

Fraudulent ATM Withdrawals Reflect a Widespread Threat

Avivah Litan

Recent automated teller machine (ATM) fraud involving Citibank and other banks points to a new wave of "personal identification number (PIN) block" schemes.

NEWS ANALYSIS

Event

On 6 and 7 March 2006, Citibank issued statements in response to consumer complaints that they were unable use their ATM cards to make cash withdrawals in certain countries (Canada, Russia and the United Kingdom). Citibank said that accounts that were "possibly compromised in previous retailer breaches in the U.S." in 2005 were being monitored for fraud.

Analysis

Citibank's actions follow similar measures taken by other U.S. banks, which have reissued ATM cards after customers' cards were compromised, allegedly through a retailer security breach. Gartner believes that these combined bank actions reflect the largest PIN theft to date — and point to a new wave of "PIN block" card fraud. Gartner believes the banking industry is less than halfway through this latest scam, which will continue to affect large numbers of cardholders.

In "PIN block" schemes, hackers break into retailer servers and steal PIN blocks that represent encrypted PIN data (which, along with card numbers, is sent to processors that execute PIN debit transactions). The thieves also steal terminal keys used to encrypt PINs. These keys are typically stored on retailers' terminal controllers. Armed with the PIN block and terminal encryption key, the thieves can determine a cardholder's PIN, then create counterfeit cards that enable them to withdraw cash at ATM machines. In this particular scam, the thieves probably also stole (likely from a retailer) magnetic-stripe data found on the back of ATM cards, which large banks typically validate.

Recommendations

- **Card issuers:** Ensure that the Payment Card Industry (PCI) Data Security standard prohibits the storage of PIN blocks and covers terminal operations.
- **Enterprises:** Never store PIN blocks or magnetic stripe card data. Never store encryption keys along with encrypted data, and keep the encryption keys in high-security environments, such as hardware storage modules available from Safenet, Thales and other providers.
- **Payment vendors:** Modify your software to make the storage of PINs, PIN blocks and cards' magnetic-stripe data impossible.
- **Banks:** Validate magnetic-stripe card data at terminals to make the use of counterfeit cards that do not have this data impossible.
- **Regulators:** Modify Regulation E, which governs consumers' rights with regard to unauthorized bank account withdrawals, loosening the consumer notification timing requirements so that consumers can get their money bank more easily.

Analytical Source: Avivah Litan, Gartner Research

Recommended Reading and Related Research

- "How to Improve the Ailing PCI Program" — PCI security compliance requires improved communications and streamlined and prioritized processes. **By Avivah Litan and John Pescatore**

- "Criminals Exploit Consumer Bank Account and ATM System Weaknesses" — Thieves are using illegal online transfers and ATM withdrawals, often with consumer data obtained online. **By Avivah Litan**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509