Payment Cards Processing at UNL

VOLUME 17, ISSUE 2 FEBRUARY, 2022

University of Nebraska —Lincoln
PCI Compliance Team

Suspicious Processing Activity on Payment Sites

UNL merchant websites continue to be the victims of fraudulent card testing attacks. A review of a recent attack of transactions processed on one merchant's account, showed there were **over 13,000 authorization testing attempts** in just a few hours.

Authorization testing is a fraudulent activity using the merchant's website to test credit card numbers to see if the numbers are valid. In most cases this is done by using a bot or program that generates random card numbers all while rapidly attempting purchases for a small amount with each unique card number. In other rarer cases, the hacker has compromised the merchant's terminal identification information.

To mitigate this attack, merchants should enable all fraud prevention rules and filters available for their payment sites and processing. Basically, do whatever is possible and practical to slow down or prevent multiple transactions from happening rapidly. It is recommended to add or enable the following:

- Captchas
- Additional Authentication
- Velocity Filters (ex. limit # of daily transactions and # of transactions from the same IP address)

Mitigating these attacks are important as the card brands can assess fines and extra fees for continued authorization testing. Also, payment processors can charge 5-10 cents per declined or failed transaction, which can up to THOUSANDS OF DOLLARS if not prevented or identified and resolved quickly.

If you do not have access to fraud settings, please contact your website provider, payment gateway and/or payment processor to see what they have done or what can be enabled on your behalf to mitigate these card testing attacks.

Lastly, make sure fraud notifications from payment processors or service providers go to an active and monitored email address to quickly identify an attack.

For assistance with reviewing your site security, fraud filters, or any other security questions or issues, please contact ITS Security at security@nebraska.edu.

Please notify the PCI Compliance Team if you think an attack has taken place.

Cvent - University of Nebraska Event Registration

cvent

Are you looking for a way to register event or conference attendees efficiently?

Cvent, also known as the University of Nebraska Event Registration merchant, may be a great option for your next event. Cvent is a robust registration management system available to the entire University community. Using Cvent can save your department time because registration payment transactions are run securely through this one system, which means the accounting and compliance are taken care of for you. Cvent, managed by the AEM Business Center and Nebraska Extension, is a customizable solution for in-person, virtual, or hybrid events.

Contact Mike Bergland-Riese at riese@unl.edu for more information.

University of Nebraska —Lincoln
PCI Compliance Team

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

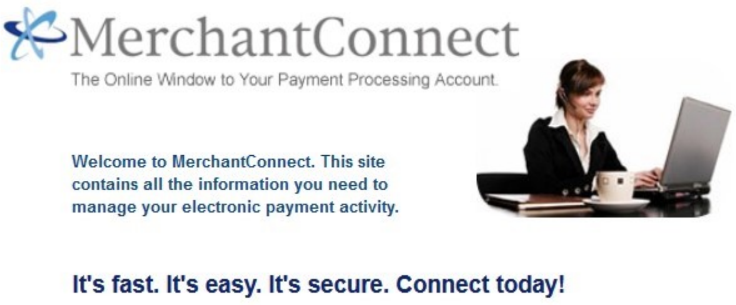
Office of the Bursar
Lisa Hilzer lhilzer3@unl.edu
Jennifer Hellwege jhellwege2@unl.edu

UNIVERSITY OF Nebraska Lincoln

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.

MerchantConnect and Reconciling Your Card Activity

As part of our contract with Elavon, we have access to their online system **MerchantConnect**.



MerchantConnect

The Online Window to Your Payment Processing Account.

Welcome to MerchantConnect. This site contains all the information you need to manage your electronic payment activity.

It's fast. It's easy. It's secure. Connect today!

MerchantConnect allows users to easily view recent batches, access monthly statements, view transaction details, access important information about payment processing support, and much more. MerchantConnect also allows users to filter and search for specific information or export date for further analysis.

Each department needs at least one individual with access. Most merchants already have someone setup, but please email Lisa Hilzer at lhilzer3@unl.edu if you need a new user setup.

MerchantConnect Login Website: https://www.merchantconnect.com

Note: When logging in on the website, if you receive a security message asking for Merchant ID and Business Checking Account Number, that means your User ID has been deactivated due to non-use or failed password attempts. Please email Lisa Hilzer with your User ID in the email, so it can be reactivated.

Reconciliation of card activity must be done regularly and at least monthly for every merchant account. The monthly sales and fees allocation and merchant statement should be included in this reconciliation. The Bursar's Office emails the sales and fees spreadsheets each month after completing the allocation. It is based on the sales activity reported by the department and the monthly merchant statement. It shows how the amount allocated was calculated and if there is any carry forward to the next month.

What to do each month:

- Review your MerchantConnect daily activity against the figures in your register or sales system.
- Confirm the amount on your SAP ledger is correct and ties to the Bursar's allocation spreadsheets and also your departmental sales figures.
- Download your monthly merchant statement in MerchantConnect. Review it for accuracy and completeness. Call the Bursar's Office if you have trouble viewing or understanding the MerchantConnect content.