PCI (Payment Card Industry) Compliance 2016

What is PCI?

The Payment Card Industry Data Security Standards (PCI DSS) have been put in place by the major card companies (Visa, MasterCard, Discover, and American Express) to help protect your business. The PCI standards require all merchants to complete a Self Assessment Questionnaire, also known as an **SAQ**, so that merchants validate they are processing secure and sensitive data in the most efficient manner.

How do we protect our merchants?

CWA has developed a unique outlet to ensure our merchants have all the tools necessary to maintain compliance and avoid fines from the major card brands. Our goal is to provide a comprehensive set of automated, online security services and hardware devices to help businesses detect and repair security problems at reasonable prices. This platform has been used with large corporations, government agencies, and financial institutions to help clients protect against fraud as well as maximize security and compliance.

CWA Merchant Services offers a PCI solution which has been crafted specifically for our merchants. Our solution offers merchants the following:

- Coverage up to **$50,000** for fines associated with data breaches on your account and up to **$500,000** for total losses. These fines would be passed down from the card brands.
- Auto-Enrollment into our PCI solution upon being accepted as a new merchant with CWA, protecting a merchant's business from Day 1.
- Username and password for PCI Toolkit will be sent within two weeks of signing with CWA.

- Direct point of contact at CWA for all PCI related questions and for Chargeback mitigation.
- Detailed reporting from all scans and updates (PenTest, etc.)

What does a merchant need to do?

Login to the CWA portal, a computer based program called the PCI TOOLKIT® which we have created to simplify merchant compliance.

https://cardworks.pcitoolkit.com/version3

What if a merchant never received their info to login and complete the PCI Questionnaire/SAQ?

We can email them their information and help the merchant through completing the SAQ. This takes about 10-15 minutes and they will receive a certificate identifying that they process credit cards in a secure manner. This certificate covers most merchants for one year and the merchant must recertify after that time period. A lot of our merchants have this certificate by their credit card machine so customers know that when using their credit card, it is being done in the safest possible manner.

All merchants are sent this information within two weeks of signing up with CWA.

What to explain to a merchant that questions about fees, compliance, and coverage:

These are actual pass through fees from our PCI Compliance Partner. CWA has researched many different companies that offer this service and our partner offers the best package for the cost of being PCI Compliant. We have developed this program so that merchants can worry about running their day to day business without fear of

being fined or even worse, banned from accepting credit cards all together. All they are required to do is answer 15-20 questions about how they process today. By completing this Self Assessment Questionnaire, the merchant is certifying that they process in a secure manner. This is important because if a merchant were to get audited by any of the card brands, they would be able to prove compliance by showing the auditors their certificate. Proving compliance can save the merchant from extensive fines levied by the card brands.

Our program also has an insurance policy, so if they were to suffer a security breach of any kind, the merchant is covered under the insurance policy up to $50,000 in fines. If they were to complete the questionnaire and receive a certificate showing they are compliant, this policy would also cover losses due to fraud for up to $500,000. Some of the expensive fees that the merchant could incur if they have a security breach are:

Paying card brand fines, reimbursing issuing banks for new credit cards, legal fees, audit fees, and customer reimbursements for fraudulent charges.

If a merchant has a certificate from their previous processor – will they still be charged?

PCI Certification is an annual requirement, so when their certificate expires, they will be required to complete another SAQ. CWA will not bill the merchant our fee until their certificate expires and they are required to recertify.

What is a PenTest (Penetration Test)?

A Penetration Test simulates a real-world attack against your information systems to identify vulnerabilities and risks which may impact the confidentiality, integrity or availability of your data. The Payment Card Industry Data Security Standard (PCI DSS) specifies requirements for organizations that store, process or transmit credit card information.

Unlike a vulnerability assessment or automated vulnerability scan, security engineers performing penetration testing manually test your systems to obtain access to sensitive data. This hands-on approach allows the tester to intelligently respond to changing conditions within the environment and discover new vectors of attack. As a result, your organization can understand how malicious entities may be attacking your systems and to what extent they are vulnerable.

There are two types of penetration tests—external and internal.

- An **External Penetration Test** shows you what anonymous attackers on the Internet see when looking at your network.
- An **Internal Penetration Test** shows you the risks your employees, contractors and guests pose to your information systems.

CWA's penetration testing methodology uses industry recognized standards to help ensure that your results are suitable for PCI validation purposes. More importantly, a CWA penetration test identifies vulnerabilities and other weaknesses in your card processing network…internally and externally.