International, Long Distance Toll Fraud Information

What is International, Long Distance Toll Fraud?
International, Long Distance Toll Fraud occurs when a hacker gains access to a company's telephone and/or voice mail system in order to place unauthorized long distance and international calls.

What is a Hacker? A hacker is a person or organization (such as criminals, drug traffickers, terrorist groups) who hacks into a telephone system in order to steal long distance service or hide the origin of their calls to avoid prosecution for illegal activities. Once the hacker breaks into the system, they can then originate calls from the client's telephone system (typically too expensive, international destinations) at the client's expense.

How can a hacker steal long distance service?
Hackers can break into a client's phone system using one of two methods:

1) Via the Internet:
   If the telephone and/or voice mail system is connected to the internet to enable features (such as unified messaging, or off-site IP phones – aka Nomadic Users) or to enable remote administration of the system, it is possible for hackers to gain control of the system and change the configuration or connect an IP phone to the system and make LD/International calls at the client's expense.

2) Via the telephone network:
   Most telephone systems include a voice mail system and/or Direct Inward System Access (DISA) number that can be dialed into and administered through a telephone interface. If hackers are able to access an administrator menu for the system (either due to weak passwords or a software bug) they may be able to configure a voicemail out-dial or call forward an extension to a LD/international destination; Enabling the hacker to make LD/international calls at the client's expense.

Once a hacker successfully breaks into system, they will often sell access to other criminals. The criminals may try to complete as many calls as possible, as quickly as possible until they are blocked, or they may use the hacked PBX sparingly in hopes of using the PBX for a long period of time without being noticed. Depending on the number of concurrent calls the client's connectivity product will support, a network of hackers can complete thousands of dollar's worth of international calls within minutes.

What are some ways that International, Long Distance Toll Fraud can be identified?
- Lights on a telephone are lit up when no one is on the phone
- Unusually high charges for long distance/international calls on your bill

Who is responsible for the charges when International, Long Distance Toll Fraud takes place?
The company (not the provider) is responsible for all charges incurred for calls made from their telephone system, including fraudulent activity.

Who is responsible for securing the network to protect against hackers?
The client is responsible to ensure that their phone system and network are secure from hackers by following best practices and working with their telephone system supplier and/or IT supplier to establish a configuration that does not allow hackers to break into their equipment.

What can clients do to improve security to reduce the risk of being hacked?
If the client's phone system is connected to the internet:
- It is critical that the system be protected by strong passwords wherever/however possible and be on an up-to-date version of software that contains the latest security bug-fixes.
- It is also critical that an up-to-date firewall appliance be used to secure the system so that it can only receive management traffic and VoIP packets from approved IP addresses (such as the public IP address of the phone system vendor and the public IP address of the session border controller of the SIP provider.) All other packets should be dropped by the firewall appliance.

If the client's phone system has an administrator menu that is accessible from the public switched telephone network:
- It is critical that the client consult with their phone system vendor to ensure the system is on an up-to-date version of software and that it has been configured with a secure PIN/Password.
- Keep telephone system equipment in a secure location where only authorized personnel have access

In either case:

- Consider disabling any outdial-related features from the phone system and/or voicemail that are not critical to the business' operation (e.g., voice mail features or DISA).
- Passwords:
  - Change default passwords
  - Change passwords regularly
  - Use complex passwords, not passwords with repeating digits or sequential numbers
  - Ensure that only trusted administrators know the administrative password
  - Change passwords when employee turnover takes place
  - Do not keep extensions active for past employees
- DISA feature:
  - Limit access to DISA feature to those employees who truly need it
  - Ensure the first few digits of the DISA access number are different than the voice line telephone number
- Voice Mail:
  - Disable the external calling feature in the voice mail unless absolutely necessary
  - Remove inactive voice mail boxes
  - Disable voice mail features that you do not need
- Educate your staff about the importance of telephone system security and the negative impact International, Long Distance Toll Fraud could have on your business
- Monitor your company's call history for unusual activity

POPP can help!

In addition to the security measures mentioned above, POPP strongly recommends the client implement either of the POPP-provided security features below:

- International Call Blocking – Unless the business has legitimate need to call outside of the US/Canada, it is strongly recommended that you allow POPP to block the lines from making calls to international destinations.
- International/LD account codes – This feature requires all callers to enter a numeric pin before a call to a LD, 411 and/or International number will complete.

These features not only protect the client from hackers, but also employee misuse of LD/International service.