Payment Cards Processing at UNL

VOLUME 2, ISSUE 4 NOVEMBER, 2008

University of Nebraska —Lincoln
Bursar's Office

Card-Not-Present Transactions

As we become involved in the busy holiday shopping season, it seems an opportune time to remind ourselves of some precautionary measures we can take to prevent fraud when processing Card-not-present (CNP) transactions.

You know your customers best so, trust your instincts if you suspect anything unusual or possibly illegal. If you do, call your voice authorization center and say, "I have a Code 10 Authorization request." And then follow the operator's instructions.

Per VISA, here are some basic procedures and warning signs.

Verify the card's legitimacy:

Ask for and record the card expiration date. Use it when you obtain your authorization.

Ask for the Card Verification Value (CVV2) code from the back of the card (3 digit number). Use it when you obtain your authorization.

Ask for the zip code of the billing address and use it when you obtain your authorization.

If you still suspect fraud:

Ask for additional information like the name of the issuing bank and verify that with the authorization center – they can tell by the numbers.

Confirm the order separately by sending a note to the customer's billing address rather than the "Ship to" address.

12 Potential Signs of CNP Fraud

1. **First time shopper**: Criminals are always looking for new victims.
2. **Larger-than-normal orders**: Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchase.
3. **Orders that include several of the same item**: Having multiples of the same item increases a criminal's profits.
4. **Orders made up of "big ticket" items**: These items have maximum resale value and therefore maximum profit potential.
5. **"Rush" or "overnight" shipping**: Crooks want

(continued on page 2)

Welcome to our

newest merchant!

UNL Digital

Imaging

(University

Communications)

Have a safe and

Happy Holiday!

PCI Data Security Standard Version 1.2 Issued

In October, the Payment Card Industry (PCI) Security Standards Council released the PCI Data Security Standard (PCI DSS) Version 1.2. The sunset date of the PCI DSS Version 1.1 is December 31, 2008.

This new standard can be found on the PCI Security Standards Council's website at:

https://www.pcisecuritystandards.org/

Along with the new standard, you can also find the following on the site:

- Glossary
- FAQ's
- Summary of Changes
- Quick Reference Guide

All of these documents are helpful in understanding the standards and what has changed.

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.

Card-Not-Present Transactions (continued from page 1)

these fraudulently obtained items as soon as possible for the quickest possible resale, and aren't concerned about the extra delivery charges.

6. **Shipping to an international address**: A significant number of fraudulent transactions are shipped to a fraudulent cardholder outside the US.
7. **Transactions with similar account numbers:** Particularly useful if the account numbers used have been generated using software available on the internet.
8. **Shipping to a single address, but transactions placed on multiple cards:** Could involve a batch of stolen cards or internet software generating card numbers.
9. **Multiple transactions on one card over a very short period of time:** Trying to "run a card."
10. **Multiple transactions on one card or a similar card with a single billing:** Organized activity rather than one individual.
11. **In online transactions, multiple cards used from one IP Address.**
12. **Orders from Internet addresses that make use of free e-mail services**: These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.

PayPal Emails ??

Ever wonder if that email from PayPal is legitimate? I know we have in our office. So, we've taken a further look at PayPal's web site looking for more information. Take a look at this page:

https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/general/RecognizePhishing-outside

There is some great information on what to look for. I'd also recommend reviewing Parts 1 and 3 of the "Pfishing Guide".

First InfoCenter Update

It was quickly determined that the First InfoCenter product discussed in the last newsletter did not provide the information that some departments were looking for from their online data. The timeliness of the data was the main issue and the format was quite different as well. Because of this discovery, we have not pursued this new product as first thought. We will continue to maintain the FNMS Online for now and fortunately, FNMS has not yet starting charging all of our merchant numbers across the board for the service. That will surely be coming, though. First InfoCenter does provide some valuable information, and we will look into how to better utilize it's features.