

Visa Inc. Fraud Alert

Personal Identification Number (PIN) Attacks

February 5, 2009



To promote the security and integrity of the payment system, Visa is committed to helping financial institutions and payment system participants better understand their responsibilities related to securing cardholder data and protecting the payment industry. As part of this commitment, Visa issues Fraud Alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Visa financial institutions may share this alert with their stakeholders to promote awareness of these emerging vulnerabilities and ensure that immediate steps are taken to mitigate risk.

Security Vulnerability

PIN Attacks

Reports from financial institutions involving PIN fraud have recently increased. Fraudsters are targeting the automated telephone banking or voice response unit (VRU) systems of financial institutions to change or obtain PIN information. After obtaining a valid PIN, fraudsters can then make unauthorized withdrawals at ATMs.

Weak PIN Change Protocols

Fraudsters utilize automated Voice over Internet Protocol (VoIP) services or other automated broadband internet phone services to dial financial institution VRUs. With stolen account numbers and other personal information (i.e., Social Security number, mother's maiden name), fraudsters are able to bypass security questions or other verification processes. For caller ID validation, "caller ID spoofing" can be used to masquerade or change the caller ID display that is transmitted with the call to appear authentic. Fraudsters can then exploit vulnerable financial institutions that have an automated PIN change option and select a new PIN to fraudulently use at ATMs.

PIN Velocity Checking

For financial institutions that require a PIN as part of their automated verification process, fraudsters employ computers that are programmed to run PIN validation. Hundreds of combinations of account numbers and PINs can be tested at high speed

until the correct PIN is entered. Many VRU systems terminate calls after a specified number of incorrect PIN attempts, but do not prohibit additional attempts from subsequent calls or lockout/suspend the account for excessive incorrect attempts. Fraudsters can automatically redial and, once the correct PIN is validated, they can create counterfeit cards in order to make unauthorized ATM withdrawals using the PIN information.

Financial institution websites that offer online bank account access are also vulnerable to these types of PIN attacks. Sites that have weak PIN change protocols or require minimum account access criteria (i.e., only card number and PIN) are particularly at risk. Fraudsters are able to easily bypass verification protocols to change PINs, and can authenticate account number/PIN combinations using a similar attack method of systemically "guessing" the PIN for stolen account numbers.

Fraudulent ATM transactions typically occur within 24 to 48 hours of a successful validation. These types of attacks and the technology used to commit them are relatively inexpensive for fraudsters. They can occur anywhere because existing Internet connections are used to transmit information.

Recommended Mitigation Strategy

To minimize the possibility of PIN attacks and mitigate the risk of a data compromise, financial institutions should take these actions:

- Verify PIN changes or notify cardholders of PIN changes
- Monitor or lockout/suspend accounts for excessive account access, balance inquiry or incorrect PIN attempts
- Require additional authentication for account access and never have cardholders enter their account number and PIN in the same call/entry
- Limit the use of cardholder PINs in VRUs and in online banking and establish other secure passwords to limit PIN usage and exposure

For more information or questions regarding the information in this alert, please visit www.visa.com/cisp or e-mail cisp@visa.com.