

Visa Data Security Brief

VoIP Security Vulnerabilities

December 28, 2007



To promote the security and integrity of the payment system, Visa is committed to helping financial institutions and payment system participants better understand their responsibilities related to securing cardholder data and protecting the payment brand. 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.

Financial institution clients may share this brief with their stakeholders to help ensure they are aware of these emerging vulnerabilities and take steps to mitigate these risks.

Security Vulnerability

VoIP Security Vulnerabilities

Voice over Internet Protocol (VoIP) is the transmission of voice communications over the Internet or through a network using Internet Protocol (IP) standards. A telecommunications breakthrough, VoIP services have gained popularity in recent years due to the technology of using the Internet for both data and voice networking. This also makes VoIP technology relatively inexpensive since the Internet connection can be used for both services and traditional telephone lines can be eliminated. However, with new and inexpensive technology come new risks.

The security vulnerability with VoIP technology is the same with any technology that transfers data or information. As network intruders can intercept e-mails and Internet transactions, they can also intercept Internet-based voice transmissions, similar to eavesdropping on telephone or cell phone conversations. Confidential information, such as social security numbers, passwords and credit card numbers can be intercepted and then used for identity theft or other criminal purposes.

Aside from eavesdropping on VoIP conversations, another VoIP fraud scheme involves voice-phishing or "vishing." Much like the more common "phishing" scam of manipulating victims into divulging sensitive information in e-mails, vishing schemes take place over the telephone. Network intruders can hack into VoIP networks and call customers claiming to be a

VoIP service provider or a legitimate financial institution. The caller uses "caller ID spoofing" to masquerade or change the caller ID display that is transmitted with the call to appear authentic. Hackers can also re-route calls to phony customer service lines. Once the caller gains the victim's confidence, they ask for account numbers, passwords and other critical information to attempt identity theft or to defraud the victim.

Recommended Mitigation Strategy

As VoIP technology and services become more prevalent with consumers, VoIP security is paramount. To mitigate the security risks and vulnerabilities associated with VoIP, the following precautions should be taken:

- Ensure VoIP providers utilize encryption
- Route all inbound VoIP traffic through firewalls and other intrusion prevention or security mechanisms
- Segment VoIP and data networks

To protect against VoIP vishing attacks, consumers are warned to take the following precautions:

- Always verify the legitimacy of the caller by asking for official business or company 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. Network intruders can spoof or re-route calls if they have compromised the VoIP network.
- No matter how official the caller sounds, legitimate businesses or financial institutions will not ask for sensitive, personal or financial information over the phone (this should always be a red flag).

For more information on VoIP vishing schemes and how to protect against them, visit the following Federal Bureau of Investigation (FBI) link:

<http://www.fbi.gov/page2/feb07/vishing022307.htm>

For more information on *Visa Security & Protection*, please visit www.usa.visa.com/personal/security.

For information on securing cardholder data, please visit www.visa.com/cisp.