WHITE PAPER

# Wall-Mount Rack Solutions for PCI Compliance

## Executive Summary

Credit, debit and ATM card fraud costs consumers, merchants and financial institutions billions in losses every year. The payment card industry has responded by creating the PCI security standard. Merchants that fail to comply with PCI face increased risk of security breaches and substantial contractual penalties. Tripp Lite Wall-Mount Rack Enclosures help merchants achieve PCI compliance by securing network/telecommunications hardware and storage media in retail point-of-sale environments and other locations.

## What is PCI?

Responding to increasing concerns about fraud, the five largest credit card companies—Visa®, MasterCard®, American Express®, Discover® and JCB® (Japan Credit Bureau)—created the Payment Card Industry Data Security Standard, or PCI for short (Figure 1). PCI sets forth requirements designed to ensure that all companies that process, store or transmit customers' credit, debit or ATM card information maintain sufficient security.

*Figure 1: The five largest credit card companies created the Payment Card Industry Data Security Standard, or PCI for short.*

## When and Where Does PCI Apply?

Any merchant that accepts payment cards bearing the logos of Visa, MasterCard, American Express, Discover or JCB as payment for goods or services is required to comply with PCI as part of the contractual obligations of the merchant account agreement. PCI also applies to all other entities that store, process or transmit cardholder data, including processors, issuers and service providers.

PCI has been in effect since 2005, but version 2.0 of the standard has been required since January 1, 2012, when version 1.2.1 expired. The latest version of PCI significantly tightens security requirements for merchants at the point of sale and increases penalties for noncompliance. **Compliance is required 24x7.**

*Credit card fraud is more than just a headline—it costs merchants more than $100 billion per year in the U.S. alone.*

## The Cost of Non-Compliance is Prohibitive

Merchants that fail to comply with PCI face fines that can reach into the millions of dollars, higher payment card transaction fees and the potential loss of credit card processing privileges, which can devastate businesses of any size. Although the costs from contractual penalties can be very high, the ultimate goal of PCI compliance is to make security breaches happen less often and mitigate the damage when they do happen.

Avoiding security breaches may be the biggest incentive for merchants to achieve PCI compliance. The loss of reputation, damage to customer relationships and increased exposure to liability caused by security breaches can be even higher than the contractual penalties:

- Credit card fraud costs merchants more than $100 billion per year in the U.S. alone.[1]
- A 2011 security breach at Sony® exposed the personal information of 77 million customers and may ultimately cost the company more than $1 billion; another breach in 2014 was estimated to cost $100 million. [2, 3]
- A 2012 breach at Zappos® (owned by Amazon®) exposed the credit card and password information of 24 million customers and damaged their hard-won reputation for customer service.[4]
- In 2014, the average cost of a security breach to a small business in the United Kingdom was £65 thousand to £115 thousand, while the average cost to a large company was £600 thousand to £1.15 million.[5]

Big players with deep pockets like Sony and Amazon can survive the damage caused by these security breaches, but smaller merchants may not. The Center for Strategic and International Studies estimates the global cost of cybercrime at $375 to $575 billion, depending on reporting models.[6]

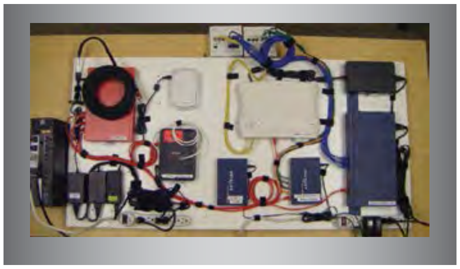

Figure 2: Before Tripp Lite, equipment and media are open to tampering, theft and access by unauthorized personnel, violating PCI requirements.

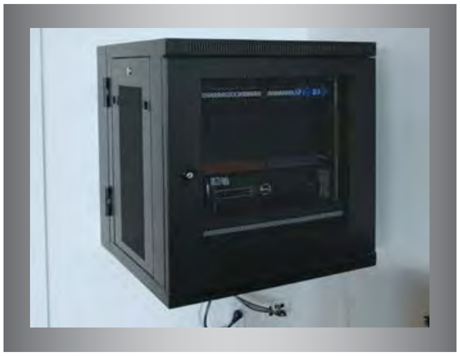

Figure 3: After Tripp Lite, physical access to equipment and media is restricted, complying with PCI requirements.

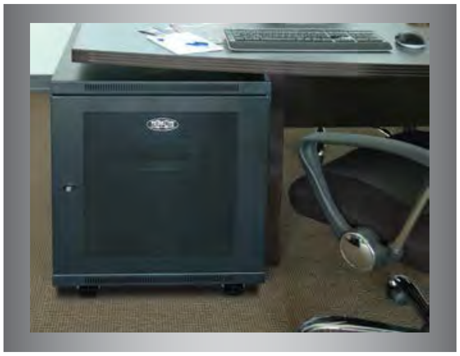

Figure 4: The optional caster kit (SRCASTER) adapts enclosures to roll under desks, tables or counters.

## Achieve PCI Compliance with Tripp Lite

One of the most important steps in the process of achieving PCI compliance is controlling access to equipment that stores or transmits credit card information. IT hardware, telecommunication lines and media that are open to tampering, theft and other unauthorized access (Figure 2) must be physically secured, as noted in this excerpt from the official PCI standard:

> ***PCI DSS Requirements***
>
> - *Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.*
> - *Physically secure all media.*
>
> ***Testing Procedures***
>
> - *Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.*
> - *Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).*[7]

Tripp Lite's SmartRack® Wall-Mount Cabinets provide a convenient, cost-effective way to protect wireless and wired network equipment and media, whether you're retrofitting an existing point-of-sale environment or installing a new one from scratch (Figure 3). They surround all sides of your equipment with sturdy steel frames and panels that prevent unauthorized access and provide ample ventilation for heat-sensitive devices. Locking doors and side panels provide convenient, controlled access during installation and configuration tasks. Cabinets range in size from 5U to 26U and store both rackmount and non-rackmount equipment to accommodate most applications and environments. Cabinets can also roll under desks, tables or counters with the addition of an optional caster kit (Figure 4).

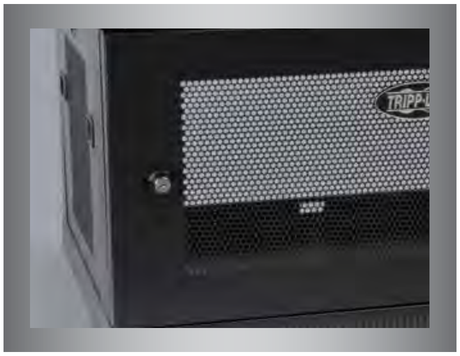

*Figure 5: Locking doors and side panels provide controlled access for authorized personnel.*

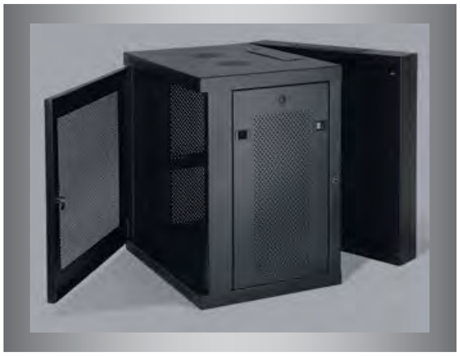

*Figure 6: Models with hinged wall brackets swing away from the wall for easier equipment installation.*

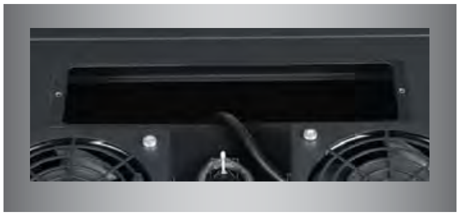

*Figure 7: The top and bottom include convenient ports for power and data cables.*

## Cost-Effective PCI Compliance Solutions

Tripp Lite's Wall-Mount Rack Enclosures are perfect for achieving PCI compliance in point-of-sale environments. Sturdy steel cabinets hold up to 500 pounds (225 kilograms) of limited-access IT equipment, media and other devices securely. They fit in tight spaces, save floor space and accommodate both rackmount and non-rackmount equipment. (See the chart below for a list of models. Visit www.tripplite.com for the full model listing and up-to-date specifications.)

### Highlights

- Sturdy steel panels surround all sides of your equipment to prevent unauthorized access
- Locking doors and side panels provide controlled access for authorized personnel (Figure 5)
- Ample ventilation keeps heat-sensitive devices cool
- Models with hinged wall brackets swing away from the wall for easier equipment installation (Figure 6)
- Convenient ports for power and data cables (Figure 7)
- Pre-assembled for quick installation

**Wall-Mount Rack Enclosures**

| Model | Size | Description |
|---|---|---|
| SRWF5U | 5U | Non-hinged wall bracket, low-profile |
| SRW6U | 6U | Non-hinged wall bracket |
| SRW9U | 9U | Non-hinged wall bracket |
| SRW10US | 10U | Hinged wall bracket |
| SRW12US | 12U | Hinged wall bracket |
| SRW12US33 | 12U | Hinged, extended depth |
| SRW12USG | 12U | Hinged, Plexiglas® door |
| SRW18US | 18U | Hinged wall bracket |
| SRW26US | 26U | Hinged wall bracket |

**Accessories**

| Model | Description |
|---|---|
| SRCASTER | Caster kit (roll cabinets under desks, counters and tables) |
| SRFANWM | Dual 120V roof fans |
| SRFANROOF | Roof-mounted 120V fan panel |
| SRXFANROOF | Roof-mounted 208-240V fan panel |
| SRSWITCH | Magnetic intrusion detection kit |

## Conclusion

If your business accepts credit, debit or ATM cards as payment, you must comply with PCI as part of the obligations outlined in your merchant account agreement. The contractual penalties for noncompliance and other damages caused by security breaches are prohibitively expensive and potentially devastating to any business. Tripp Lite's SmartRack Wall-Mount Enclosures provide convenient, cost-effective solutions that help you achieve PCI compliance.

For more information, including specifications and ordering information, contact your local Tripp Lite representative via e-mail at **international@tripplite.com** or **visit www.tripplite.com/pci**.

## About Tripp Lite

Since 1922, Tripp Lite has established a global reputation for quality manufacturing, superior value and excellent service. Tripp Lite makes more than 3,000 products to power, protect and connect electronic equipment in commercial and retail point-of-sale environments, including UPS systems, replacement batteries, power distribution units, rack systems, cooling solutions, surge suppressors, KVM switches, cables, IP console servers, display solutions, power strips and inverters. Headquartered in Chicago, Tripp Lite has offices worldwide. Learn more at www.tripplite.com.

OVER 90 YEARS Manufacturing Excellence.

[1] Source: *LexisNexis® 2011 True Cost of Fraud Study*.

[2] Source: "As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill," *The Wall Street Journal*, May 9, 2011.

[3] Source: "Cyber attack could cost Sony studio as much as $100 million," Reuters, December 9, 2014.

[4] Source: "Zappos, Amazon Sued Over Customer Data Breach," USA Today, January 18, 2012.

[5] Source: United Kingdom, Department for Business Innovation and Skills, 2014 Information Security Breaches Survey. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307297/bis-14-766-information-security-breaches-survey-2014-executive-summary-revision1.pdf

[6] Source: Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies, June 2014. Retrieved from: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[7] Source: PCI DSS Requirements and Security Assessment Procedures, Version 2.0, Sections 9.1.3 and 9.6.

*Tripp Lite has a policy of continuous improvement. Specifications are subject to change without notice. The information contained in this document is not intended to be legal advice. Consult a qualified professional if you require legal advice.*