

Welcome to the newest edition of SafeCommerce, our newsletter to inform and remind you of security-related topics that affect your Campus Commerce initiatives.

Payment Application Data Security Standard (PA-DSS) Overview

PA-DSS compliance has received a lot of press in the past few months, but there is still plenty of confusion on the scope of PA-DSS and how it affects your campus. TouchNet has put together the following FAQ to help clarify PA-DSS issues:

- **What is PA-DSS?**
PA-DSS establishes standards for handling data securely in payment applications. It is aimed at software developers and integrators. The requirements were adapted from Visa's Payment Application Best Practices (PABP) security standard. For more information on the standard, visit the PCI web site at:
https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
- **Who is affected?**
The PCI Security Council requires companies which sell, license, or distribute software that processes, transmits, or stores cardholder data to certify their products as PA-DSS compliant. Schools must verify that all payment applications in use on campus are PA-DSS compliant.
- **Which applications are in scope?**
Any campus business application used to process, transmit, or store cardholder data. This includes applications such as your ERP, parking systems, ticketing software, and more. Also included in the scope are Point of Sale (POS) applications. Custom payment applications are not covered by PA-DSS.
- **Why is it important?**
PA-DSS doesn't make your campus exempt from PCI compliance, but using PA-DSS-certified applications should make compliance easier. Be sure to follow your vendor's PA-DSS Implementation Guide for guidance on configuring your applications in a PCI-compliant manner.
- **What are the timelines?**
There are a series of milestone dates for compliance. All payment applications used on campus must be PA-DSS compliant by July 1, 2010 at the latest. If your campus requests a new merchant ID or makes changes to existing merchant accounts, then compliance must be achieved before these changes are made.

A Special Note for Schools Accepting PIN Debit at the Point of Sale

There are two additional requirements that coincide with the July 1, 2010 deadline that affect those schools processing PIN debit transactions at the point of sale. First, any merchant processing PIN debit payments must be using PCI PED-compliant devices. The list of PED-compliant devices can be found at: https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html?mn=1. Second, those devices must transmit the user's PIN number using Triple DES encryption. This may necessitate having your card-swipe devices injected with the Triple DES encryption keys by a third-party company designated by your processor.



TouchNet will distribute a follow up bulletin to those customers affected by these additional requirements containing more specific instructions.

Red Flag Rule Update

The Federal Trade Commission (FTC) has extended the compliance deadline for the Red Flag Rules to August 1, 2009. The Red Flag Rules require all financial institutions to develop polices and safeguards for detecting and responding to activities that may indicate identity theft. TouchNet released a statement earlier this year explaining its position on Red Flag compliance. As a software service provider, we see our role as providing your institution with tools for tracking suspicious behavior. Upcoming service packs for Bill+Payment and Marketplace will provide a new series of email notifications that are sent to users as changes are made to their TouchNet profiles. Please refer to TouchNet's Red Flag Compliance bulletin on the customer portal for more information.

Update on Securing Payment Card Stations

Our previous edition of SafeCommerce described a series of best practices for securing Payment Card Stations (PCSs), sometimes referred to as cashiering stations. The term "PCS" broadens the scope to include any PC where a person is entering payment card data. In response to customer feedback, TouchNet has developed a new document, "Recommendations for Securing Payment Card Stations," that expands on each of these best practices. This document is a reference guide for securing POS transactions originating from TouchNet Cashiering, TouchNet Payment Gateway, and TouchNet uPay. Regarding uPay, we continue to point out that uPay was designed for online eCommerce transactions and not for in-person (pCommerce) transactions. If used as documented and intended, uPay falls outside the scope of this discussion.

You can find this new documentation online in the client portal. We encourage you to read it and review the implementation of all PCSs on campus, including those not provided by TouchNet. This effort will dovetail well with the PA-DSS mandate discussed on page 1, as PA-DSS covers both eCommerce and pCommerce software and systems.

Please contact TouchNet at securityquestions@touchnet.com with any questions.

TouchNet Information Systems, Inc.
15520 College Blvd.
Lenexa, KS 66219

www.touchnet.com • 800.869.8329