

October 2007

In this issue:

*Visa Fraud
Investigations*

*Way Systems
Trainings Moved to
Colorado*

*PC software
Application Versions*

*Certified Software
Quiz*

FYI's

Fall Conference

Fall Conference being held at the Hyatt Grand Champions Resort and Spa in Indian Wells, California on October 14-17, 2007.



**For comments
or suggestions
contact**

jwarren@transfirst.com
or
smiska@transfirst.com

TransFirst, LLC
371 Centennial Parkway
Louisville, CO 80027

Client Relations
800-745-2659 Phone
303-417-8698 Fax

TRANSFIRST In Focus Insightful. Innovative. In depth.

Visa Fraud Investigations



Overview

Fraud investigation was recently covered on the August 30 ABC call. For more details please see the e-mailed presentation files on September 24th. Organized crime is run just like a legitimate business and is aimed at data compromise.

Strategy

Basic security strategy used by Visa to fight fraud:

- Secure the Payment Environment
- Monitor, Identify, and Prevent Fraud
- Manage the Impact of Fraud
- Maintain Trust in Visa Payments
- Create an environment of Partnership

Visa manages fraud by actively investigating hacking incidents. They work with federal and local law enforcement, and gather "carder" intelligence from various sources including chat rooms. They share intelligence across all Visa regions, publish vulnerabilities to all members and all merchants. They communicate best practices on specific fraud issues to members, and distribute at-risk accounts via the Compromised Account Management System.

Current fraud landscape includes:

- ⇒ Skimming
- ⇒ Account take over
- ⇒ ID theft

- ⇒ Phishing
- ⇒ Date Compromise
- ⇒ Lost data, i.e., laptops, tapes, etc.
- ⇒ Prepaid fraud

Data compromises have evolved from E-commerce, to retail, to processors, to PIN's.

Trends

Compromise activity is on the increase. Visa had been seeing about 12 compromises per month, but since January 2007, this has risen to 16 incidents per month. 76% of accounts exposed are brick and mortar businesses. Food services, universities, and clothing businesses are the top three retailer types that account for compromises. 69% of the number of accounts exposed are clothing stores. Large retailers and agents present the largest exposure.

Global threat:

Cyber criminals are globally connected and work with other criminal groups. Global attacks are now originating from "safe" countries. Global criminals may be untouchable and are difficult to pursue with their high level of attack technology.

What the criminals are after:

Theft of card data including account numbers, track data, CVV2, and PIN blocks.

For more information:

Go to cardholder Security Program website
www.visa.com/cisp

Way Systems Training Moved to Colorado

WAY Systems trainings have been moved in-house to the Colorado Training department!

On August 9th, our Training department started performing WAY Systems trainings in-house.

Moving the trainings in-house will improve the level of customer service and set up times by eliminating the need to refer the merchant to another office. Our Training department will follow their normal procedures and attempt to contact the merchant three times. If a merchant calls in to our Merchant Support Desk after these attempts for training, they will be warm-transferred to our Training Dept. We will no longer refer merchants directly to WAY for training.

All technical support will remain at WAY Systems. We have been working with WAY to improve the current procedures on their help desk in order to assure our merchants are receiving the best service. The supported WAY Systems terminals are the MTT 1500 and the MTT 1510. The MTT 1510 is the model of terminal currently being deployed by POS Portal.

See memo dated August 23, 2007 or contact your Account Manager if you have any questions



PC Application Versions



The version number will be required for all new applications and coding requests/changes for third party software products. Third party software products are any product that is not sold or recommended by TransFirst. Some examples include: Micros, IC Verify, etc. Any application or coding request/change to third party software that does not include a version number will be pended until a version number has been provided.

An increasing number of breaches have occurred at merchant locations where non-compliant software versions are in place. Visa and MasterCard require processors as part of their PCI Compliance strategy to target both new and existing merchants to ensure the software belonging to a merchant is PCI Compliant. PCI compliance is an important part of processing credit card transactions on a PC or over the Internet. It is increasingly important that software solutions utilized by TransFirst merchants meet the PCI requirements which are set forth by Visa and MasterCard.

TransFirst boards a multitude of software types that our merchants would like to utilize for their

processing. In order to separate compliant software from non-compliant software, it is now required that software versions are supplied with all new software researches.

When requesting a PC software research, please obtain the following information and e-mail to your account manager.

1. Vendor Business name—required
2. Vendor phone number—required
3. Merchant DBA name—required
4. Product name—required
5. Product Version number—required
6. Vendor contact name—optional
7. Vendor web site—optional

See memo dated September 21st from your account managers for more details and list of common third party software vendors and version numbers that we know are compliant and some that we know are not. This list changes frequently so check with your account manager when setting up merchants with third party software.

Version numbers are also required on software products sold or recommended by TransFirst such as PC Charge and POS Partner.



Certified Software Quiz

Questions:

1. What is level II? What additional prompts will the merchant have to enter for level II transactions?
2. Barb's Righteous Bikes has an Omni 3730 LE, they have customers that come into the store to purchase the bikes, but they also get orders over the phone. What prompts do you need to make sure to turn on for this merchant? What additional information will be required for their over the phone transactions?
3. What is level III? What types of merchants would need level III?



Answers:

1. Level II refers to purchasing cards which require more information than consumer cards. Level II purchasing card data includes the same information captured at level I, plus the following: sales tax amount and customers accounting code.
2. Turn on AVS and invoice #. They will need to enter invoice #, street address and zip code.
3. Level III purchasing card data includes the same information contained at levels I and II plus the following: quantities, product codes, product descriptions, ship to zip, freight amount, duty amount, order/ticket number, unit of measure, extended item amount, discount indicator, discount amount, net/gross indicator, tax rate applied, debit or credit indicator, and alternate tax identifier. Government entities or merchants accepting cards from a government agency are merchants that could benefit from Level III data capture.

For help, see Certified Software list included with emailed newsletter.

FYI's and Reminders

- **Pending applications:** Applications can be pended for missing or illegible information. Examples of commonly missed items include: PCI fee, discount and transaction fees, set up options page, social security number, tax ID number, length in business, a complete business description of what the merchant does, ACH DDA and Routing numbers. Applications also come in illegible. One way to avoid this problem is to get signed up for our online application.
- **Discover cards:** Discover charges a \$0.50 fee on all key entered transactions that are processed without the CVV code. If the transaction does include the CVV code, they are not charged for this fee.
- **Meta Demos:** Demos for Meta have been changed to only be available on Thursdays at 2:00 p.m. Central time. Contact your account manager for more details.
- **POS Partner reminder:** Merchants using older versions need to be upgraded to the POS Partner 6.2, the latest version which is fully PCI compliant.
- **TenderCard demo login information has changed:** new address is: <https://myaccount.imatts.com/index.aspx>. The login is demo and password is demo.
- **Transaction Central Set-up form:** The TC set-up form has been changed. The changes made are: Renamed WebConnect to Pocket Verifier and the training section will show Merchant Support and Agent as options. Contact your account manager if you don't have the new copy.