Toll Fraud Information and Customer Security Best Practices

What Is Toll Fraud?

Toll Fraud is the fraudulent use of a phone system by an unauthorized third party making long distance (LD) or international long distance (ILD) calls where the phone system owner incurs the cost while the hacker does not.

- Individuals or organized groups devise methods to gain entry to a business telephone Private Branch Exchange (PBX) or voice mail system by exploiting weaknesses in the phone system.
- Typically, hackers gain unauthorized access through the PBX's maintenance port, voice mail (if voice mail can be accessed remotely) or the **Direct Inward System Access (DISA)** feature of a PBX. Some hackers call in on toll free lines intended for customer use; some use stolen calling cards; some even impersonate someone else to socially engineer their way into a system.
- Once the hackers gain entry into the phone system, they make outgoing long-distance calls or sell access to the phone system to other hackers, potentially racking up tens of thousands of dollars' worth of long distance calls in a very short time.

Most PBXs today are software-driven. When they are not built correctly, it gives hackers the opportunity to easily access the system remotely. PBX administrators usually manage the system using a PBX maintenance port and communicate via a modem from remote service centers. Hackers take control of this PBX maintenance port and change the call routing, alter passwords, add or delete extensions, or even shut down a PBX, all of which unfavorably impact business operations.

Some voice mail systems may be accessed remotely and programmed to make outbound voice calls. The hacker will search for voice mailboxes that still have active default passwords or have passwords with easy combinations; i.e., 123456. Hackers use the outbound calling feature to forward calls to a "phantom" mailbox that will give a dial tone. This allows them to make domestic or international calls from anywhere on a business account at the business owner's expense. Hackers can also gain access to a mailbox to listen to messages, change greetings or delete messages.

DISA is a feature that offers remote users access to an outside line via a PBX with authorization or account codes. This is a very useful feature for employees who are on frequently on the road or who make long distance calls or international conference calls after business hours. By gaining access to this feature, hackers can access an outside line and make domestic or international toll calls at the business' expense.

More information pertaining to fraudulent or unauthorized use of telephone services that may occur through your account is listed in Fidelity Communications Terms and Conditions, which can be found at the following link: *http://www.fidelitycommunications.com/legal/terms-conditions*.

How will you know if hackers are/have been in your system?

You may notice phone lines that are lit up without anyone using the phone system. You may also be notified by Fidelity or your long-distance carrier that there is suspicious/unusual usage associated with your phone numbers. Unfortunately, you may only find out you have been hacked when you receive a bill for international calls made from one or more of your lines that were not dialed by anyone in your company.

What can you do about it?

As the owner of a PBX or VoIP server, it is your responsibility to secure your system to prevent unauthorized access. Having a properly secured telephone system is the best way to prevent telephone hacking and stop a hacker in his tracks. As a

Toll Fraud Information and Customer Security Best Practices

safeguard, we have listed some industry best practice guidelines that, if followed, could help reduce the risk of telephone hacking. You may have to consult your PBX or telephone system equipment vendor to assist in your system security efforts.

When I get hacked, who is going to pay for the calls?

Should there be any charges incurred on your account due to fraud (including toll fraud), abuse, or misuse of services, known or unknown, your business would be ultimately responsible, whether or not your long-distance provider takes any actions to stop or block Toll Fraud. **Your business is responsible for the security of your PBX system; you should be sure take steps to protect your assets.**

Why don't the carriers write off these charges?

Today, fraudulent calls are placed over many different inter-exchange carriers (IXCs); each carrier must pay the portion of the call they handle. When the call is placed to an international location, the domestic carrier still pays the foreign carrier – even if it is a fraudulent call. As the end user, and because you are the only one who controls access to your PBX system, you and your business would ultimately be responsible for the charges.

Why is identifying or stopping the fraudulent calls the customer's responsibility?

Only the customer can distinguish legitimate calls from fraudulent ones. The carriers do not have access or permission to work on your PBX, which is the vehicle that hackers use most to conduct their activities.

How do I justify the expense of corrective action when we have not suffered a loss?

Past performance is not a good indicator of present threats. The equipment and the motivation to commit this criminal act did not exist many years ago. It is important to educate managers and employees about the pitfalls of not protecting your corporate assets. Enlist their support by implementing a corporate policy on unauthorized access as your first step.

We are a small business, why should hacker activity concern me?

Hackers use auto-dialers to search entire area codes to find systems to hack; they do not care who or where their victims are located. No one is safe—smaller companies may be less able to absorb the average loss ranging from $2,000 to $100,000 plus dollars per incident.

What can we do to protect ourselves from these crooks and con artists?

As with your personal life, the better informed you are the better protected you are from risks. Stay on top of current threats, establish and follow a policy on security, secure your system set-up, create a team approach to security and service, and work with your equipment vendor. Do not let management or your business be taken by surprise. This is one disaster that can be very predictable and equally preventable.

Remember that you can control the severity of these attacks. It is much easier to prevent an attack than to recover your system from hackers.

Toll Fraud Information and Customer Security Best Practices

PBX and VoIP Servers Best Practices

Restrict ILD Countries

Below is a list of International Long-Distance countries with North American Long-Distance area codes, which allows these areas to be direct dialed (i.e., they have an area code and are dialed like any other toll call). Please add these Caribbean area codes to your PBX and have them blocked or accessed only through a dialing code. For the most current list, visit www.nanpa.com/area_codes

242 Bahamas
246 Barbados
264 Anguilla
268 Antigua/Barbuda
284 The British Virgin Islands
340 The U.S. Virgin Islands
345 Cayman Islands
441 Bermuda
473 Grenada
509 Haiti
649 The Turks and Caicos Islands
664 Montserrat
670 U.S. commonwealth of the Northern Mariana Islands
671 Guam
684 American Samoa
721 Saint Maarten
758 St. Lucia
767 Dominica
784 Saint Vincent and the Grenadines
787 & 939 Puerto Rico
809, 829 and 849 Dominican Republic
869 St. Kitts & Nevis
868 Trinidad & Tobago
876 Jamaica

Install Firewalls

- Firewalls are extremely important. If the network enabled PBX is not behind a firewall, it will be hacked.

Authorization Codes/Passwords and Voice Mail

- Do not use default extensions, codes or passwords. Use letters, capital and lowercase, with numbers, and special characters. Be sure to change default settings immediately after PBX install, and update regularly
- Voice mail passwords should be changed often by the user. They should be complex and random, and not any part of the telephone number.
- Dialing out or returning calls through the voice mail system should be disabled. The passwords are not secure since they are numeric and can easily be scanned.
- The amount of login attempts should be lowered to the maximum length 3 before the voice mail system disconnects the call.

- Remove any inactive mailboxes.
- Block international Dialing in dial plans. If you need to place calls internationally, put specific numbers only on dial plans or password protect 011 or NANP international dialing, set spending limits on accounts, whitelist calls to desired countries and blacklist everything else if possible.

DISA

- Limit the DISA access number and authorization codes to only those employees that have a real need for such a feature.
- If possible, ensure the first few digits of the access number for DISA are different from the voice line.

Network Enabled PBX Systems (Discuss with your PBX Vendor)

- Make sure the software version of your PBX is a current, supported version, long-term support release, where security patches are routinely developed. Make sure that the core system is updated and patched for vulnerabilities that are discovered and published. If you have a software version that is no longer supported, update or migrate to an updated version, otherwise you will not be able to obtain security patches for current and future exploits.
- When calls are forwarded but not seen in the Graphical User Interface (GUI) of the PBX administration, check the telephone system database. Identify the section that deals with call forwarding for any numbers or addresses that are possibly call forwarded. Attackers will mask their call forwarding in the database where most people never look. Seriously consider consulting a certified professional for any installation, maintenance or security audits.

When Network Enabled PBX Systems are Hacked (Discuss with your PBX Vendor)

- If the web interface is exposed to the public internet, then it will not matter how complicated the login password is for the administration. The attackers will exploit the code on the interface to gain access and then dump every password. In the event of a security breach, it is necessary to rebuild the system over again, formatting the disk. If you have a trusted backup prior to the attack, then all passwords will need to be changed and new security measures put in place that were lacking initially.

Toll Fraud Information and Customer Security Best Practices

When an Employee is Terminated:

- Whenever an employee is terminated, always make sure that the ex-employee access is removed from company systems just moments prior to or during the termination. You will need to change all passwords related to user and remember to remove email access for that individual.

Social Engineering:

- Make sure all staff is aware of what social engineering is. Prepare your employees when someone attempts to trick them into revealing confidential and private information regarding the company organization and customer information. The attackers will sound convincing. Make sure they are certain they know who they are dealing with.

General Tips:

- Whitelist access to the PBX for Administration to specific IP Addresses
- Run periodic security audits to check for exploits in the PBX
- Frequently audit and change all active codes
- Restrict Toll Free dialing from areas where there is no business requirement
- Do not allow pass-through dialing
- Eliminate trunk to trunk transfer capability
- Restrict 0+, 0- and 10-1XXXX dialing out of PBX
- Restrict all calls to 900, 976, 950 and 411 area codes, and all 1+ dialing to any extent possible
- Restrict all possible means of out-dial (through-dial) capability in your voice mail system
- Consider allowing only attendant-assisted international calling
- Restrict after-hours calling capability: DISA, International, Caribbean and Toll calls
- To combat Social Engineering, make sure that system administration and maintenance telephone numbers are randomly selected, unlisted and that they deviate from normal sequence of other business numbers
- Use multiple levels of security on maintenance access
- Monitor Call-Forwarding activities
- Shred anything listing PBX access numbers, passwords or codes
- Deactivate all unassigned authorization codes
- Do not allow generic or group authorization codes
- Test all PBX voice menus to ensure there's no unintended routing or access exposure to outside lines or internal systems
- Send e-mail reminders to all employees to change passwords on their voice mail periodically