Dear FirstLight Customer,

The telecommunications industry has recently experienced an increase in the number of occurrences of unauthorized users accessing PBX and Key Systems to place international calls. This has resulted in some businesses being left to pick up the charges for these fraudulent calls.

As your trusted telecommunications and technology solution partner we are hoping to provide some useful information around best practices that might help prevent this from happening to your organization. Securing your PBX or Key System is a critical step towards stopping this type of fraudulent activity.

IF MY PBX OR KEY SYSTEM IS HACKED WHO IS RESPONSIBLE FOR THE CHARGES?

Toll charges incurred for ALL calls made over the business owners telecommunications equipment and facilities are the responsibility of the PBX owner, regardless of how those charges were incurred. It is important to work with your PBX provider and risk management team to safeguard your system. The following are some suggestions to get started.

WHAT CAN MY ORGANIZATION DO TO SAFEGUARD OUR SYSTEM?

Take the steps outlined below to prevent unauthorized access to your PBX and other phone equipment.

- Do not transfer callers to outside lines. Train your users to never transfer a caller to an open line, or to any number that begins with your outside line code, normally 9 followed by a 0 or 001.
- Disable remote call out feature. Disable the feature that allows users to connect to an outside line after dialing into their voice mail box. This will prevent hackers from gaining an outside line through the voice mail system.
- Enforce Digital Call Blocking. Make sure your dial plan only allows calling to areas where your organization needs to place calls. If you do not require international calling then don't allow that from your phone system. Your administrator may be able to prevent dialing of '901' or '9011' to access outside lines.

WHAT IS PBX FRAUD?

PBX Fraud, or Key System fraud, is a hacking of your system or other phone equipment by an unauthorized user with the intent to initiate international calls resulting in unauthorized charges for the PBX owner.

- Use Strong Passwords. Most unauthorized access is gained by cracking simple passwords. Make sure your system and your voice mail system are configured with passwords that contain numbers, letters and special characters.
- Manage connectivity via a remote maintenance line. Many systems have a phone line into the PBX for remote maintenance. Unauthorized users can use this line to gain access and make international calls. If you require this for vendor support, develop a process for connecting and disconnecting the line so that only your remote administrator can use this line for system access.

WHAT CAN MY ORGANIZATION DO TO BE PREPARED?

- Create a plan to disable international calling and provide instructions to shut down PBX equipment and make code changes
- Establish a process so vendors can secure access to PBX equipment and perform a shutdown
- Make sure your contact information for all telecommunications related personnel and vendors is up to date and readily available
- If you suspect fraudulent activity, contact **your PBX vendor** immediately to report your suspicions

IT COULD BE YOUR DEVICE!

Much of the recent toll fraud activity has occurred through security breaches of end devices such as Laptops, Smart Phones and Tablets that were running software voice clients or soft phones. These end devices can be running remotely off a premise based system as well as a cloud system. Work with your IT department to ensure that adequate security is being enabled and enforced on these devices to minimize the risk of toll fraud.

To report suspected fraudulent calls or to request an international toll block please contact your Account Manager or call customer service at 1-800-520-9911.