Introduction: Protecting Cardholder Data with PCI Security Standards

The twentieth century U.S. criminal Willie Sutton was said to rob banks because "that's where the money is." The same motivation in our digital age makes merchants the new target for financial fraud. Occasionally lax security by some merchants enables criminals to easily steal and use personal consumer financial information from payment card transactions and processing systems.

It's a serious problem – more than 10.9 billion records with sensitive information have been breached according to public disclosures between January 2005 and July 2018, according to PrivacyRights.org. As you are a key participant in payment card transactions, it is imperative that you use standard security procedures and technologies to thwart theft of cardholder data.

Merchant-based vulnerabilities may appear almost anywhere in the card-processing ecosystem including:

- point-of-sale devices;
- mobile devices, personal computers or servers;
- wireless hotspots;
- web shopping applications;
- paper-based storage systems;
- the transmission of cardholder data to service providers;
- in remote access connections.

Vulnerabilities may also extend to systems operated by service providers and acquirers, which are the financial institutions that initiate and maintain the relationships with merchants that accept payment cards (see diagram on page 5).

Compliance with the PCI DSS helps to alleviate these vulnerabilities and protect cardholder data.

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

DATA TYPES COMPROMISED IN BREACHES

22% card track data

18% card-not-present (e-commerce)

16% financial/user credentials

Source: 2018 Trustwave Global Security Report, p. 30
https://www2.trustwave.com/GlobalSecurityReport.html
(form to access report)