Protecting your business from Toll Fraud

Shaw Business

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 system 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.

We highly recommend engaging the provider or maintainer of your phone system and equipment to learn how to prevent toll fraud. Should we identify unusual long-distance calling activities on your account, we may contact you to inquire as to the legitimacy of those calls. However, it is your responsibility of ensuring your phone system and equipment is secure.

What can I do to protect my phone system?

Just as you would not leave the front door unlocked or the keys in the ignition, your phone system must be appropriately secured. We have outlined below protective measures you may take to reduce the risk of toll fraud. Keep in mind these are general guidelines, and we do encourage you to contact the provider or maintainer of your phone system to discuss security measures specific to your own set up.

• **General Security:** Develop policies, maintain strong physical security, follow best practices for securing an IP-based service, monitor resources for new vulnerabilities, maintain patches, and review logs. Consider utilizing standards-based security add-ons where possible.

• **Toll Restriction:** International locations are the major destination for toll fraud calls. Recommended practice is to block all international numbers and only enable those you need to call. Some systems allow for passwords to be required for long-distance calls.

• Restrict outbound calling after hours.

• **Passwords:** Immediately change the default passwords provided with your phone systems. Change user and administration passwords frequently. Change phone system passwords when key personnel leave your organization.

• **Unused Mailboxes & Phones:** When employees leave the company, remove their access from all phone systems immediately. This is not only to protect against retaliation from a disgruntled ex-employee but also from anyone who may obtain that ex-employee's
login information.

• **External Transfer:** Restrict call forwarding and call transfer features. Program your phone system so that extensions can forward only to known numbers and restrict all others. Never forward a caller to 901 or 90#.

• **Software Patches:** Make sure that your phone and voice mail systems are up to date and have all current patches or firmware updates installed.

• **Monitoring:** Monitor calling patterns and usage using whatever auditing features are provided with the system on a daily or weekly basis. Most toll fraud is generated in a short time – days to weeks and usually after hours when detection is least likely. Encourage employees to report strange languages on voice messages, especially those left after hours, or unusual & unexpected activity by the phone systems (i.e. all lines busy first thing in the morning).

• **Social Engineering:** Instruct employees to never give out technical information about your phone systems to unknown callers. Taking a moment to return a call can help to ensure you are speaking to the correct people.

• **Full Security Audit:** We strongly suggest having a qualified or certified telecommunications technician or your iT department audit your phone systems to probe for any vulnerabilities that may have been overlooked or neglected. IT or telecom technicians may open ports 5060, 5070, and 5080 for testing. When testing is completed ensure the ports are closed or turned back off, otherwise fraudsters can enter through this weakness.

• **IP PBX:** IP PBXs are susceptible to the same fraud issues as traditional phone systems. Additionally, they are also subject to security gaps in your data network. Control administrative access, user host-based intrusion prevention, and use network firewalls/intrusion prevention systems.

What to do if you suspect Toll Fraud

1. Contact the provider/maintainer of your phone system immediately
2. Call Shaw **and ask to speak to the Shaw Telephony Investigation team** or your long-distance provider immediately
3. Report the incident to your local police authority

For enquiries or further information regarding toll fraud, please contact our Shaw Phone Security Team directly at

1 855 551 7429 or by email at **ShawTelephonyInvestigations@sjrb.ca**

Shaw Business owns and operates a 625,000 kilometre fibre route network that connects North American businesses from coast to coast, providing data networking, video, voice and Internet services to companies of all sizes. We are continually investing in our infrastructure and advancing our technology so that you can count on us for an industry leading experience that scales to meet your business needs today, as well as in the future.

For more information see business.shaw.ca

Shaw Business

1-877-742-9249 inquiries@shawbusiness.ca

linkedin.com/company/shaw-business