

Securing your phone system from attack by fraudsters

**From Deborah Gillis QC
Risk and Practice Management Advisor
Lawyers' Insurance Association of Nova Scotia
May 2010**

Last year a Burlington, Ontario, law firm was hit by fraudsters who broke into its voice mail system and charged more than \$207,000 in calls to Sierra Leone. The law firm's service provider expected it to pay \$100,000 of this amount.

A Nova Scotia law firm reported to me that it was recently targeted in a similar scheme.

How it often works

Fraudsters frequently target businesses using a PBX (Private Branch Exchange) phone system or voice mail. Nights, weekends and holidays are prime times for this type of fraud. Often using an automatic dialer, fraudsters target a specific phone number and then wait for a voice mail response. Once into voice mail, password cracking software is used to try all possible combination of characters until it hits the right password and gains access to the firm's voice mail. The fraudster then chooses the option that allows a long-distance call to be made, and racks up a huge long-distance bill on your account. Thousands of calls can be made in a very short period of time.

Voice mail systems using only simple passwords (e.g.3456, 3333, 4444) or unchanged factory default passwords are particularly vulnerable.

To protect yourself

To protect yourself, learn more about your telephone system, its vulnerabilities and the signs of a security breach.

At http://www.allstream.com/customercare/bulletins/long_distance_fraud.html, you will find an excellent resource prepared by Allstream that discusses long-distance fraud, security breach signs and tips for securing your phone system(s). I strongly recommend that you read this and take immediate steps to protect your phone system and your financial well-being.

If you have any questions on this or any other risk and practice management matter, you may contact me at 902-423-1300 (345) or at dgillis@lians.ca.