

## ***The Payment Card Industry (PCI) Data Security Standard (DSS)***

Accepting credit and debit cards is a fact of life at campuses nationwide. Hand-in-hand with card acceptance comes the responsibility to safeguard and protect all transaction and consumer data. Unfortunately, education institutions because of their open networks and occasionally inadequate security procedures are particularly vulnerable to hacking and other compromises of confidential data: of the 321 information security breaches nationwide reported in 2006, 84 – or 26% – were at education institutions. This 26% share for Education is particularly disproportionate when we consider that education represents only a small percent of total payment activity nationwide. As a result, financial institutions and card issuers increasingly view education institutions as risky merchants.

The Payment Card Industry Data Security Standard (PCI DSS) represents a common set of technical requirements and testing methodologies created to help ensure the safe handling of sensitive information. It was initially created to align the separate security programs of MasterCard and Visa, and later was adopted by other major card programs. In 2006 the PCI Security Standards Council was created to govern the security standards for the payment industry. Founding members of the Council are American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

According to the Council: “The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.” In practical terms, PCI DSS is a set of twelve general requirements grouped into six areas: build and maintain a secure network; protect cardholder data; maintain a vulnerability management program; implement strong access control measures; regularly monitor and test networks; and maintain an information security policy.

There are two things treasury managers at every education institution need to understand about PCI DSS. The first is that the standards are not optional – if you accept payment cards anywhere on your campus, you are subject to the standards. The second thing to understand is that there can be significant financial costs to non-compliance. For example, if your institution suffers a security breach and cardholder information is compromised, there are potential direct costs (e.g., notifying affected cardholders, paying

for credit monitoring, paying for unauthorized charges, implementing needed hardware or software upgrades) and indirect costs (e.g., unfavorable publicity, brand damage to the institution) resulting from a breach. In addition, you may be fined by the card association(s) whose cardholders were affected. It is worth noting that in 2006, Visa alone issued merchant fines totaling \$4.4 million.

The Treasury Institute has a number of resources available on its website to help all education institutions protect their sensitive data and comply with the Data Security Standards. These include:

- ❑ A paper addressing the unique challenges of education institutions face implementing the Standards
- ❑ An implementation checklist to help guide institutions through the process of achieving and maintaining compliance
- ❑ Results from a survey of education institutions analyzing how they are organized and staffed to implement the Standards and maintain compliance across their campuses.
- ❑ Links to the PCI Study Group website (where you can download the Standards) and other industry information sources.

The Treasury Institute sponsored a 2-day workshop in May 2006 to share common experiences, lessons learned, and insights among education institutions. The workshop featured presentations by four universities describing their implementation of the Standards. It also included a panel discussion and Q&A with representatives from American Express, Discover, Visa, Bank of America, and Citibank. The workshop attracted 89 professionals representing 49 education institutions nationwide, and it featured energetic discussion and information sharing among participants.

Recognizing the continuing need to share best practices – the Standards were revised in July of 2006 – the Institute is again sponsoring a workshop May 14, 15, and 16, 2007. May 14 is an optional half-day afternoon session for attendees who may not be completely up to date on PCI-DSS, its rationale and history, and its implementation. The 2-day workshop May 15 and 16 features education institutions and industry experts describing how they implemented PCI DSS, how they are maintaining compliance, how

to protect against hacking and other security breaches, and what challenges are posed by the revisions made to PCI DSS in the past year. You can find additional information on this workshop including on-line registration on Institute's website. Attendance will be limited to allow maximum participation by all attendees. To guarantee your place at the workshop, sign up today!