

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

July 24, 2007



To support compliance with the Payment Card Industry Data Security Standard (PCI DSS), Visa USA is committed to helping members and payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues Data Security Briefs when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Members may share this brief 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

Jury Duty Scam – A Lesson in Identity Theft

This is a scam! Consumers are urged not to give any personal information over the phone! These fraudsters are attempting to commit identity theft by appealing to the victim's sense of social conscience and fear of prosecution.

Fraudsters are very skilled in devising creative ways to gain the trust of their victims. One of the most common tactics fraudsters use to commit identity theft is called "phishing," and is the use of social engineering or manipulation techniques to trick victims into divulging sensitive information. While phishing usually refers to e-mail scams, similar fraud schemes can take place over the telephone – this is referred to as "vishing" or voice-phishing.

Although not a new concept, this scam is a classic example of a vishing scheme with a new twist, exploiting civic-minded individuals.

Recommended Mitigation Strategy

Visa, the Federal Bureau of Investigation (FBI) and Snopes.com all advise consumers to never give out confidential or personal information when receiving unsolicited phone calls or e-mails. Additionally, court personnel will never ask for private information over the phone and typically only communicate via traditional mail.

To protect against identity theft, consumers are warned to take the following precautions:

- Always verify the legitimacy of the caller by asking for official company or agency contact information, and then using directory assistance to verify and cross-reference the information given.
- Never solely rely on the phone number the caller provides as a means of verifying the authenticity of the call. Scam artists will often have an accomplice answer the phone to appear legitimate in the event of a return call.
- For e-mails, never respond directly to or click on a link in the e-mail. Always close the e-mail and open a new Web browser window to go to the official company or agency Web site to verify the authenticity of the e-mail.
- No matter how official the caller sounds or the e-mail appears, legitimate businesses or government agencies will not ask for sensitive, personal or financial information in their correspondence (this should always be a red flag).

For additional tips on identity theft prevention, visit:

Visa link:

http://usa.visa.com/personal/security/protect_yourself/id_theft/theft_prevention.html

FBI link:

http://www.fbi.gov/page2/june06/jury_scams060206

For more information on *Visa Security & Protection*, please visit

www.usa.visa.com/personal/security