



Visa U.S.A. Inc. Data Security Alert

September 29, 2006

To support compliance with the Visa U.S.A. Cardholder Information Security Program, Visa is committed to helping all payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues security alerts when vulnerabilities are detected in the marketplace, or as a reminder about best practices.

Members 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.

Security Vulnerability

Unauthorized Access to Automated Fuel Dispenser Card Readers

Organized crime rings are increasingly targeting merchants to obtain magnetic stripe data (“track data”) and Personal Identification Numbers (“PINs”). Recently, these attacks have focused on Automated Fuel Dispensers (“AFDs”) typically found at gasoline stations. Members and their merchants that operate AFDs should be alerted to the following attack strategy and take steps to reduce potential threats.

Certain AFD models are known to share common pump keys (aka “brass keys”) that allow service station employees and service technicians to gain access to the interior of the pump. This ease-of-entry feature supports legitimate maintenance activity. However, it has been exploited by criminals that have obtained duplicate brass keys to gain unauthorized access to the AFD.

In most cases, criminals are attaching a skimming device to the AFDs card reader in order to directly capture account data. In some isolated cases, PINs have been captured through modifications of the PIN pad. These skimming devices may read and store track data and PINs while allowing a legitimate authorization to occur. The device is typically left in place for several days until the criminal returns and disconnects it. Crime rings have been focusing their efforts in several states with increased activity in Florida and Southern California.

Recommended Mitigation Strategy

To safeguard against the compromise of Visa account information and PINs caused by unauthorized access to AFDs, merchants and agents should take the following actions:

- Merchants should work with their AFD vendors and service providers to ensure AFD access keys are never shared among large populations of devices and all copies of brass keys are securely managed at all times.
- Merchants should implement processes and procedures to ensure AFD access is strictly limited to designated employees or service technicians as appropriate.
- Merchants should conduct regular inspections of AFD interiors to look for any sign of tampering. Legitimate servicing of AFDs should also serve as an opportunity to perform device inspections.
- Acquirers and merchants should work closely with AFD manufacturers to evaluate newer tamper resistant and alarm equipped models.
- Merchants should develop training and security bulletins to support ongoing employee education and inspection efforts. To assist in these efforts, AFD manufacturers have developed several security related publications.
- Merchant security cameras should be trained on AFDs whenever feasible to discourage unauthorized access.
- Merchants that locate AFD skimming devices are asked to immediately contact their sponsoring Visa member financial institution, their local office of the US Secret Service, and Visa Fraud Control at (650) 432-2978.

For more information on Visa’s PIN Security or Cardholder Information Security Programs, please visit: www.visa.com/pin and www.visa.com/cisp

Alert 092906