



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

December 18, 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.

Security Vulnerability: New Social Engineering Schemes Detected

Recently, criminals seeking account information have applied new techniques to previously used schemes to improve their effectiveness. Members are urged to be aware of these emerging attack strategies and to educate their cardholders about these risks when appropriate.

Phone scheme targeting CVV2

In a new twist on the traditional form of phishing, criminals have developed new schemes targeting CVV2 information.

Unlike e-mail in traditional phishing, the communication vehicle for this scheme is a phone or a VoIP ("Voice over IP") device. These schemes are sometimes referred to as "vishing" ("voice phishing").

Vishing is used to supplement information already known to the criminals with pieces of information they may be missing. While many data elements are targeted, CVV2 information is of main concern.

The scheme usually relies on using known information to achieve a level of comfort in the initial stages of the conversation. Additionally, VoIP technology allows for spoofing of the Caller ID which makes the phone call appear more legitimate (i.e. coming from the cardholder's issuing institution).

Once this is achieved, an element of fear is introduced to the conversation to facilitate the extraction of sensitive data. This is commonly done by presenting a fraud scenario which the

caller immediately offers to remedy.

As part of the remediation effort, cardholders are duped into revealing sensitive information the criminals are missing (e.g. CVV2).

Issuers are advised to communicate this threat to their customer service representatives and cardholders as appropriate.

Combined Threat: Distributed Denial of Service Attacks and Phishing

To improve the effectiveness of phishing schemes, criminals have recently combined two techniques: Distributed Denial of Service Attacks (DDoS) with the use of phishing e-mails.

In this scheme, criminals focus their efforts on the cardholder base of a specific institution. Cardholders from a single bank are sent a bogus email advising them of an unexpected network outage while the criminal simultaneously begins to subject the financial institution to a DDoS attack.

A DDoS attack sends an overwhelming number of network requests to a single location from computers scattered around the world. In this case, the objective of the DDoS attack is to create an actual network outage to make the phishing email appear legitimate.

Once the issuer's web infrastructure is unable to respond to cardholder requests, a phishing email is sent. This email contains an 'alternate' link to be used until the issue is resolved.

The link redirects the cardholder to a web page that usually replicates the 'look and feel' of the legitimate member web site and contributes to the effectiveness of this scheme.

If subjected to a DDoS attack, issuers should be on alert for this attack method and communicate the threat to their customer service representatives and cardholders as appropriate. The added element of credibility provided by the DDoS attack can make this phishing scheme more dangerous than other forms.

To minimize this risk, issuers should ensure their policies about requesting sensitive information from customers is communicated to customer so they are less susceptible to this scheme.

For more information on Visa's Cardholder Information Security Program, please visit <http://www.visa.com/cisp>. Questions about this alert may be directed to CISP@Visa.com

Alert 121806