

MerchantResource



Am I at Risk for a Data Compromise?

You ARE at Risk ... But, to What Degree?

Merchants may be protected from security breaches and fraud, due to their business setup, lower transaction volumes, payment system security features, etc. The truth is all merchants are at risk. And the penalties can be detrimental to a thriving business.

Did you know ...

- The majority of payment card compromises occur at traditional street-side merchant locations as opposed to e-commerce Web sites.
- A payment card compromise can result in fines up to \$500,000 per card brand, per incident – with victim notification costs up to \$100,000.
- If compromised, a merchant can be permanently expelled from the payment card networks – preventing them from accepting payment cards.
- A compromised merchant is responsible for the fines, as well as costs associated with the investigation of the compromise.

A compromised merchant faces harsh consequences, because security breaches and payment fraud is not only devastating to the merchant, but also to consumers and the payment card brands. Banding together to enhance protection against payment card compromises, the card brands created the Payment Card Industry Data Security Standard (PCI DSS). Through PCI DSS, substantial penalties are established for non-compliant merchants to reinforce that security breach fines far outweigh the costs of maintaining compliance.

PCI DSS: Designed for Secure Payment Card Transactions

A payment card compromise or security breach involves an unauthorized individual taking advantage of a flaw in a payment system that processes, transmits or stores cardholder data to gain access to such data. PCI DSS serves as a means to protect cardholder data and prevent compromises.

Every merchant that processes, stores or transmits cardholder data, is at risk for payment card compromise. The question is, to what degree are you at risk?

Don't Risk it ... Get Compliant.

To help its merchants achieve PCI DSS compliance, Chase Paymentech partnered with AmbironTrustWave, a compliance management and data security expert, to provide the expertise you need to get compliant. AmbironTrustWave works with thousands of merchants, from mom-and-pop shops to global operations, guiding them through the PCI DSS compliance process.

AmbironTrustWave's TrustKeeper® is an easy-to-use Web portal that helps merchants complete the PCI DSS Self-Assessment Questionnaire, schedule required scans, manage onsite audits and answer the questions they have about their network environment and PCI DSS compliance.

To get started, visit

<http://www.chasepaymentech.trustkeeper.net>

If you have any questions, please contact AmbironTrustWave support at 1-888-878-7817.

Key Questions

Answering the following merchant questions will help you begin to understand the risk level your business faces, in regards to payment card compromise:

- Is a Point of Sale (POS) device, terminal or computer used for face-to-face, card present transactions at your facility?
 - Each of these types of payment acceptance methods presents unique risks to a merchant's environment.
- Is your payment acceptance application on Visa's list of validated payment applications, which have all been approved under Visa's Payment Application Best Practices (PABP)?
 - Choose a service provider listed on either Visa's or MasterCard's list of PCI DSS compliant service providers (Note: Not one of the 170 compromised merchants investigated by AmbironTrustWave used a payment application that listed with Visa's PABP). Check your application's compliance at the following links:
 - Visa: <http://www.visa.com/cisp>
 - MasterCard: <https://sdp.mastercardintl.com>
- If a POS device is used, does it connect to a telephone line, private network (leased line or frame relay) or Ethernet network (i.e., DSL or Cable Modem)?
 - 21 percent of compromises occur through telephone line or dial-up connections
 - 30 percent of compromises occur through T1 or leased-line connections
 - 49 percent of compromises occur through DSL or cable modem connections
- Do you store any cardholder data electronically, whether it is collected face-to-face, via the Internet, or by mail or phone orders?
 - 80 percent of compromised merchants do not protect stored data.

PCI Compliance: A Merchant's Best Protection

A merchant can't afford not to comply with the PCI DSS. PCI DSS is a robust and protects against attack methods used by cyber criminals today. According to a thorough analysis of more than 170 payment card breach investigations conducted by AmbironTrustWave's data security experts, the top ten methods of compromise are:

1. Backdoor/Trojan
2. No Firewall
3. Password Brute Force
4. Remote Access
5. SQL Injection
6. Internal Theft
7. Remote Buffer Overflow
8. FTP Access to Data
9. Remote Exploit
10. Wireless Exploit

Most of these are complex hacking techniques that require an IT security expert to develop a protection plan against; therefore, the card associations require that merchants submit quarterly vulnerability scans conducted by an approved scanning vendor to ensure PCI compliance. Scans prod a network-environment for vulnerabilities that can allow a hacker to utilize one of the methods above to compromise a merchant's network.