

NPC PCI PROGRAM



GUIDE TO ASSIST YOU IN
PROTECTING YOUR BUSINESS
FROM CARD DATA BREACHES



NPC[®]

WHO MUST COMPLY?

YOU.



The Card Brands have mandated that ALL MERCHANTS must comply with the PCI DSS (Payment Card Industry Data Security Standards) found at www.pcisecuritystandards.org.

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.

The majority of all card data security breach cases occur at small retail locations, including land-line dial terminal merchants. How?

- **Improper storage of paper receipts and reports 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**
- **The use of unsecured voice over IP communication technology**

WHAT DO YOU RECEIVE?

NPC takes data security very seriously. Merchants are required to comply with the PCI DSS, and are ultimately responsible for damages or liability that may result from a data security breach or non-compliance with PCI DSS.

To make it easier for you to comply with the PCI DSS, NPC has developed a comprehensive security package to help you protect your business. What do you receive in the program?

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

- Your PCI certificate number
- Your certificate renewal date
- Updated PCI regulations

Access to TrustKeeper remote scanning services, provided by Trustwave, which includes the following (for PC/IP only):

- Monthly vulnerability scanning for up to five (5) of your computer website (IP) addresses (additional fees apply if you have more than 5 IPs)
- Online support and remediation guidance

**Call us at 1-877-479-6649
for more details.**



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 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 card data breach! See the Terms and Conditions of the merchant agreement for important information and limitations on the waiver.

HOW TO COMPLETE PCI VALIDATION ONLINE

1. Go to **www.npcdata.net**.
2. Select the yellow 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 NPC can find the MID on your terminal sticker located on the side of the terminal.
 - **Tax ID/SSN** = Merchant's 9 digit tax identification 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 "Enter" key to submit registration.
4. The system will prompt merchant to change their passwords.
 - **Old Password** = 9-digit Tax Identification number or 9 digit Social Security Number that was used to sign into the online system.
 - **New Password** = Merchant will choose 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 "Enter" key to submit password change.

LOG-IN INSTRUCTIONS FOR FIRST-TIME MERCHANTS



5. The new screen will provide a message in a blue box that states **“NPC Password Change”**. Under the blue box, the screen states **“You have successfully changed your password...”** Click the NPC logo to continue.
6. Select the yellow box that says **“Click here to complete the questionnaire online”**.
7. Select the yellow 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.

SECURITY POLICY

As part of the PCI DSS, the Card Brands require that each merchant have a security policy that covers the security of credit card information. A sample security policy is available at www.NPC.net. This sample is provided for your convenience only to assist you in developing your own security policy that addresses the security of cardholder information as required by the PCI DSS. NPC makes no representations that this sample security policy will satisfy your requirements under the PCI DSS as it relates to your processing environment. You may use the security policy as a template, but it is your responsibility to ensure that the security policy you implement meets all of your security needs. If you already have a security policy in place, you may want to compare it to the sample policy to verify that your policy contains the required items. You should review and update your security policy on an annual basis.

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).

REQUIRED INFORMATION

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.



SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

A Self-Assessment Questionnaire is a list of questions developed by the PCI DSS Council. There are 5 questionnaires covering different types of merchants:

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, no electronic cardholder data storage.
SAQ C	Merchants with payment application systems 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.

Any Questions?

Please contact our
dedicated PCI Specialty
Team by email at
pcicompliance@npc.net, or
by phone at **877-479-6649**.



NPC PCI PROGRAM



NPC®

Copyright 2011 NPC

NPCPCI 0611