

# MerchantResource



## Voice Over IP (VoIP) Risks and Tips

### What is Voice Over IP?

Voice Over IP (VoIP) technology allows for telephone communication over the Internet. The technology converts a caller's audio signal (voice) to a digital signal or data packet. Transferred through the Internet the data packets are converted back to an audio signal before reaching their destination – the other caller. The conversions occur in milliseconds, making Internet telephone calls as streamlined as landline calls.

### Benefits of VoIP

Businesses and consumers continue to adopt VoIP systems to take advantage of lower rates, as the Internet makes long-distant call charges obsolete. Additionally, many providers of VoIP charge a flat rate for unlimited calls and include extra features such as caller ID and teleconferencing.

VoIP is a relatively new technology, and enhanced features are continually being developed. Beyond cost savings, many organizations appreciate VoIP's mobility. For example, a remote employee with a stable Internet connection can utilize the VoIP to receive and make calls all over the world. VoIP also works in tandem with other technologies, allowing video conferencing, as well as uploading, downloading and exchanging files.

### Did you know?

- Soon, you may have to wade through SPAM in your voicemail box just as you do in your e-mail inbox.
- Someday, merely answering the phone could expose your computer to viruses.
- Tools available for free download on the Internet allow individuals to eavesdrop on Voice over IP (VoIP) telephone calls.

In their investigation of over 170 payment card compromises, AmbironTrustWave's SpiderLabs<sup>SM</sup> division finds that malicious code embedded in an application is the number one method of payment card compromise. This method can consist of either a Trojan or backdoor attack. With VoIP adoption continuing to accelerate, attackers may soon begin launching Trojan and backdoor attacks through the technology.

CHASE Paymentech<sup>™</sup>

## VoIP Security

VoIP has remained relatively secure due to limited availability of the technology. But, with its growing popularity among businesses and consumers, security risks are rising. As VoIP utilizes the Internet and local networks, it is vulnerable to attacks that hackers have been launching and perfecting for years. With due diligence, an organization can implement VoIP securely.

We recommend the following:

- **PCI DSS Considerations**  
If an organization accepts payment card information, they must comply with PCI DSS. If they also use VoIP, organizations must take additional steps to secure the network. Just as Internet payment transactions must be encrypted for protection, VoIP calls should also encrypt voice data and perform two-factor authentication, using a Virtual Private Network (VPN). Because VoIP uses IP addresses and can open a network to attack, patch management is also important. Any VoIP user should ensure their VoIP software and operating system is regularly updated and patched.
- **Segmentation**  
There are free Internet tools available that allow individuals to “sniff” for VoIP traffic. An individual can intercept this traffic, inject malicious code into the data packet and then send it along to its destination. If this traffic has no boundaries to the network’s other assets, the code can exploit the network. This threat is similar to that of malicious code downloaded with a file or SPAM.
- **Routing Calls**  
Businesses should use traditional phone lines – Private Branch Exchange (PBX) or Plain Old Telephone System (POTS) – for incoming calls. Those calls are then directed over IP through the internal network. This protects against sniffer tools that allow intercepting VoIP traffic and redirecting.

Remember, incorporating the information above into your data security policy alone will not make you PCI compliant, nor will it completely secure your VoIP technology. These recommendations serve as general guidelines to help enhance your organization’s VoIP security.

## To Get Started

To help its merchants achieve PCI DSS compliance, Chase Paymentech partnered with AmbironTrustWave, a compliance management and data security expert, to provide the expertise you need to get compliant. AmbironTrustWave works with thousands of merchants, from mom-and-pop shops to global operations, guiding them through the PCI DSS compliance process.

AmbironTrustWave’s TrustKeeper® is an easy-to-use Web portal that helps merchants complete the PCI DSS Self-Assessment Questionnaire, schedule required scans, manage onsite audits and answer the questions they have about their network environment and PCI DSS compliance.

To get started, visit

<http://www.chasepaymentech.trustkeeper.net>

If you have any questions, please contact AmbironTrustWave support at 1-888-878-7817.