Payment Cards Processing at UNL

Volume 17, Issue 3 April, 2022

University of Nebraska —Lincoln
PCI Compliance Team

PCI Compliance Paperwork Due May 20th

The first step in compliance is to collect each merchant account's compliance paperwork. The same documentation as in past years will be required: **Merchant Profile and Procedures Document, including a Cardholder Data (CHD) flowchart**. Merchants will also need to do the SAQ coming soon (see page 2). PCI DSS v3.2.1 is the current PCI version and a wealth of information can be found on the PCI DSS website: https://www.pcisecuritystandards.org/document_library

How do you get started? For each merchant number, you need to review, update and submit:

- **Merchant Profile** – forms available here: http://pci.unl.edu/merchant-profile
- **Procedures Document (including a current CHD flowchart)** – narrative (no standard form)

  REMINDER: Do not combine merchant accounts on these documents. We need a completed profile and procedures document for each merchant account.

Create a PCI 2022 folder for retaining your documents. Access last year's PCI files. Review your 2021 paperwork, update the information as needed to accurately reflect this year's processes, and save a copy for this year's documentation. New merchants will need to create all documentation. The procedures document is a narrative of your processes and should incorporate the following:

- make, model, serial number and location of all equipment*****
- details of all payment channels
- storage/purge details of cardholder data (if appl.)
- demonstration of segregation of duties in place
- flowchart of cardholder data
- individuals involved in payment processing
- staff training requirements
- information on reconciliation process
- signature of department head

*****Many departments have purchased new terminals recently. Be sure your PCI documentation is updated to reflect your new equipment and processes. The new stand-alone terminals are purchased with Elavon's Safe-T to encrypt the data and allow for processing via Ethernet.

There have been many changes on campus this year. Any equipment or procedural changes need to be reflected in your documentation.

Each merchant must have a detailed description of the processes in place for their card activity. These procedures are not only necessary for us to gain an understanding of your CHD environment but are needed so you, in the department, have an understanding of the process and ensure all necessary safeguards are in place for safe cash handling and security. They are also essential to meet PCI documentation requirements.

Please submit your updated documentation by Friday, May 20th to: bursar@unl.edu

payments insider

Migration to Payments Insider from Merchant Connect

Recently some users have been testing Elavon's upgraded payments portal, Payments Insider. The same data you're used to seeing in MerchantConnect is available in Payments Insider with better design, performance, functionality and security. The migration process will begin soon as Elavon is retiring MerchantConnect as of May 10th. Current MerchantConnect users will receive an email with instructions and training in the next couple of weeks. This would be a good time to setup any new employees that need access to payment information.

Please email Lisa Hilzer at lhilzer3@unl.edu with questions or to setup new users with Payments Insider access.

University of Nebraska —Lincoln
PCI Compliance Team

Information Technology Services (ITS)
Chris Cashmere ccashmere@nebraska.edu

Office of the Bursar
Lisa Hilzer lhilzer3@unl.edu
Jennifer Hellwege jhellwege2@unl.edu

The PCI Compliance Team is a collaboration between Information Technology Services (ITS) and the Office of the Bursar. It is a cross-functional team responsible for administering the University of Nebraska-Lincoln payment card policies and procedures, monitoring payment card activity, and educating merchants.

COMING SOON: PCI Compliance Self Assessment Questionnaires (SAQs)

The next step in compliance is the **Self Assessment Questionnaires (SAQs)**. Each merchant account must submit an SAQ to Elavon. Elavon utilizes PCI Compliance Manger for this process. It is a tool which allows online submission of our SAQs. Similar to last year, we expect to accumulate the information for the SAQs for those departments using only stand-alone terminals. The PCI Team will then submit the information electronically for the group rather than each merchant account having to do the compliance separately. For departments with other setups (i.e. online, POS), we will schedule meetings with our PCI Team to assist with the SAQ(s) you must complete. We expect these meetings to primarily take place in June. They will be conducted through Zoom.

ATTN NEW MERCHANTS: If your merchant account is new this year, you may have done a mid-year attestation. We will still ask you to do one at this time to bring your compliance in line with the rest of the University's compliance dates.

We will continue with the goal of completing our compliance efforts by June 30th of each year. This is consistent with efforts on the other campuses as well.

Password Protect Terminal Processing of Returns and Voids

Elavon has the ability to enable a password feature on your terminal when a return or void needs to be processed. When enabled, anytime a user attempts a refund or void, they will have to enter the password in order to complete the transaction. This could be helpful to departments for authorization of these transactions or for eliminating accidental returns due to the wrong button being pushed on the terminal.

Please send an email to Lisa Hilzer at lhilzer3@unl.edu if you're interested in enabling the password feature on your terminal.

Google Voice NOT an Option for Collecting Credit Card Data

Google Voice or a "softphone" should not be used for taking credit card information from customers. Google Voice or other software phones that work through your workstation or desktop do not meet PCI compliance standards. The University's Cisco VoIP phone can be used for taking credit card information. The VoIP system is encrypted, securely managed, has a firewall, and is properly segmented.

As a reminder - credit card information cannot be recorded in any way. A phone line which records calls should not be used in accepting credit cards.