

# Fraud Alert for U.S. Financial Institutions

## New POS Tamper Scheme

November 13, 2007

Visa is committed to helping payment system participants better understand their responsibilities regarding securing non-public information. As part of this commitment, Visa issues Fraud Alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder of best practices.

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

### **New Point of Sale (POS) Tamper Scheme**

Visa is receiving reports of a new fraud pattern where suspects are attempting to install tampering devices on merchant POS terminals.

Typically, the scheme is executed by a suspect contacting the merchant via telephone stating they are from the “wholesale division of Visa.” The suspect then proceeds to tell the merchant that they can influence and adjust the interchange rates the merchant is charged by their acquiring bank, and attempts to arrange an appointment to visit the merchant’s location to “adjust” their POS terminal to administer these new rates.

Merchants should be advised that there is no “wholesale” division within Visa, and merchants would never be contacted directly to negotiate interchange rates.

### **“Social Engineering”**

Social Engineering is the art of persuading a person to disclose confidential information or access to “privileged” areas within an organization, relying on the natural tendency of people to be trusting and helpful. It is a non-technical form of intrusion that depends heavily on human interaction and often involves tricking others into breaking normal security procedures. The social engineer may claim to be part of Visa (i.e., Help Desk, IT Staff, Security) and will utilize publicly available information in order to “fit in” and seem credible.

### **Recommended Strategies and Best Practices**

Visa strongly recommends heightened vigilance in the management of merchant payment systems, and recommends the following best practices for these fraud scenarios:

- Merchants must ensure that all POS devices are tamper-proof.
- Merchants are advised to immediately contact their merchant bank, Visa and law enforcement if they suspect tampering of any POS PIN Entry Devices (PEDs).
- Merchants should have policies in place to address “social engineering.”
- Merchants are advised to immediately contact their merchant bank and Visa if they are suspicious of any communications with individuals claiming to be from Visa.
- If a merchant receives a suspicious communication, they are advised to tell the person that you will call them back from their publicly listed business phone number.

For additional information on this alert, please call the Fraud Control Hotline at 650-432-2978, option 4, or e-mail [usfraudcontrol@visa.com](mailto:usfraudcontrol@visa.com).