

# MERCHANT PROCESSING NEWS



## PURPOSE OF THIS NEWSLETTER

It is my desire to both educate and assist business owners on the subject of “merchant services”.

This month’s newsletter covers some industry changes and how they affect your way of doing business on a daily basis. I have also added a Visa USA Data Security Alert dated November 19, 2007 for your perusal.

## STATE LEGISLATION CHANGES



Over the past several years there have been rule changes within Visa and MasterCard (V / MC) that have had a major affect on how bankcard processors view the approval of accounts along with how they decide the policies and procedures for the risk issues of accounts. For example, V / MC have added a lot of different interchange rate categories, policies and procedures, etc. (Please refer to August 2006, June 2007 and July 2007 Newsletters along with

January 2008

### What’s Inside:

- Purpose of this newsletter
- State legislation changes
- What does this mean to my business.
- Ignorance is not bliss
- Where do I find this information
- POS Vulnerabilities

the Updates section on our website). As the world creates and adapts newer and updated technologies, V / MC continue to add security requirements and updates to the credit card processing vehicles such as in equipment (hardwired and wireless) along with internet protocols for gateway transactions. (To review gateways refer to the March 2007 Newsletter).

These changes also factor into how equipment manufacturers design the functionality of equipment and the software technologies that incorporate the changes mandated by V / MC.

State Legislatures also play a part in how the rules and regulations of V / MC affect each and every merchant in their respective States. The State where you sell your product or service predisposes how transactions are ran, what transaction information is available to you, your customers, etc. As an example of a regulation change, due to rise in Identity Theft it was mandated by V / MC that all customer receipts depict a truncated account number - - only the last 4 or 5 numbers of the account number can be viewed. (September 2007 Newsletter). The fines for non-compliance are stiff.

Over the past 12 months a majority of State Attorney Generals (AG) have started an unprecedented and aggressive attack on individuals who commit criminal acts in regards to credit card fraud. In over 35 states there is a bill put forth to be voted on or a law already passed in reference to not having the full account number on the merchant copy of

the credit card receipt. This has forced bankcard processors to know which states allow and / or disallow full account numbers.

## IGNORANCE IS NOT BLISS



I have stated in previous Newsletters and cannot stress enough how important it is to work with a “trained and knowledgeable” merchant services representative. You, as a business owner, need to be aware of the qualifications of the merchant services representative that is going to handle all your merchant services needs.

Remember, you are placing one of your most valued assets in the hands of the representative, the financial future of your business. Please be very careful who you choose. In our May 2007 Newsletter I cover the topics: Duties of Sales Representative, Duties of Business Owner, Documentation, Use Common Sense and Do Some Research. I highly recommend that you review the May 2007 Newsletter.

## WHAT DOES THIS MEAN TO MY BUSINESS



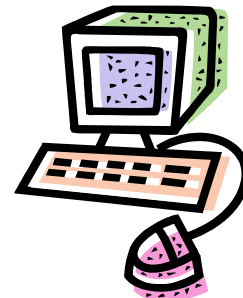
It is very important that you know what rules and regulations apply to your day to day business and the merchant services you utilize, as well as the different State regulations that govern how you must conduct business. For example, an event coordinator from a very large company in Florida contacted me in regards to rumors she'd heard pertaining to various state laws and the truncated account

number issue on the merchant copy of the receipt. This company systematically sends out groups of individuals to various cities all over the US in support of all facets of the events -- set up, presentations and handling the financial transactions. Her concern was how this requirement would affect how they do business.

I explained to her that it doesn't matter what State your business resides in but *where the transaction occurs that is the key*. If this “Florida Company” creates sales in Washington State, for example, the company must abide by Washington State's regulation by which neither copy of the credit card transaction can contain the full credit card account number. It doesn't matter if you are a retailer, a tradeshow business, etc. Knowledge will keep you out of hot water! Each state has its own disciplinary actions ranging from small, large or daily fines for each occurrence up to and possibly including prosecution for a felony offense depending on the legislative procedures.

After our discussion she contacted her current merchant service representative to inquire which states have laws about these issues. That individual's lack of knowledge was his loss and our gain. Now we have a new client to work with and help educate.

## WHERE DO I FIND THIS INFORMATION



My suggestion is to go to that particular State's website. Start with researching business rules and regulations; each website is different. You may want to just pick up the phone and ask if there are any State laws pertaining to this subject matter.

**For more information and timely updates visit:**

[www.merchantprocessingnews.com](http://www.merchantprocessingnews.com)



# Visa USA Data Security Alert

## POS PIN Entry Device Vulnerabilities

November 19, 2007

To support compliance with the *Payment Card Industry PIN Security Requirements*, Visa is committed to helping members and payment system participants better understand their responsibilities related to securing PIN data. As part of this commitment, Visa issues alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Acquirers may share this alert with their merchants, agents and other parties to help ensure they are aware of emerging vulnerabilities, and take steps, where appropriate, to mitigate risk.

### POS Vulnerabilities

Visa has received an increasing number of reports regarding point-of-sale (POS) PIN Entry Device (PED) thefts from merchant store locations, typically occurring late at night. Evidence indicates POS PEDs are being physically removed from their locations and are being replaced with modified devices designed to skim account and PIN data. Surveillance has also shown that suspects in most of these cases were able to remove and install a POS PED in under one minute.

This type of fraud is typically occurring in merchant locations with “after-hours” operations, and where there is minimal customer traffic and employee supervision over cash registers. The types of merchant locations that have been targeted include supermarkets (MCC 5411), drug stores (MCC 5912) and convenience stores (MCC 5499). However, any store may be affected by this scheme if they have deployed older POS PEDs that are not tamper-evident or tamper-resistant, as required by Visa security requirements. PEDs that are known to be targeted by criminals include VeriFone PINpad 101, 201 and 2000, VeriFone Everest model P003-3xx, Hypercom S7S and S8, and the Ingenico eN-Crypt 2400 (also known as the C2000 Protégé).

### Recommended Mitigation Strategies and Best Practices

Visa strongly recommends merchants use heightened vigilance and maintain a secure store environment at all times, especially around cash registers and POS PEDs. Additionally, Visa recommends the following best practices:

- Merchants should have the ability to monitor PED internal serial numbers and detect when PEDs are disconnected or removed.

- Merchants must ensure that only authorized personnel service deployed terminals and PEDs in accordance with *Payment Card Industry PIN Security Requirements* (see [www.visa.com/pin](http://www.visa.com/pin)). Merchants must properly manage PED inventories and physically secure PEDs at all locations so they cannot be easily modified or replaced.
- Merchants are advised to purchase only PCI-approved PEDs that have been lab-evaluated. *The Visa U.S.A. Inc. Operating Regulations* and *Visa U.S.A. Inc. Interlink Networks Operating Rules* require that PEDs deployed by members and their agents comply with *Payment Card Industry PED Security Requirements*. Visa requires that newly purchased attended POS PEDs from Original Equipment Manufacturers must be Visa-approved and lab-evaluated as of January 1, 2004. Visa/Interlink merchants must deploy PEDs listed on the *Visa PIN-Entry Device Approval List* found at [www.visa.com/pin](http://www.visa.com/pin).
- Merchants are encouraged to work with their merchant bank and/or Encryption and Support Organization (ESO) to create a plan that ensures **all** deployed POS PEDs are Visa-approved, lab-evaluated and comply with the *Triple Data Encryption Standards (TDES)* by July 2010.
- Merchants should train their employees about the potential of PIN compromise when POS PEDs are stolen or missing, or when there are any noticeable signs of device-tampering. Merchants should also be advised to inspect POS PED inventories regularly.
- Merchants are advised to immediately contact their merchant bank, Visa and law enforcement if they suspect tampering of any POS PEDs.

To aid member and merchant compliance efforts, Visa provides ongoing educational workshops to help entities gain further knowledge in all aspects of secure key management. For workshop information, please e-mail [pinusa@visa.com](mailto:pinusa@visa.com).

Additionally, Visa has recently updated the *Visa PIN Security Tools and Best Practices for Merchants* brochure, now available online at [www.visa.com/pin](http://www.visa.com/pin). Hard copies can be requested from the Visa Fulfillment Center at 800-235-3580. This brochure reviews all of Visa’s upcoming PED testing and TDES mandates and their impacts to merchants.

**For more information on Visa’s PIN Security Program, please visit [www.visa.com/pin](http://www.visa.com/pin).**