

## Top 10 Tips to Help Keep Your Data Safe

*Your customers expect you to keep their personal cardholder data safe – not an unreasonable expectation, and merchants must take it seriously. Such protection requires merchants to make an ongoing commitment to human and monetary resources, including new technologies, stronger policies and continuous diligence.*

*\*NOTE: The following list is a selection of suggestions only and not intended to be an exhaustive or comprehensive list of data security tips.*

**b>yond** the transaction<sup>sm</sup>

## ***Ensure your business is PCI DSS compliant***

The Payment Card Industry (PCI) establishes and enforces security requirements for its constituents. Ongoing compliance with the PCI DSS (Data Security Standard) is the critical first step towards a successful data security program.

## ***Review how data is used in your payments system***

Before you can protect it, you must understand the ins and outs of the confidential data in your system:

- › What data you have
- › Where it resides
- › Who is accessing your data
- › When and how users access it

## ***Limit use and storage of sensitive cardholder data within your system***

Use your customers' personal cardholder data only for applications directly pertaining to payments (transaction authentication and daily settlements, for example).

## ***Minimize access to cardholders' data***

Limit access to customer information only to employees whose jobs require it. Do periodic spot checks to ensure procedures are being followed.

## ***Conduct detailed background checks before you hire***

Be selective about whom you hire; employees have the most access to your customers' data and systems. 41% of reported small business fraud in 2007 was committed by employees.<sup>1</sup>

## ***Make any necessary system changes***

You may have to update existing systems and implement new hardware and software, install firewalls, deploy data encryption technologies, implement data access controls and track and monitor access to data and networks.

Consider implementing a layered data security approach such as the combination of encryption and tokenization that will allow you flexibility and a solid defense.

### ***Be on the lookout for signs of skimming***

There has recently been a tremendous rise in card-skimming fraud at the Point-of-Sale (POS). Skilled fraudsters can reconfigure a payment terminal by adding a skimming device in less than one minute. Payment terminals should be routinely inspected to ensure there have been no changes. Signs that your POS may have been compromised include:

- › Changes in the screws or seams of the payment terminals or unexplained scratches
- › A new or fake label or sticker that has been placed to hide a drill hole
- › Serial numbers that do not match between the payment terminal and the sticker

### ***Pay attention to customers' buying behaviors***

Some things to look for include customers who:

- › Purchase a large amount of merchandise without regard to size, style, color or price
- › Don't ask questions on major purchases
- › Try to distract or rush you during the sale
- › Make purchases and leave the store but then return to make additional purchases
- › Make large purchases just after the store has opened or as the store is closing
- › Refuse free delivery for large items

### ***Avoid falling victim to phishing scams***

Never click on links that ask for your personal or account information even if the e-mail message appears to be from your payment processor or financial institution. Always type the service provider's address directly into your Web browser's address bar to access your account. If you believe you have been a victim of a phishing scam, change your online password immediately and contact your service provider.

### ***Don't stop now***

Data security is an ongoing responsibility. Frequently audit your payment acceptance practices and systems. Fraudsters are always looking for vulnerabilities and consistently changing tactics to stay ahead of the curve. You should be, too.

Proactive steps to keep your customers' sensitive data secure is not a luxury. It's a necessity.

<sup>1</sup> National Small Business Administration Survey 2007