TelecomOptions
CLEARLY YOUR BEST CHOICE

Protect Your Business From Fraud

What is toll fraud?

Toll fraud is the theft of long distance services by an unknown third party. It takes many forms including but not limited to the unauthorized entry into a customer's phone system or equipment. By way of example, businesses that use third party private exchange (PBX) telephone systems and/or third party voicemail systems are particularly at risk if these systems are not secure. Toll fraud is a global, industry wide problem with potentially devastating effects--racking up tens of thousands of dollars worth of long distance calls in a very short time.

Understanding your legal responsibility

Securing your phone system is an imperative step in protecting your company from toll fraud. In such cases, if a call has originated with, or passed through your phone system or equipment, you are responsible for the charges associated with the call, whether the call is authorized or not. This means that if you are the victim of toll fraud, you are liable for the costs.

How could an unauthorized person gain access to your long distance service?

There are many possibilities. Thieves or hackers can:

- Break into your PBX, using Direct System Access (DISA), remote access and maintenance ports, or modems, and place calls as though they originated from your system
- Break into your voicemail system and take over mailboxes, and/or steal long distance by obtaining an outside line, or by programming a mailbox to accept 3rd party billed calls
- Use your toll free (800.888.877.866.855) numbers and make calls that you didn't intend to or want to pay for
- Use your company calling card numbers to place international calls
- Go through your trash, commonly known as 'dumpster diving'-- searching for codes
- Use your printed internal telephone directory to try & 'recruit' your employees
- Con your switchboard and reception staff into accepting collect calls or connecting them to long distance trunks--a technique known as 'social engineering'
- Bill international calls to your telephone number by employing a third number billing scam
- 'Shoulder surf' in airports or other public locations to obtain calling card numbers and authorization codes by looking over callers' shoulders as they use them

Know the access paths that open doors to fraud

Thieves can gain access to your telephone equipment via:

- Direct Inward System Access (DISA)
- Voicemail Systems
- Remote System Administration (Maintenance Ports)
- Direct Inward Dialing
- Tie Trucks and Tandem Network Services
- Modems

Secure your Systems

PBX (Private Branch Exchange), DISA (Direct Inward System Access) and Remote Access Ports:

- Never publish a DISA telephone number
- Change the DISA access telephone number periodically
- Use longer DISA authorization codes--9digits ideally, never less than 7
- Issue a different DISA authorization code for all users
- Warn DISA users not to write down authorization codes
- Restrict DISA access at night, and on weekends and holidays, as these are prime times for fraud
- Block or restrict overseas access, or only allow access to certain country or area codes
- Program your system to answer with silence after five or six rings (Most systems are programmed to answer with a steady tone after two rings and this is what hackers look for)
- If possible, route invalid access attempts to your operator
- If possible, program your PBX to generate an alarm if an unusual number of invalid attempts are made
- Program your PBX so that the port will disable itself after a set number of invalid attempts
- Disconnect all telephone extensions the moment they are no longer needed
- Block access to remote maintenance/administration ports, or use maximum length passwords and change them frequently--do not use sequential access numbers
- Disconnect modems that are not in use

Voicemail Systems

- Assign and change passwords regularly
- Increase password length, and prohibit the use of trivial, simple passwords such as 222 or 123
- Prohibit the sharing or posting of passwords, or entering them into programmable keys or speed dial buttons
- Limit the number of consecutive login attempts to five or less

- Keep time-out limits short
- Change all factory-installed passwords
- Change the maintenance password regularly, and limit distribution
- Block access to long distance trunking facilities
- Block collect call options on the auto attendant
- Restrict access to directories that give directions on how to get into the voicemail system
- Restrict out-calling
- In systems that allow callers to transfer to other extensions, block any digits that hackers could use to get outside lines, especially trunk access codes
- Use maximum length passwords for system manager box & maintenance ports
- Delete all inactive mailboxes

Long distance Calling

- Restrict access to specific times & limit calling ranges
- Restrict access to business hours only
- Block all toll calls at night, on weekends and on holidays
- Block or limit access to overseas calls--If your company has no requirement to call overseas block overseas calls completely

For further reference please check these websites:

MTS (Allstream): www.allstream.com/support/customer-bulletins/Long-Distance-Fraud-How-To-Protect-Your-Business.html

Shaw:
www.shaw.ca/uploadedFiles/Support/Business_Home_Phone/Learn/Shaw_Business_Phone_Toll_Fraud.pdf

Bell: www.bell.ca/shop/SB-viewCustom.page?pageID=SB_LONG_DISTANCE_FRAUD

Telus: about.telus.com/publicpolicy/unauthorized_person.html