Ocean Telecom / Ocean Talk Toll Fraud Precautions

The key to preventing Toll Fraud is having the appropriate knowledge to defend yourself and your business.

Ocean is dedicated to reducing the risk our customers face to the best extent possible. Whilst we appreciate that no telecommunications system will be completely immune to the danger, our advice regarding security can alleviate the risk significantly. The main points to consider are discussed below.

Cases of Toll Fraud are extensively linked with the stealing of authorisation codes and passwords. It is essential that your staff safeguard these to the best of their ability. The numbers should never be written down or programmed into auto diallers. If you have staff who travel outside of the office they should also be aware that thieves can be watching or listening in to phone calls in order to find out the relevant numbers.

Furthermore, it is important to establish the identity of anyone placing a collect call to the company before accepting charges. An ever increasing problem is the receipt of a phone call where the caller asks to be transferred. This is yet another way in which access can be gained to your network and an outside line. An advisable approach would be to establish a system whereby any suspicious activity is reported immediately by your employees. Suspicions may be aroused by the nature of the call or by the number of phone calls received.

Secondly, control of your phone calls is a good way to heighten the security of your firm. Most thieves will focus on making non permitted long distance calls. You are able to place restrictions on this with your network provider or Ocean Telecom upon request, by eliminating or restricting unnecessary calls to other countries. This is ideal if you know the countries you do not do business with. You could also place limits on which of your workers are allowed to make such calls or on what times calls are made, as this could stop phone calls in the evening.

There are certain signals to look out for that will alert you of toll fraud. A growing number of thieves will try to deceive your workforce in order to gain access. For example, they could ring you on a local access number or 0800 service and ask to be continually transferred between personnel until they obtain an outside line. It is recommended that all of the following should be looked into; obscene phone calls, continuous hanging up of the phone, recurring incidents of asking for an invalid extension number, wrong numbers, callers asking who they have reached and silent calls that wait for you to hang up. All of these techniques have been used in the past and should raise alarm bells if they occur in your office.

Passwords are the easiest form of protection but there are several ways to make these more secure. The more characters you use the better. You should also avoid patterns in your system such as digits that follow in order or all of the same numbers. Do not use default passwords or access numbers as they are simple to crack. Keep away from making the password the same as the extension number or those which are related to the owner, such as an I.D. Room or National Insurance number. In line with this it is also advisable to frequently change the user passwords. We would recommend doing this quarterly, as well as when anyone leaves the firm who had access to them.

In addition, you should keep a regular check on your voice mail system. Within this fraudsters could access messages, make their own mailboxes or transfer until they find an outside line. You could stop this by the use of internal calls only within the voice mail, getting rid of mailboxes of previous employees immediately or making sure there are no spare, needless mailboxes. Users should change their Personal Identification Numbers (PIN) routinely for access to the voice mailbox, as well as taking the previous advice of making sure that these involve the maximum amount of characters to reduce the chances of a hacker. Remote access telephone numbers should not be published either as this puts you at risk.

Next, automated attendants that answer a company's telephones can also leave them open to fraud. The toll fraudsters will go from the automated attendant and dial the 90XX or 900 extensions. On several telephone systems these numbers may connect them to outside lines. You can limit or block the capabilities of local dialling or long distance trunks in order to stop this. Request that Ocean Telecom or your line provider block access codes such as 900XXX can be used in these circumstances. Ocean Telecom & lines providers do not block premium rate numbers automatically as many businesses use them for legitimate purposes.

A more recent method for fraudsters to access you systems has developed, following the more widespread use of IP services by businesses. It affects business is using SIP trunks, has off-site IP telephones or is using PC client applications (on smart phones, desktops or laptops) to make calls through your telephone system. If you are using any SIP applications like SIP trunks or softphones over the Internet we would recommend that you must look at the security of your network when implementing. SIP hacking is highly prevalent over the Internet so any ports you leave open could be a way in for a hacker to make fraudulent calls. We would recommend running any SIP applications over a secure VPN connection. If this is not available and you have to open ports on your router/firewall, then we would recommend locking down the access to the source IP addresses (remote end IP addresses). If you are unsure of how to set this up or how this can be achieved then please consult documentation for your router/firewall or speak to your IT department or IT Support Company. Ocean Telecom is not responsible for our customers IT network, therefore the responsibility of security with SIP applications lies with the end user.

In summary, the best way to prevent toll fraud is to look out for the warning signs, such as anything out of the normal. This may manifest itself in the form of out of hour's calls, calls to other countries that you don't recognise having done business with or several incoming calls on your call detail records followed by long outbound calls.

If you notice any of these signs you should take the following steps as toll fraud can lead to extensive losses that can ascend extremely quickly. You should call Ocean and your line/least cost routing provider. We can then help you to prevent further instances of toll fraud. Although there is currently no way to stop toll fraud, you can educate yourself and your workforce to lower the chances of it happening, stop it when it occurs and thereby reduce the harm it can do. The most likely times for it to happen will be when security is lowest, which is normally outside of working hours. You should therefore keep a list of things to look out for as well as what to do if you notice them.

Ocean recommends that the customer include the telephone system related applications as part of their company security policy and seek insurance against such acts. New policies are becoming available called **“Cyber Liability”** that can cover toll fraud as well as the hacking of your IT systems, websites and a number of other items.

Ocean will not be liable for any cost incurred due to toll fraud of any kind.