NORTH CAROLINA COMMUNITY COLLEGE SYSTEM

R. Scott Ralls, Ph.D.
President

July 21, 2010

MEMORANDUM

TO: Presidents
Business Officers
System Administrators
Network Administrators

FROM: Dr. Saundra W. Williams, Senior Vice President
Technology and Workforce Development

SUBJECT: Payment Card Industry (PCI) Compliance with Datatel E-Commerce 3.x

Overview

On July 1, 2010 the PCI Security Standards Council adopted a new standard -- the Payment Application Data Security Standard (PA-DSS). PA-DSS directly impacts PCI compliance for colleges using Datatel's E-Commerce 3.x module. The PA-DSS requirement states that after July 1, 2010, in order for merchants (colleges) to remain compliant only validated payment applications can be used to conduct credit card transactions. Currently the PA-DSS standard is applicable to VISA transactions but will be adopted by other card issuers.

Provided your college was PCI compliant prior to PA-DSS, there is no increased risk of a data breech as a result of this new standard.

E-Commerce 3.x falls under the PA-DSS standard because it is a payment application. Due to the requirement for a payment application to be validated to be compliant, E-Commerce 3.x is not PA-DSS compliant. Datatel has communicated to the System Office that they have no intention to seek PA-DSS validation with E-Commerce 3.x. (A copy of Datatel's statement, dated June 15, 2010, regarding E-Commerce 4.x is attached.) Datatel intends to remove the need for E-Commerce to be PA-DSS compliant by changing the way payment transactions are handled with the upcoming version of E-Commerce 4.x. The System Office has verified this information with Datatel. This issue impacts all Datatel customers using E-Commerce 3.x, not just the North Carolina Community Colleges

CC10-029
E-mail

MAILING ADDRESS: 5006 MAIL SERVICE CENTER ~ RALEIGH, NC 27699-5006
Street Address: 200 West Jones ~ Raleigh, NC 27603 ~ 919-807-7100 ~ Fax 919-807-7164
AN EQUAL OPPORTUNITY EMPLOYER

E-Commerce 4.x is tentatively scheduled for release by Datatel in September 2010 and will be released in a two-phase process; however, the Datatel release time frame does not take into account the additional time that will be required for the System Office to merge, test, validate and pilot the E-Commerce 4.x module with the system template prior to general release. The System Office currently anticipates a 2nd Quarter 2011 general release of E-Commerce 4.x to the colleges, provided Datatel does release the software in September 2010.

Risks

Our review revealed two possible ways an acquiring bank may discover that a college is using a non-compliant payment application:

1. *The acquiring bank or merchant account provider, which is the organization handling credit card transactions on behalf of a college, could request a review of a college's PCI Compliance to determine if the payment application software meets the DA-PSS standard.*
   or
2. *During the next Self Assessment Questionnaire (SAQ), each college who is a Level 3 merchant using E-Commerce will be required to identify that they are not PCI compliant under the PA-DSS requirements.*

Level 3 merchants are required to complete an SAQ quarterly. For Level 4 merchants, that requirement is defined by the acquiring bank, and completion of a SAQ is only recommended.

Risks for continued use of a non-compliant payment application include:

1. *Fines levied by the acquiring bank or merchant account provider against any merchant using a non-compliant payment application.*
   and/or
2. *The loss of merchant certification by VISA.*

Possible Mitigation Solutions

At this time, the likelihood of a college experiencing these risks is unclear. Each college should determine what mitigation actions it will take as a result of this change in PCI Compliance. Assuming your college was PCI compliant prior to PA-DSS, possible mitigation solutions include:

1. **Contacting your college's bank or merchant account provider to ask for specific direction on processing credit card transactions and the PA-DSS requirement while using E-Commerce 3.x.**
2. Creating a documented action plan of efforts to achieve PCI compliance, if you are using E-Commerce 3.x. That action plan should reference the anticipated dates of deployment

3. associated with the release of E-Commerce 4.x from Datatel and the System Office. Where applicable, this action plan should be attached to quarterly SAQs.

4. While it may not be feasible, the only way to ensure compliance is to stop accepting credit card payments through E-Commerce 3.x until such a time as E-Commerce 4.x is deployed.

The System Office strongly encourages all colleges to thoroughly review the PA-DSS requirements, the related impact on PCI Compliance and make those changes that best represent their business goals. The System Office will continue to work with Datatel on getting E-Commerce 4.x validated and released as quickly as possible along with providing pertinent information as it becomes available.

If you have any PCI related questions, please contact Stephen Reeves, Director of IT Security at 919.807.7054 or reeves@nccommunitycolleges.edu.

Links

Link to the PCI Security Standards Council
https://www.pcisecuritystandards.org/index.shtml
Link to PA-DSS Information
https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml
Datatel User's Community Forum Thread on Topic (Account Required, See Attachment)
http://corpforum.datatel.com/forums/viewtopic.php?t=19851&highlight=padss
Link to VISA's CISP Bulletin on Payment Application Security Mandates:
http://usa.visa.com/download/merchants/payment_application_security_mandates.pdf
Link to VISA's Merchant Classification
http://usa.visa.com/merchants/risk_management/cisp_merchants.html
Link to VISA's Payment Applications Overview
http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html

SWW/ssr/dcm

Attachment

c: Jennifer Haygood
Bruce Humphrey
Kim Van Metre
Arthur Hohnsbehn
Stephen Reeves

CC10-029
E-mail

Colleague e-Commerce Enhancement Project Update – June 2010

Posted June 15, 2010

Datatel e-Commerce 4.0 is scheduled to be delivered in two phases. The first phase will include all modifications and enhancements related to credit card transaction entry with the exception of those related to encrypted card-swipe capabilities. The first phase is targeted for general delivery in September 2010. The second phase will follow in Q4 2010.

These enhancements are a result of Datatel's evaluation of the Payment Card Industry's data security standards for payment application providers.

The Payment Application – Data Security Standard (PA-DSS) is the Payment Card Industry (PCI) Council-managed program formerly under the supervision of the Visa Inc. program, and previously known as the Payment Application Best Practices (PABP) standard.

The objective of PA-DSS is to help software vendors and others develop secure payment applications and ensure that their payment applications support the PCI-DSS compliance of their merchants. Payment applications that are sold, distributed, or licensed to third parties are subject to PA-DSS requirements. In-house payment applications developed by merchants or service providers that are not sold to a third party are not subject to PA-DSS requirements, but they must still be secured in accordance with PCI-DSS.

As currently designed, Datatel Colleague e-Commerce 3.x is, by definition, a payment application. Datatel evaluated two options: to become compliant with PA-DSS or to modify the solution so that it was no longer a payment application. After extensive analysis the decision was made to modify Colleague e-Commerce in such a manner that it would no longer be a payment application.

With the modifications Datatel is making there will be no entry, storage, or transmission of sensitive credit card information within the Colleague/WebAdvisor solution. Instead, during the processing of an e-Commerce payment, Datatel will pass control of the processing to our PCI compliant partner sites for the entry and validation of credit card information. Once the transaction is complete, control will then be passed back to the appropriate Colleague and/or WebAdvisor process, where only non-sensitive data will be stored.

This methodology will be implemented in both Colleague and WebAdvisor interfaces for Colleague Student, Colleague AR/CR, Colleague Advancement, and Datatel Recruiter in all places where credit card payments are accepted. Please note that there will be no change to the processing of electronic checks (e-Checks) which are also a part of e-Commerce.

This project enables Datatel Colleague e-Commerce users to be PCI-DSS compliant with respect to this solution. Maintaining compliance with PCI-DSS is an institution-wide responsibility that covers a wide range of security issues for which the merchants are responsible. The use of PA-DSS compliant software does not, in and of itself, translate into PCI-DSS compliance. These Colleague modifications are a component of your intuition's overall plan to ensure your compliance with PCI's data security standards.

As part of this project, modifications will be made to the following Colleague and WebAdvisor payment entry forms

and related processing:

Staff Entry forms

- Application fee entry
- Cash receipt entry
- Batch cash receipt entry
- Gift entry
- Auto-Pay Pledge entry
- Pledge Payment entry
- Planned Gift entry
- Matching Gift entry
- Recurring Donation entry

- Automatic Payment Processing
- Membership Dues entry

Self-service transactions (WebAdvisor)

- Make a Gift
- Make a Pledge Payment
- Make a Payment
- Payment Plan Payment entry
- Transcript Request payments
- Graduate Application Fee payments
- Enrollment Verification Request payments
- Instant Enrollment

Datatel Recruiter

- Application Fee payment

ActiveAdmissions, ActiveApply, and ActiveAlumni will not utilize the new e-Commerce gateway. For clients who are concerned about the new PCI requirements, Datatel has developed services that push all payment processing to an external payment provider. After the service is complete, ActiveAdmissions, ActiveApply, and ActiveAlumni will no longer be considered payment applications.
The following environmental requirements have been identified:

- UI 4.1 (recommended but not required)
- WebAdvisor 3.1.6

The project will include the following components:

- InstallShield for the Payment Gateway
- InstallShield for WebAdvisor 3.1.6
- UT Install for WebAdvisor 3.1.6
- DMI Install for e-Commerce
- CORE Software Update for the Payment Gateway and e-Commerce
- ST Software Update for changes to Cash Receipting and WebAdvisor payments
- CA Software Update for changes to Contribution Processing

PayPal and Official Payments Corp. are making complementary modifications to their gateway solutions leveraged by Datatel's e-Commerce solutions. Datatel is working in lockstep with these partners to meet the targeted delivery dates.

As we move through 2010 Datatel will continue to work closely with our partners in the identification and testing of encrypted card readers that will be key to managing the transmission of sensitive data. Recommendations will be announced in Q4 2010.

If you have any questions, please contact Moira Kirkland, Datatel Senior Product Manager, at msk@datatel.com.