IMPORTANT: *If you have any questions or even the slightest suspicion the international toll fraud has been committed against your company, please call FirstLight's Customer Care Department at* **1–800–461–4863** *to open an incident report.*

Mitigating International Toll Fraud Exposure

FirstLight Fiber is committed to assisting our customers in limiting international toll fraud on their internal phone systems, also known as Private Branch Exchange (PBX) systems. While FirstLight operates a fraud detection and monitoring system that identifies and restricts suspicious international calling to reduce international toll fraud exposure, *the security of your company's PBX and its internal processes are beyond FirstLight's scope*. As such, FirstLight recommends that you consider these simple and sound practices.

Secure Your PBX

- Speak with your PBX vendor about implementing every security feature on your PBX.
- Replace default passwords and access codes with original passwords and change them often.
- Restrict Remote Access and remove Direct Inward System Access (DISA).
- Secure your PBX remote maintenance port, which allows authorized technicians to perform remote repairs. An optional Remote Port Security Device (RPSD) can also be employed. Make sure your vendor has a schedule to regularly change maintenance access passwords.
- Use best practices to protect internal documentation of the PBX.
- Meet regularly with your PBX vendor to review software and hardware changes as they become available to remain as secure as possible.

Educate Your Employees

Educate your employees on potential exposure and explain the need to follow security protocols. PBX security is your company's responsibility and it is every employee's job to remain alert and notify management about abnormal events including but not limited to:

- Excessive hang-ups.
- Apologetic wrong number messages.
- Dead air.
- Frequent calls requesting nonexistent extensions.
- Make sure your reception staff knows the valid extension patterns for your PBX.

Passwords and Access Code Protection

Security measures to deter criminals include the establishment of passwords and access codes for all PBX related systems including Voicemail and Auto Attendants. Best practices include:

- Use of maximum number of characters allowed by the PBX
- Use of (#) and (*)
- Do not use ascending or descending digits; for examples, "1234" or "4321"
- Do not use identical digits; for example "1111"
- Block access codes such as "9-XXX"
- Do not use internal extensions as passwords or access codes.
- Mandate that default passwords or access codes are not used.
- Require users to change passwords and access codes on a regular basis; i.e. monthly, quarterly, etc. This includes voicemail passwords as well as access codes for International or toll completion.
- Remove/change passwords and access codes when employees leave the company.

Voicemail and Auto Attendant Security

Voicemail and Auto Attendants are common vulnerability points of your PBX. In addition to the above, methods to improve security include but are not limited to:

- Use the maximum number of digits including (#) and (*) to secure your voicemail passwords/access codes.

(over)

- Delete all inactive voicemail accounts.
- Ensure outbound access is not enabled on your auto attendant.

Limit Your Exposure

Implementing tighter controls will provide greater security from toll fraud. Common practices include:

- Select restriction of calls to company that you do not need to reach.
- Calls that do not start with 011 can also be international and are often overlooked in security arrangements. Consult with your PBX vendor to identify these exposure points.
- Limit international call capabilities to select employees/staff.
- Activate time of day restrictions to prohibit toll calling during non-business hours, at night, on weekends or holidays. *Criminals often will direct their heaviest assaults on your network when vigilance is at its lowest.*

Be Proactive

The FCC has ruled that the end-user (customer) is responsible to pay the long distance charges resulting from Fraudulent use of the phone. You cannot completely eliminate the risk of international toll fraud, but you can be prepared if and when it occurs, and thus minimize the damage to your company's operations and finances. There is no limit to the potential loss and liability in the event of international toll fraud, and charges can mount very quickly.

If, despite your best anti-fraud efforts, you suspect or actually detect international toll fraud, ***immediately contact:***

- **Your PBX equipment vendor**
- **FirstLight Fiber (1–800–461–4863)**

You should also immediately notify State Police, the Federal Bureau of Investigation (FBI) and your insurance carrier.

We at FirstLight Fiber are thoroughly committed to joining with our customers and law enforcement officials to combat international toll fraud.