INTRODUCTION TO PCI COMPLIANCE

All merchants (regardless of business size) are required to adopt the security standards in accordance with the **Payment Card Industry Data Security Standard (PCI/DSS)** to increase card data security and reduce fraud. The breach or theft of cardholder data affects the entire payment card ecosystem. Customers suddenly lose trust in merchants or financial institutions, their credit can be negatively affected – there is enormous personal fallout. Merchants and financial institutions lose credibility (and in turn, business), they are also subject to numerous financial liabilities. It is FrontStream's mission to keep your customer data safe but we need you to do your part and register for PCI and become PCI compliant.

Important Contact Information

PCI Security Council
https://www.pcisecuritystandards.org/
FNBO Merchants
https://www.securitymetrics.com/pcidss/frontstream
FDR Merchants
https://login.pcirapidcomply2.com/portal-core/home
Elavon Merchants
https://pcicompliancemanager.com/services/login/login
Cynergy Merchants
https://www.securitymetrics.com/pcidss/frontstream

For PCI Data Security Standards information and requirements, visit the following websites:

PCI Security Standards Council
https://www.pcisecuritystandards.org/#
American Express
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=pci&ln=en&frm=US
Discover Network
http://www.discovernetwork.com/fraudsecurity/disc.html
MasterCard SDP
http://www.mastercard.com/us/merchant/security/what_can_co/SDP/merchant/index.html
Visa CISP
http://usa.visa.com/merchants/risk_management/cisp.html

frontstream® payments

10 PRACTICAL STEPS

From the PCI Data Security Standard

1. Educate
Employees should be trained annually on both online and physical security threats as well as on the best practices for protection cardholder data.

2. Update
Keep your employee manuals up-to-date with the information on the proper handling of sensitive information, including card data.

3. Screen
Pre-employment screening is a basic and essential practice for any business owner, especially for those employees that have access to sensitive customer or financial data.

4. Protect
Make sure your business has a firewall, anti-virus, malware and spyware detection software. And don't forget to regularly update the software.

5. Control
Tightly control downloads, software installations, the use of thumb drives and public Wi-Fi connections on computers used for payment card processing.

6. Be Aware
Pay attention to fraud prevention alerts from your virus and malware services, make sure you install updates as soon as they become available.

7. Separate
Designate a separate computer for processing of all your online financial transactions. Try to keep this computer separate from social media sites, email and general internet browsing which can presser changes for the computer to be susceptible to vulnerabilities.

8. Change
Change your password regularly, and especially after you have outside contractors do hardware, software or Point of Sale System installations or upgrades. Make sure that you use complex passwords to make them more difficult to guess (include upper case letters, numbers and special characters).

9. Back up
Regularly back up your computers and the key data you want to protect, whether it's to a local machine or an offsite facility, so your business can be up and running again quickly in the unfortunate event of an unauthorized attack.

10. Learn
Check out the PCI security standards council website for more information on the Data Security standards, education and training resources available to you.

frontstream® payments

Happy Processing!