Payment Cards Processing at UNL

VOLUME 6, ISSUE 4 NOVEMBER, 2012

University of Nebraska —Lincoln
Bursar's Office

Chargeback Activity on the Rise at UNL

We have seen an increase in chargeback activity recently. Reviewing your credit card processes can assist you in minimizing the time and money spent on chargeback situations. At a minimum:

- Be Responsive –Respond to all customer inquiries promptly. This will increase customer satisfaction and prevent frustrations which escalate into a chargeback situation.
- Provide Return/Refund Policy –Clearly state your return/refund policy so customers are not surprised later.
- Provide Contact Information –Make sure your customer knows how to reach you and can easily get in contact with you regarding any problems they might have. Provide an email address and phone number on your receipt and website.
- Require Card Expiration Date –Verifies validity of card.

Some further items to consider in order to minimize chargeback situations are:

- Use Address Verification Service (AVS) –Checks against the cardholder's billing address to test authenticity of the cardholder.
- Require the Card Verification Value (CVV2) –Another means to check the cardholder's authenticity. This should **not** be utilized when customers are mailing in payment information or you are in any way writing down/storing the value. Per PCI DSS, the CVV2 cannot be stored. It may be used for online processing, or phone and in-person transactions where the operator is directly entering the CVV2 into a terminal. The CVV2 is also known as the Card Validation Code or Value or Card Security Code depending on the type of card being used.
- Establish Velocity Limits and Controls –Limit the number or dollar amount of transactions by a cardholder throughout the day.

Welcome to our new merchants:

Veterinary Diagnostic Center

and

Agronomy & Horticulture

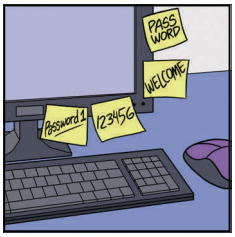
Awareness Training Available

Trustwave, a PCI Qualified Security Assessor (QSA), has awareness training available online called "Takes One to Know One" or TOTKO. It's available at:

http://totko.net/ #totko

The site has three links which are useful in educating any individual about cybercrime and how to defend against it. They appear on the right-hand side of the web page: 1) Infographic "Uneducated Employees . . .", 2) WhitePaper "TAKES ONE TO KNOW ONE: Think Like a Hacker . . .", and 3) Free Practice Class: "Become a Human Firewall".

Here are just a few of the



University of Nebraska —Lincoln
Bursar's Office

121 Canfield Administration Bldg
Lincoln, NE 68588-0412

Phone: 402-472-1734
Fax: 402-472-2959
E-mail: bursar@unlnotes.unl.edu

The Office of the Bursar is responsible for administering the University of Nebraska-Lincoln money handling policies and procedures. Don't ever hesitate to contact us with any receipting questions you may have.

Point-of-Sale Terminal Tampering in News Again

With the recent Barnes & Noble breach, the tampering of point-of-sale terminals is again a topic of conversation. The following safeguards are some of VISA's suggestions to prevent such an event:

POS Equipment Protection

- Continually track and monitor all POS terminals that accept Visa cards.
- At a minimum, routinely inspect your POS terminals.
    - Is the POS terminal in its designated location?
    - Is the POS terminal's manufacturer name and/or model number correct?
    - Is the POS terminal's serial number correct?
    - Is the number of POS terminals in use the same as the number of devices installed?
    - Is the color and condition of the POS terminal as expected with no additional marks or scratches, especially around the seams or terminal window display?
    - Are the manufacturer's security seals and labels present with no signs of peeling or tampering?
    - Is the number of connections to the POS terminal as expected, with the same type and color of cables, and with no loose wires or broken connectors?

Physical Security

- Whenever possible, secure POS equipment to prevent any unauthorized removal attempts from your merchant location.
- Carefully check your POS environment for hidden cameras or recording devices.
- Use a CCTV recording system to deter criminals from removing or tampering with POS equipment.

Staff Communication and Education

- As part of card acceptance training, make sure your staff is up to speed on how to recognize noticeable signs of equipment tampering.
- Control POS terminal access by service support representatives.

For the full article by VISA go to "Point-of-Sale Terminal Tampering is a Crime . . . And You Can Stop It" under Data Security Alerts : http://usa.visa.com/merchants/risk_management/cisp_alerts.html#anchor_2