

# Here Comes the Payment Card Industry Data Security Standard: Are You Prepared?

Securing customer data in electronic form is vital. Threats and vulnerabilities must be assessed and addressed.

BY SUMIT K. PAL

WITHUMSMITH+BROWN GLOBAL ASSURANCE, LLC

**T**HE PCI SECURITY STANDARDS COUNCIL—founded by Visa International, MasterCard Worldwide, American Express, Discover Financial Services and Japan Credit Bureau—is an open worldwide forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. It assists organizations that process credit and debit card payments by helping to prevent fraud and various other security threats and vulnerabilities.

Clearly, cardholder theft and fraud is a very real problem, costing financial institutions more than \$48 billion and an additional \$6 billion in individual losses. Arguably the most well-known case involved TJX Companies, Inc., the largest international apparel and home fashions off-price department store chain and parent company of retailers T.J. Maxx and Marshalls.

In January 2007, the company announced that it was a victim of an unauthorized computer systems intrusion, resulting in hackers attaining data of the stores' credit card, debit card and check transactions. It was initially determined that 45.7 million customers were affected by this breach, but later reports indicated that the number may be as high as 94 million (according to legal documents). In addition to credit card numbers, intruders also gained access to the social security numbers and driver's license numbers of 451,000 consumers through merchandise return records.

This well-publicized breach proved to be costly for the company. That September, TJX agreed to settle customers' class action lawsuits in the United States and

Canada, which was estimated at \$118 million (including related expenses) with a projected future charge of \$21 million per their second quarter filing. Additionally, the negative attention damaged the company's reputation.

The Payment Card Industry Data Security Standard (PCI DSS) applies to any organization that processes, stores, or transmits a Primary Account Number (PAN) for credit and debit cards, with all channels—retail, money order, phone order, and e-commerce—covered. This incorporates a wide array of institutions and occupations, including: online trading companies; retail outlets; colleges and universities; hospitals; hotels and restaurants; gas stations; banks and insurance companies; Web hosting companies; merchants; service providers; software providers; ATM providers; and managed security providers. These entities are separated by the council into four levels based on their annual volume of processed transactions.

*Level 1*—More than 6 million annual credit card transactions and those that have experienced a data breach. Compliance needs: an annual onsite PCI Data Security assessment and quarterly network scan.

*Level 2*—Between 1 million and 6 million annual credit card transactions. Compliance needs: an annual self-assessment and quarterly network security scan.

*Level 3*—Between 20,000 and 1 million annual credit card transactions. Compliance needs: an annual self-assessment and quarterly network security scan.

*Level 4*—Less than 20,000 credit card transactions. Compliance needs: an annual self-assessment and annual network security scan.

*continued on page 80*

*continued from page 78*

The PCI DSS is a set of 12 specific IT and security needs that have to be fulfilled satisfactorily in order to obtain compliance.

Of particular interest are companies in the Level 4 category. Studies have shown that organizations in Levels 1 and 2 have made good progress. Level 3 organizations are also on the move, but there is a dearth of knowledge about the status of the Level 4 organizations. A considerable number of the organizations that are impacted by this standard fall in Level 4 and they may not have the qualifications or expertise necessary to properly secure cardholder data. Using an outsourcing firm for assistance is an efficient and cost-effective solution.

With an intimate understanding of internal audit programs, risk assessment, anti-fraud programs, vendor management programs, compliance plans, and control culture, outsourcing firms are fully equipped to cope with the extensive PCI DSS requirements.

It is estimated that if companies have a good data security infrastructure, the administration of the annual self-assessment and network scan would be completed in up to 25 business hours each. However, if any gaps or shortcomings are found, the efforts will be appropriately more.


Merely meeting the requirements the first time is insufficient, as merchants and service providers must

sustain continuous compliance as part of the overall operations strategy and framework. This ongoing, annual obligation requires regular attention from the IT department, and it is recommended that an auditor periodically validates the compliance.

Companies that fail to fulfill these requirements are in danger of losing their ability to process credit and debit card payments and will be susceptible to audits and fines of up to \$500,000 if data is lost or stolen. Additionally, should a cardholder take legal action, the resulting bad publicity may ultimately lead to loss of business. According to research, the cost of compliance is only a small fraction of the potential price of non-compliance and the cost of a breach can easily be up to 20 times as much as the cost of compliance.

With credit card use increasing significantly (76 percent of Americans have at least one credit card), losing the ability to process these payments could debilitate a company's sales volume. Additionally, it would be equally devastating if the clientele loses faith in an organization's data security system. ■

*Sumit K. Pal is executive vice president and chief intelligence officer of WithumSmith+Brown Global Assurance, LLC.*



**We're WithumSmith+Brown. We're That Kind Of CPA Firm.**

**Hindsight. Insight. Foresight.** We make it our business to know your business. And to know you. From multimillion dollar publicly-held companies to local privately-held enterprises, our clients have enjoyed our expert advice and exceptional client service for over 30 years.

Audit • Tax • Corporate Governance • SOX Compliance • International Tax • Management Consulting • Litigation Support • Government Services  
Forensic Accounting • Accounting • Bankruptcy • Reorganization Services • Estate and Financial Planning • Succession Planning • Business Valuations  
Health Care and Benefits Consulting • Not-for-Profit Business Advisement • Construction Industry Consulting

**No matter what lies ahead for your business, WithumSmith+Brown will help you go the distance.**  
[www.withum.com](http://www.withum.com) ■ [info@withum.com](mailto:info@withum.com)

New Jersey ■ New York ■ Pennsylvania ■ Maryland ■ Florida ■ Colorado ■ Member of HLB International