PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) FREQUENTLY ASKED QUESTIONS

This FAQ for PCI Data Security Standard is provided to inform and educate merchants that process, store or transmit cardholder data.

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) was created by the five major credit card companies as a guideline to help business owners implement the necessary hardware, software and other procedures to safeguard sensitive credit card and personal information. PCI DSS is a set of requirements for enhancing payment account data security. The five major credit card companies that developed the PCI Security Standards Council are American Express, Discover® Financial Services, JCB International, Mastercard® and Visa.

What does PCI Compliance mean?

PCI Compliance means that your business is exhibiting the best practices to protect cardholder information and prevent data security breaches. While PCI Compliance is not a guarantee of security, it is an important step in prevention.

I have never heard of PCI Compliance before. Is this new?

No. PCI was created in 2004 and business owners began taking the PCI Self-Assessment Questionnaire (SAQ) to identify potential security risks to achieve PCI Compliance starting in 2005.

What am I required to do to become PCI Compliant?

The minimum requirement is to complete a Payment Card Industry Data Security Standard Self-Assessment Questionnaire (SAQ) on an annual basis and achieve a passing score. If cardholder information is stored or if your processing systems have any internet connectivity, a quarterly scan is required.

How long will obtaining PCI Compliance take?

PCI Compliance can vary based on how your business processes, stores or transmits cardholder data. It takes about 5 to 10 minutes to enroll in the program and 15 minutes to complete the self-assessment questionnaire. In less than 30 minutes, you could be PCI Compliant.

How long is the PCI Compliance certification valid?

The length of time a PCI Compliance certificate is valid for depends on whether your business requires a questionnaire and, where applicable, a scan. If your business requires only the questionnaire, the PCI certification is valid for one year. If your business also requires quarterly scans, the PCI certification is valid for three months, at which time your next quarterly scan will be due.

Am I required to certify for PCI Compliance?

Participation in a certified PCI DSS Compliance program is mandatory for every merchant, regardless of the bank you use. Failure to comply may result in fines of up to US$500,000 (levied by the Payment Associations such as Visa or Mastercard). It is important to note that these fines do not include the expenses or costs of fraudulent transactions that may arise from a breach. In addition to avoiding potential fines, PCI Compliance gives you the confidence that your customer's credit card information is protected at your business.

What does PCI mean to the Bank?

The Bank has upgraded its procedures, physical security, hardware and software to further enhance the security around card data and our customers personal account data.

NATIONAL COMMERCIAL BANK JAMAICA LIMITED