CONSUMER TIPS FOR PROTECTING THE PRIVACY OF THEIR BILLING RECORDS

"If telephone service were billed as a utility, as it was in the past for local service and may be in the future with VOIP service, many of the threats to privacy would simply disappear."

-- Marc Rotenberg
Electronic Privacy Information Center
February 8, 2006, US Senate hearing

Although many VoIP providers already have measures in place to protect customer information, VoIP consumers can nonetheless take proactive steps to further protect the privacy of their phone records. Recent stories have revealed that unscrupulous data brokers have violated the law by illegally obtaining and selling phone records. In some cases, these crafty criminals and identity thieves have pretended to be a customer asking for information about their account in order to obtain a phone bill.

What can customers can do to protect themselves?
VoIP providers generally have a variety of safeguards in place to protect against unauthorized access to customer information, and companies continue to evaluate and enhance these safeguards. In addition to these safeguards, consumers who wish to better protect themselves should follow standard practices to prevent identity theft, such as adding a password to their account, guarding their password and other personal information, and shredding invoices and account information before discarding these documents.

As with any type of phone service or Internet application, consumers should follow basic password protection steps. When customers use passwords, they are prompted to provide the password before accessing online account information or when calling customer support – thus providing extra protection against unscrupulous data miners.

Consumers should:

- **Create separate passwords.** Create separate passwords for voicemail, online access, and for use when calling customer support about your billing account when possible.
- **Set complex passwords using both numbers and letters where appropriate**.
- **Adopt passwords that are not commonly used.** Avoid common passwords such as birth dates, anniversary dates, family or pet names and street addresses.
- **Regularly change the passwords.** Change your password at least every 60 days.
- **Guard your Passwords.**
  - Memorize your passwords
  - Don't share passwords with anyone
- **Protect Paper Documents.** Shred invoices and account information before discarding these documents in the trash.
- **Review the Federal Trade Commission's consumer pre-texting alert --** *Pretexting: Your Personal Information Revealed* -- describing how pretexters operate, the laws against it, and advising consumers how to avoid having their information obtained through pretexting. Available at: http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm

If You Think You're a Victim:
Contact the Federal Trade Commission as soon as possible. The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint, or to get free information on any of 150 consumer topics, call toll-free, 1-877-ID-THEFT (1-877-438-4338), or use the complaint form at www.ftc.gov/idtheft. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

"Companies that engage in pretexting – the practice of obtaining personal information, such as telephone records, under false pretenses – not only violate the law, but they undermine consumers' confidence in the marketplace and in the security of their sensitive data."

-- Federal Trade Commissioner, Jonathan Leibowitz