Security Standards

Cardholder Data Security is your Responsibility

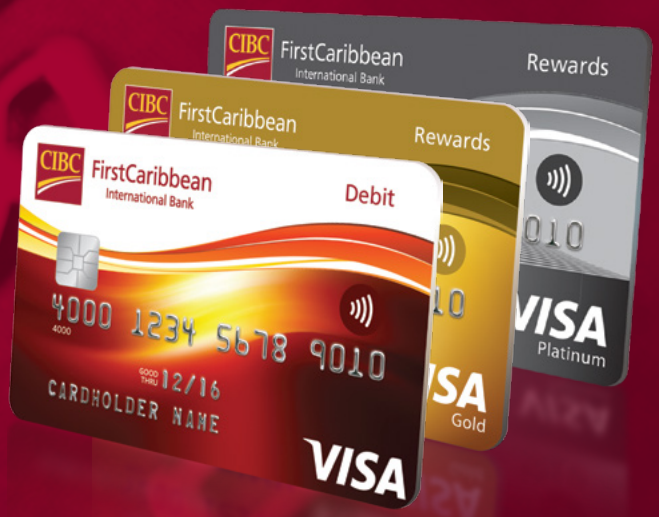
Ensuring the safety of your customers' cardholder information can help your business create and maintain a positive image, enhance customer confidence and assist in improving your bottom line.

As part of CIBC FirstCaribbean International Bank's provision of card processing services, we want to provide you with some critical information regarding maintenance of Data security and how the Payment Card Industry (PCI) Data Security Standard (DSS) and the Card Networks' Compliance Programs will assist with this goal.

Please note that all Merchants who store, process, or transmit cardholder data must comply with PCI DSS and the Card Networks' Compliance Programs. However, certification requirements vary by business and are contingent upon your "Merchant Level". Failure to comply with PCI DSS and the Card Networks' Compliance Programs may result in your business being subject to fines, fees or assessments and/or termination of processing services.

The PCI DSS is enforced by the Card Networks (American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International).

CIBC FirstCaribbean International Bank has taken the steps to provide you, our valued client, with necessary information and associated links to assist in assessing the actions your business should take to ensure that you are compliant.



Contents

About PCI SSC

The PCI Security Standards Council (PCI SSC) is an independent body founded in September 2006 by five major credit card networks - American Express, Discover Financial, JCB, MasterCard Worldwide, and Visa International. The PCI SSC is responsible for the development and ongoing evolution of security standards for account data protection.

For more information on the PCI SSC please visit:

https://www.pcisecuritystandards.org/pci_security/

About PCI DSS

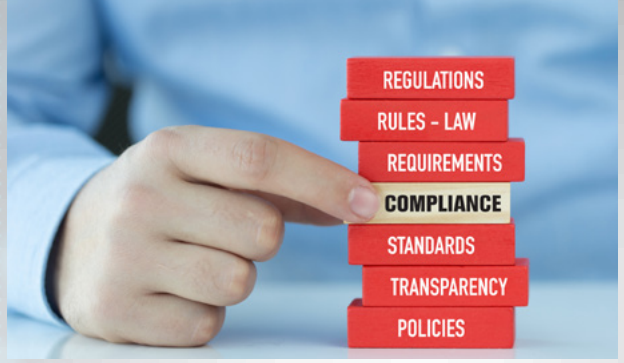
The Payment Card Industry Data Security Standards (PCI DSS) was created to assist with the protection of cardholder data. Due to a few high profile security breaches it became apparent that a global set of data security standards was required to assist merchants and service providers in meeting these technical and operational requirements.

In direct response to this need, the PCI SSC developed the six goals which translate to the twelve requirements of the PCI DSS

Twelve Principle Requirements of PCI DSS

PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures This comprehensive standard is intended to help organizations proactively protect customer account data.

The Twelve standards can be found here:
https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security



Importance of PCI DSS Compliance and/or Certification

CIBC FirstCaribbean International Bank strongly endorses the need for stringent standards regarding the handling of cardholder data. In addition, we are taking proactive measures to ensure that all merchants adopt these standards and maintain compliance on an on-going basis.

Compliance with the PCI DSS is mandatory. If you and your service providers are not compliant with PCI DSS, the Card Networks could levy fees and fines against you and your card processing services could be terminated.

Compliance means all technical and operational requirements of the PCI DSS have been met. To become certified, an entity must engage the services of Qualified Security Assessor "QSA" to validate an entity's compliance to PCI DSS. The QSA will work on identifying areas of non-compliance. The merchant must remedy each area of non-compliance. Once all areas of non-compliance have been addressed the QSA will re-evaluate and issue confirmation of compliance. Certification to PCI DSS is at the merchant's expense. **Merchants will be required to provide evidence of certification when requested by CIBC FirstCaribbean.**

To assist merchants with understanding the environment in which you accept cards and the risks that you may be exposed to the PCI SSC has developed a number of tools that you can refer to:

Merchant Guide to Safe Payments:
https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf

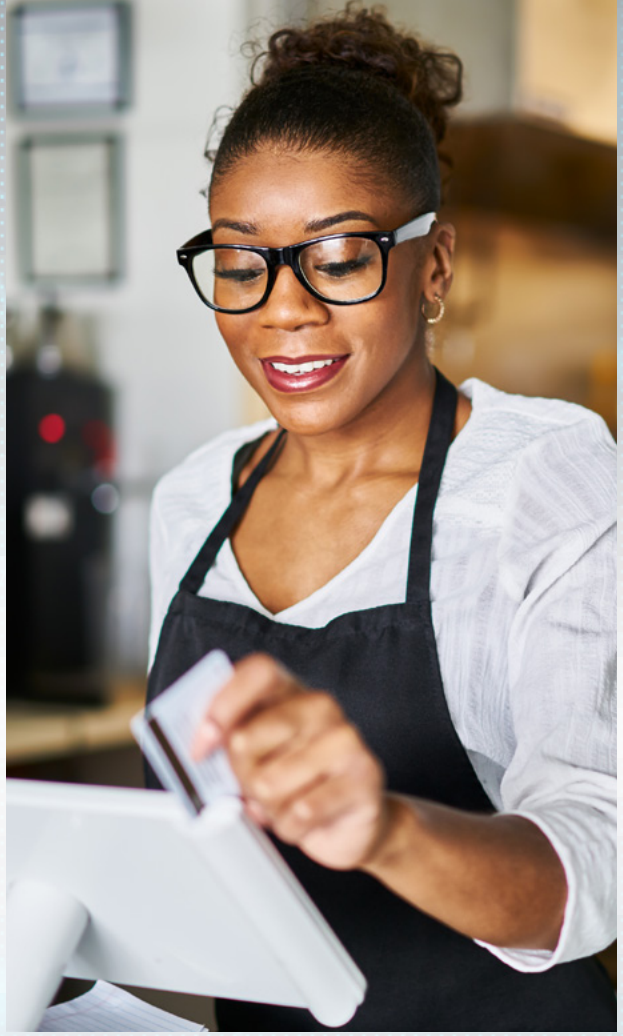
Merchant Data Security Essentials Evaluation Tool:
https://www.pcisecuritystandards.org/pci_security/small_merchant_tool/index.html

Merchant Levels and Validation Requirements

It is important to note that all merchants that store, process, or transmit cardholder data must comply with the PCI DSS regardless of the volume of transactions processed or the method in which they are processed. However, certification requirements vary by business and are contingent upon your "Merchant Level".

Merchant Level Description	
Level	**Level Description**
1	Any merchant regardless of acceptance channel, processing over 6,000,000 Visa or MasterCard transactions annually (all channels). Any merchant that has suffered a hack or an attack that resulted in an account data compromise. Any merchant that a Card Network, at its sole discretion, determines should meet the Level 1 merchant requirements.
2	Any merchant processing between 1,000,000 and 6,000,000 Visa or MasterCard transactions annually of one card plan (all acceptance channels).
3	Any merchant processing between 20,000 and 1,000,000 Visa or MasterCard e-commerce transactions annually.
4	Any e-commerce merchant processing fewer than 20,000 Visa or MasterCard e-commerce transactions annually. Any merchant (regardless of acceptance channel) processing fewer than 1,000,000 Visa or MasterCard transactions annually.

Validation Requirements			
Merchant Level	**Validation Requirements**	**Validated By**	**Validation Due Date**
1	Annual On-site PCI Data Security Assessment	Qualified Security Assessor (QSA)	Annually
	Annual PCI Self Assessment Questionnaire		
	Quarterly Network Scan	Approved Scanning Vendor (ASV)	
2	Annual PCI Self Assessment Questionnaire	Qualified Security Assessor (QSA)	Annually
	Quarterly Network Scan	Approved Scanning Vendor (ASV)	
3	Annual PCI Self Assessment Questionnaire	Qualified Security Assessor (QSA)	Annually
	Quarterly Network Scan	Approved Scanning Vendor (ASV)	
4*	Annual PCI Self Assessment Questionnaire	Qualified Security Assessor (QSA)	Annually
	Quarterly Network Scan	Approved Scanning Vendor (ASV) *PCI DSS requires that all merchants perform external network scanning to achieve compliance (requirement 11.2). Acquirers may require submission of scan reports and/or questionnaires by level 4 merchants.	



Service Providers

A service provider is defined as an organization that stores, processes, or transmits cardholder data on behalf of merchants or other service providers. All service providers are required to comply with PCI DSS. In addition all service providers are required to validate their compliance to PCI DSS through the services of a QSA.

Visa and MasterCard each publish a list of compliant service providers on their websites. For a list of service providers that have validated their compliance to PCI DSS please see:

Visa Global Registry of Service Providers:
https://www.visa.com/splisting/searchGrsp.do

The MasterCard SDP Compliant Registered Service Provider Listing:
https://www.mastercard.us/content/dam/mccom/global/documents/Sitedataprotection/site-data-protection pci-list.pdf

Payment Application Data Security Standard

The Payment Application Data Security Standard (PA-DSS) is a standard managed by the PCI SSC. This standard is based on Visa's Payment Application Best Practices (PABP). Many merchants deploy third party payment applications that are tailored to their business needs to assist them in accepting credit card payments.

The goal of PA-DSS is to assist software vendors develop secure payment applications that do not store prohibited data, such as full magnetic stripe data, card verification values, or PIN data, and ensure their payment applications support compliance with the PCI DSS. Vulnerable payment applications that store prohibited dat are the leading cause of account data compromises among small merchants.

Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements. In-house Payment applications developed by merchants or service providers that are not sold to third parties are not subject to the PA-DSS requirements, but must still be secured in accordance with the PCI DSS. PA-DSS is not applicable to standalone point-of-sale terminals, database software or web server software.

Further information on PA-DSS including a list of payment applications that have validated their compliance to PA-DSS can be found at:
www.pcisecuritystandards.org

Helpful/Related Links

For more information on the PCI security standards and the Card Network Compliance Programs, please review the following websites:

PCI Security Standards Council:
https://www.pcisecuritystandards.org

Visa LAC AIS Program:
https://www.visa.com.bs/run-your-business/small-business/information-security.html

MasterCard Worldwide SDP Program:
https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html

Industry Websites

PCI Security Standards Council:
https://www.pcisecuritystandards.org

Visa LAC AIS Program:
https://lac.vis.com/merchant.security.jsp

MasterCard Worldwide SDP Program:
http://mastercard.com/sdp

Call us toll free at 1-866-743-2257 for more details.

CIBC FirstCaribbean International Bank