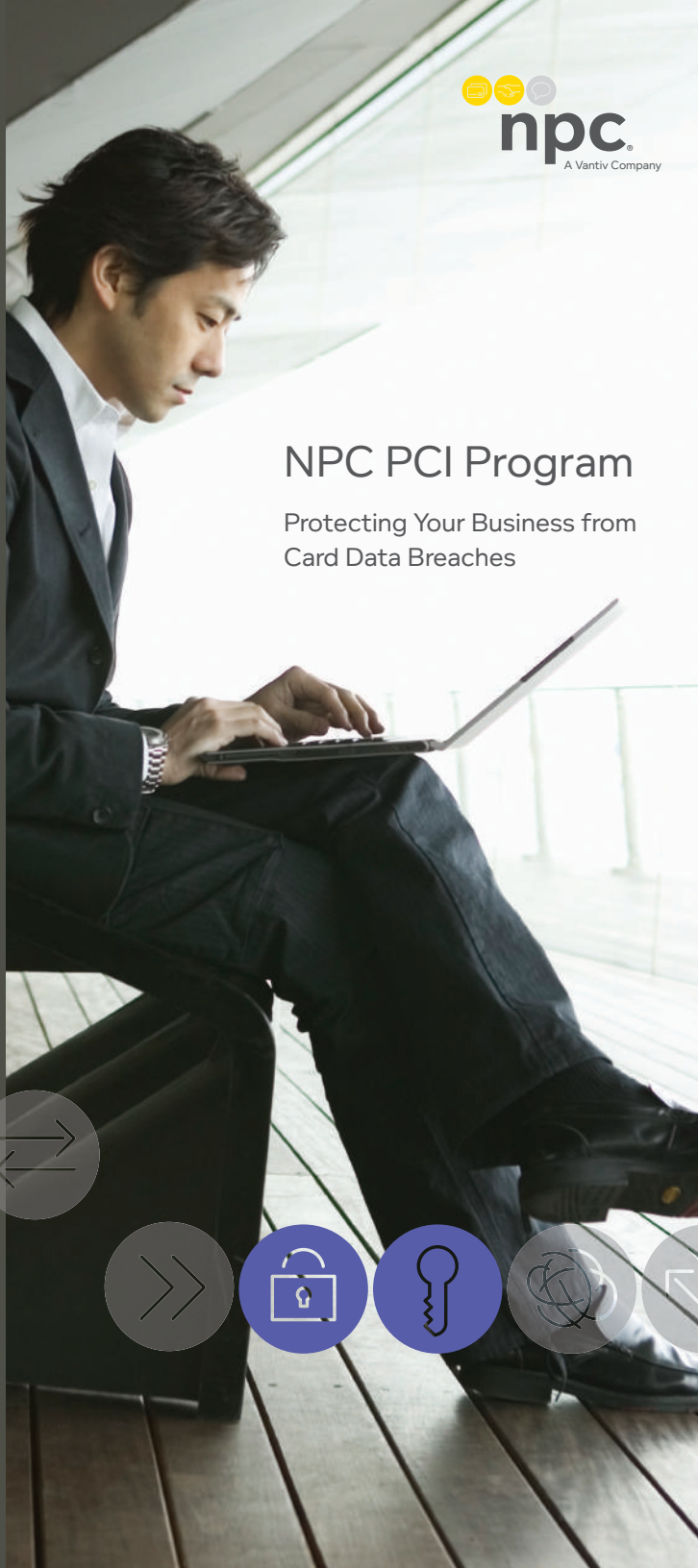


NPC PCI Program

Protecting Your Business from Card Data Breaches

For more information about the NPC PCI Program, please contact our dedicated PCI Specialty Team by email at pcicompliance@npc.net, or by phone at 877.479.6649

npcdata.net

NPCIBRO002 05.14

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, NPC has developed the NPC PCI Program as your roadmap to protection and PCI DSS validation.

FACTA and Other Applicable Laws

In addition to complying with PCI DSS, you are also required to comply with all local, state and federal laws that apply to your business. One such law is the Fair and Accurate Credit Transactions Act (FACTA) regarding the protection of cardholder data. FACTA is a federal law that states "no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of sale or transaction." U.S.C. §1681(c)(g).

In addition, the Card Brand rules require that all merchants truncate all but the last four digits of the cardholder number, and also mask the expiration date on the merchants' copies of the electronically printed receipts.

It is every merchant's responsibility to understand and comply with FACTA, and, in general, to protect each customer's cardholder information. In addition, your business may be subject to other state laws that impact the information you may print on receipts. It is a good business practice to check the laws of your state to determine if you are compliant.

You should evaluate your obligations under FACTA and other applicable state laws and review your receipts to determine if the receipts are compliant.

You should also ensure that your security policy not only complies with the requirements of the PCI DSS, but also with FACTA and other applicable laws.

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's **Easy** To Complete PCI Validation Online

1. Go to npcdata.net.
2. Select the box labeled "New Registration".
3. Sign-in Information:

MID = Merchant Identification Number: this number can be found on your monthly processing statement labeled "Merchant NBR". Also, merchants who use terminals purchased through Vantiv can find the MID on your terminal sticker located on the side of the terminal.

Tax ID/SSN = Merchant's 9 digit tax identification number for the business.

No tax identification number?
Enter in the 9 digit social security number of the signer on the account.

Billing ZIP = (First Time Use Only) The postal zip code for the business.

Hit the "Enter" key to submit your registration.

4. The system will prompt you to change your password.

Old Password = 9-digit Tax Identification number or 9 digit Social Security Number that was used to sign into the online system.

New Password = You will create a new password. The password should be minimum of 8 characters. Include at least one letter and one number.

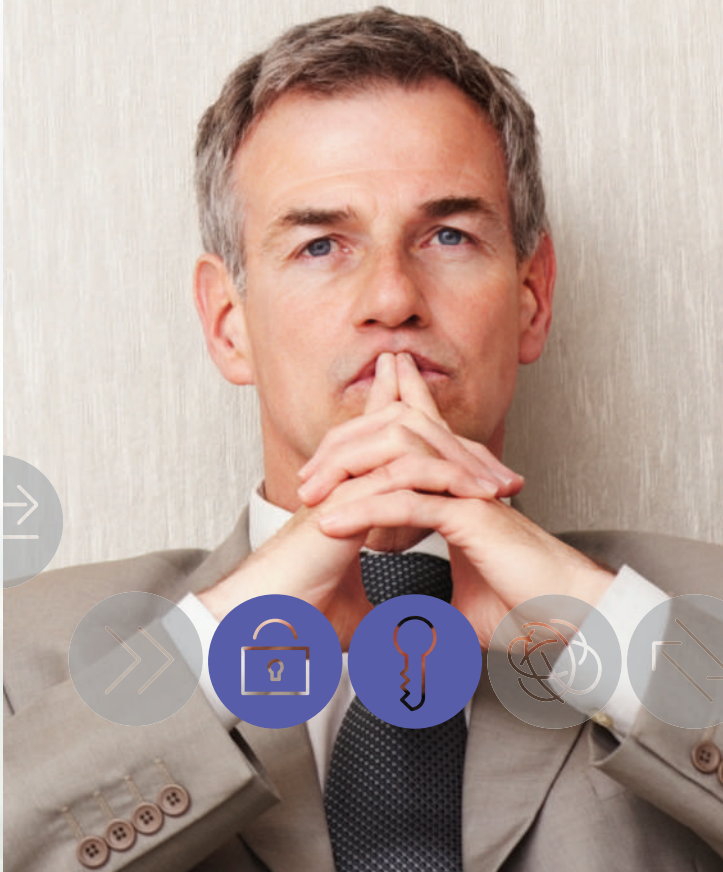
New Password Confirmation = Retype the newly created password for confirmation.

Hit the "Enter" key to submit the password change.

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.



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

5. The new screen will provide a message that states "**NPC Password Change**". Under the box, the screen states "**You have successfully changed your password…**" Click the NPC logo to continue.

6. Select the box that says "**Click here to complete the questionnaire online**".

7. Select the box that says "**Begin Data Security Compliance**" at the bottom of the page.

8. This is the education page of the survey and the first of five steps in validating your compliance with the PCI DSS.

NPC 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, NPC has 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 5 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 B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial out terminal merchants with no electronic cardholder data storage.
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 D	Merchants who process credit card transactions electronically and DO STORE cardholder information electronically at their merchant locations. Or those merchants that do no meet the eligibility criteria for one of the four shortened questionnaires above.

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 MyNPCData, which allows you to:

- Evaluate daily, weekly, and monthly batch summaries and detail
- Research transactional detail
- Track return history
- Access retrievals and chargeback information
- Look up payment deposit history on a daily or monthly basis
- Review up to two years of prior statements

Waiver Benefit*

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