SecurityMetrics

Introduction to PCI Compliance

Card Data Compromise

What is a card data compromise?

A card data compromise occurs when payment card information is stolen from a merchant. Some examples of card data theft include:

- Theft of card data from merchant receipt copies or merchant transaction information (i.e. printed batch summaries)
- Internet hacking of card data from computer-based point of sale systems with Internet connections (common with restaurants and hotels)
- Internet hacking of card data from e-commerce websites

Small merchants experience compromise

Many businesses assume data compromise only happens to large companies. While you may have heard about several large-scale merchant compromises in the media, hundreds of small-merchant compromises happen every year that are not made public. The majority of data compromises happen to merchants who process fewer than 1 million transactions annually.

Internet-connected businesses of all sizes face the same threat. Cyber-criminals use similar techniques to hack small and large businesses. To prevent compromise, small Internet-connected merchants must apply the same data security principles used in large-scale corporations.

A recent survey found the following consumer trends that result in the event of a data compromise:

- 55% of breach victims lost serious trust in the company responsible for their data being stolen
- 30% of victims state that they would never purchase products from the company again
- 29% would never maintain any relationship with the organization in the future

Data compromise consequences

Data compromise consequences depend on the status of your PCI DSS compliance at the time of the compromise. The costs for a compromise also vary depending on the size and scope of the incident. Forensic investigation costs vary by the investigator, the size and complexity of the systems being reviewed, the extent of the compromise, and other fees as required by the investigator. Card data compromise costs typically range from $12,000 to over $100,000 per investigation.

If you suspect you've been compromised, inform your merchant processor immediately.

About PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) was created by the major card brands (MasterCard Worldwide, Discover Financial Services, American Express, JCB International, and Visa Inc.) to reduce payment card theft and electronic data loss.

What is the PCI DSS?

The PCI DSS is a list of card-handling practices merchants must follow to accept payment cards. This standard details how to securely handle, process, and store sensitive payment card data.

Who is required to comply with the PCI DSS?

All merchants that accept Visa, MasterCard, Discover, AMEX, or JCB are required to comply with the PCI DSS.

Is PCI compliance mandatory?

Yes. PCI DSS compliance is mandated by the card brands.

What are the penalties for noncompliance?

Failure to comply with the PCI DSS may result in the revocation of the merchant's card processing ability. In the event of a data breach, merchants found to be in violation of the PCI DSS are subject to fines, penalties, and associated costs resulting from the breach. These fees frequently total over $100,000.

Why should I validate my compliance with the PCI DSS?

The best reason to validate your compliance with the PCI DSS is to prevent a credit card breach. PCI compliance not only teaches you how to protect your business from hackers and data thieves, but can also limit your liability in the event of an unavoidable compromise.

How do I validate my compliance?

Validation requirements are based on how you handle and process payment cards and the number of transactions you process annually. Some of your requirements may include:

- Self-Assessment Questionnaire (SAQ)
- Internal vulnerability scanning
- External vulnerability scanning
- Penetration testing
- Security policy implementation

Commonly Neglected Points of Security

SecurityMetrics is a Payment Card Industry Forensic Investigator (PFI) and has conducted hundreds of investigations on breached merchants. The following list contains commonly neglected points of security that result in card data compromise.

Passwords
Change default passwords. Ensure all authorized users have unique credentials

Anti-Virus Software
Regularly update anti-virus software…on all devices

Payment Processing Software
Ensure payment software is PA-DSS compliant and properly configured

Separate payment processing software from all other systems

Payment Card Data
Encrypt, truncate, and/or tokenize payment card data

PCI Compliance
Achieve and maintain PCI DSS compliance

Wireless Security
Secure remote access and wireless network access

Event Logging
Store and review computer event logs for malicious activity

Firewall
Properly configure firewalls

Social
Be cautious, don't provide information to just anyone

Getting Started

To get started with your PCI compliance call SecurityMetrics at 801.705.5665 or click here: www.securitymetrics.com/enroll

About SecurityMetrics

SecurityMetrics is a global leader in merchant data security and compliance for all business sizes and merchant levels, and has helped over 1 million organizations manage PCI DSS compliance and/or secure their network infrastructure, data communication, and other information assets. As an Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Payment Application Qualified Security Assessor (PA-QSA), Point-to-Point Encryption Qualified Security Assessor (P2PE QSA), Penetration Test Analyst, and Payment Card Industry Forensic Investigator (PFI), SecurityMetrics has the tools available to help businesses achieve lasting security and validate accurate PCI compliance.

If you need assistance in your PCI compliance and liability reduction efforts, don't hesitate to call SecurityMetrics at 801.705.5700 or email support@securitymetrics.com.

SecurityMetrics Social Media

To get more educated about all aspects of business security, subscribe to our YouTube channel, follow us on twitter, like us on Facebook, and follow us on Linked In.

www.youtube.com/securitymetricsinc

www.facebook.com/securitymetrics

www.twitter.com/securitymetrics

www.linkedin.com/company/securitymetrics