Toll Fraud & International Long Distance Blocking

What is Toll Fraud?

Toll Fraud is the theft of long-distance services by an unknown third party. It occurs when there is a security breach to your phone system or equipment, resulting in unauthorized long-distance calls which can result in severe charges on your account. Businesses using a third party Private Branch Exchange (PBX) telephone system and/or third party voicemail systems are particularly at risk if these systems are not secure. It is a global, industry-wide problem with potentially devastating effects – incurring immense long-distance charges in a very short time.

Understanding Your Legal Responsibility

Securing your phone system is an imperative step in protecting your company from toll fraud. 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. Ultimately it is your responsibility to ensure that your phone system and equipment are 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. Below are protective measures you may take to reduce the risk of toll fraud. Keep in mind these are general guidelines and we encourage you to contact the provider or maintainer of your phone system to discuss security measures specific to your own setup.

- 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 a 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.

- After Hours 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 not only protects 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 installed.

- Monitoring: Monitor calling patterns and usage when 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 system (ie: 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.

- Formal Audit: Consider having an accredited, professional third party audit your phone systems to probe for any vulnerabilities that may have been overlooked or neglected.

- IP PBX: IP PBX's 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 can Shaw Business do to help?

International Long Distance Blocking

To assist our customers in preventing toll fraud, Shaw Business blocks International Long Distance calling unless a customer has requested by way of signed authorization to have International Long Distance calling enabled. If you do not wish to have international long distance calling blocked, please sign and return the attached request by email to your project coordinator prior to your service hand-off.

International Long Distance access can be requested at any time after service hand-off by contacting our client services team at 1.866.244.7474 or by sending the attached authorization via email to clientservices@shawbusiness.ca. International Long Distance will be available within 1 business day of the request. Please note that due to the authorization requirement, after-hours requests will be fulfilled the following business day.

Even with the blocking that Shaw Business will employ, Toll Fraud is still possible so it is critical that your phone system is secured to protect your company from potential intrusion threats. 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.

Port State Monitoring

Shaw Business does not monitor voice traffic, however we do monitor the Port State of the switch (ie: up, down or flapping). Because we do not monitor traffic, unusual and suspicious activity would not be captured.

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 to ensure that your phone system and equipment are secure. If you would like further information on how to protect your company from toll fraud, please visit our website at:

http://www.shawbusinesssolutions.ca/sbs/solutions/voice.jsp.

What to do if You Suspect Toll Fraud

1. Contact the provider/maintainer of your phone system immediately
2. Call Shaw Business or your long-distance provider immediately
3. Report the incident to your local police authority

For inquiries or further information regarding toll fraud, please contact our Network Operations Team directly at 1.866.244.7475.

Shaw Business Acceptable Use Policy

As per Acceptable Usage Policy located online at http://www.shawbusinesssolutions.ca/sbs/aup.jsp, the customer is solely responsible for use of their Shaw Business account, regardless if such use occurred without the account holder's consent or knowledge.