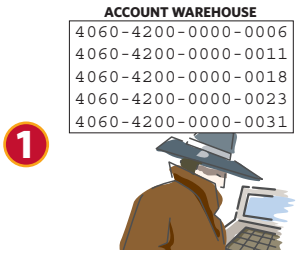
Visa Fraud Alert

Visa USA has learned of a new scam being used to obtain and validate Personal Identification Number (PIN) and account data using member web sites that offer online account access. Hackers and other criminal groups have focused their attention on obtaining PINs in order to make fraudulent ATM withdrawals. The actual source of the PIN can vary; however, Visa recently noticed a pattern of fraudulent card activity that allows hackers to match existing track data with an "easily guessable" corresponding PIN.

How the Scam Works

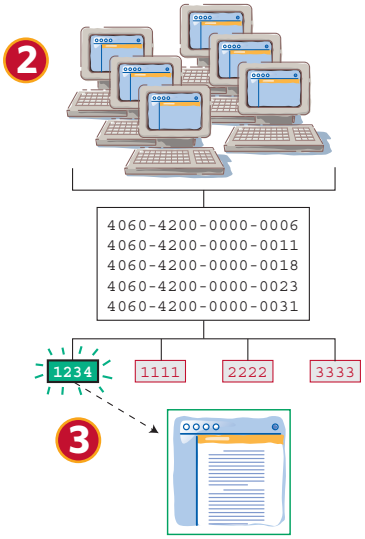
1. Hackers surf the Internet looking for online banking sites that require minimum account access criteria (i.e. only the card number and PIN). The hackers are able to target their attacks since they already hold a large quantity of stolen account data for a given financial institution.



2. Once the hackers identify a vulnerable site, they employ a network of hijacked computers to run their validation against an online banking site.

3. The computers are programmed to test hundreds of combinations of account numbers and PINs at high speed.

If a computer receives:	It is programmed to:
An “invalid” or “denial” response	Initiate the **next** account number/PIN combination
A “valid” response	Alert the hacker that the account number/ PIN combination has been authenticated



4. Hackers use the **authenticated** account number/PIN combinations to create counterfeit cards and withdraw cash at ATMs. The hackers may also have online access to the cardholder’s statements, and perhaps other banking data. Fraudulent ATM transactions typically occur within 24 to 48 hours of a successful validation.

What You Can Do to Prevent This Scam from Happening

This particular scam demonstrates how the nature of PIN theft threats are continuing to evolve, requiring the need for greater member security measures. To protect your web site from this type of PIN authentication attack:

- Continually monitor your web site for “higher than normal” account access attempt volume. If volume exceeds threshold limits, investigate the situation immediately.
- Require additional criteria for online account access, other than just the bankcard account number and PIN.
- Implement controls that restrict or prevent cardholders from selecting “easy to guess” PINs, particularly PINs with sequential or same characters such as 1234, 1111, 2222, or other easily identifiable code patterns such as birth years.

For more information, contact Visa Fraud Control at (650) 432-2978 or at *usfraudcontrol@visa.com*.

© 2006 Visa U.S.A. Inc. Visa Confidential, for member internal use only.