



## Fraud FAQs

Telephone and Internet fraud happens every day. It rings up billions in fraudulent phone charges and victimizes millions of people a year. It can happen in public, in your home, at your business or even in your car. Here at CCT Telecomm we are committed to ensuring our customers are informed to help prevent this fraud from occurring.

### **Preventing Phone Fraud at Your Home or Business**

CCT Telecomm offers the following tips to ensure your protection from phone fraud at your home or business:

1. Don't accept collect calls from people you don't know. By accepting a call, you have agreed to pay the phone charges.
2. Block third-number billing to your phone number. Third-number billing allows you to bill calls you make from other phones to your phone number, but it is also a potential source of phone fraud. If you have a calling card, it's a good idea to block all third-number calls.
3. Watch out for individuals claiming to be law enforcement or telephone companies who ask you to accept collect calls or third-party calls as part of an investigation or telephone repair/analysis project. Legitimate law enforcement and telephone officials will never ask you to accept collect calls or third-number charges. If anyone asks for sensitive information as part of an "investigation," be wary. Don't provide any information and report the activity to the alleged agency or company. Either use the telephone number printed on your statement or look up the inquiring agency number in the telephone book.

### **Preventing PBX Fraud**

CCT Telecomm offers the following tips to ensure your protection from PBX fraud:

A Private Branch Exchange (PBX) is a private switch, either automatic or manually operated, serving extensions in a business and providing access to the public network. Direct Inward System Access (DISA) permits remote access to a PBX from a phone outside the business, usually via a toll-free number or other special access number. Authorized persons can bill long distance calls to the company's PBX. However, criminals can use DISA as a potential fraud opportunity by setting up an illegal call / sell operation at the company's expense.

1. In general, you should always be aware of the signs of PBX abuse, such as:

- Repeated calls of short duration.
- Changes in after-hours calling patterns.
- Sudden increases in 800 / 888 number usage.
- Unexplained increases in incoming or outgoing calls.



2. If practical, eliminate remote access to your PBX and replace it with calling cards for authorized personnel. If you eliminate remote access, make sure the system is disabled when not in use. If eliminating remote access is not an option, try implementing these suggestions to minimize the risk of toll fraud:

- Limit the number of persons who use remote access.
- Use an unpublished number for remote access instead of 800 numbers.
- Add a delayed electronic call response.
- Program the PBX to wait at least five rings before answering a call.
- Use a voice recording or silent prompt instead of a tone.
- Tailor access to the PBX to conform to the needs of your business.
- Block access to international and long distance numbers your company does not call.
- Consider using "time-of-day" routing features to restrict international calls to daytime hours only.
- Always change all default passwords.
- Whenever possible, limit remote PBX access to local calling during normal business hours.
- Be sure to restrict access after hours and on weekends.
- Delete all authorization codes that were programmed into the PBX for testing and servicing.
- Assign authorization codes on a need-to-know basis only.
- Advise employees to treat codes as they would credit card numbers. Never print codes on billing records.

### **Preventing Voicemail Fraud**

CCT Telecomm offers the following tips to ensure your protection from Voicemail fraud:

Voicemail systems answer phones and allow the caller to record messages. The receiver may play and delete the messages or forward them to another person on the same system.

- On voicemail systems that provide out-dial, through-dial capability, or message notification features, always be sure to change any default authorization codes. Trespassers look for default codes on mailboxes, so they can change the codes and control the boxes. Assign users the longest passwords possible, and do not use extension numbers or simple combinations like "1234" as passwords.
- If you have to document passwords, authorization codes, and access codes, keep the information in a secure location and be careful not to share them with anyone who you are not familiar with. Trespassers will seek out passwords, authorization codes, and access codes by snooping around the office, calling businesses and even rummaging through dumpsters. Resulting comprised numbers are sold and traded in the "phone underworld" with the unsuspecting business owners picking up the tab.



## **Social Engineering**

In the communications industry, a Social Engineer uses his or her conversational skills to trick an unsuspecting victim into providing access to dial-tone or other information. Once dial-tone is received on the fraudster's end, calls can be made anywhere, for any length of time. The victim, usually a business owner, is left holding the bill.

Social Engineering happens in a variety of ways:

1. A caller posing as an employee of the "telephone company" calls into the receptionist at ABC Company. He asks the receptionist for assistance in testing the line. He may ask to dial 9, 0, #, and then hit the "connect" key on the telephone set. The 9 will allow him to get an outside line, the 0 will take him to the Operator, and from there he can call any destination, billing back to ABC Company. He may also ask to be connected to extension 90(X) and attempt to get an outside line that way.
2. A caller calls into ABC Company and requests Customer Service. When Customer Service answers, he takes the name of that person and then says he was transferred to the wrong department. He asks to go back to the receptionist, and pretends to be the Customer Service representative asking for help getting an outside line. Once he gets the outside line, he places a fraudulent call, which is then billed back to ABC Company.
3. Social Engineers can manipulate representatives of ABC Company into providing PIN numbers for calling cards, extension numbers, names, password information, telephone system information, or any information that would enable them to make a free phone call. This includes the ability to talk or trick a victim into accepting third-party billed or collect calls.

What can you do?

**EDUCATE!** Tell everyone in your organization and then spread the word externally. Educating employees is the number one deterrent against successful Social Engineering.

**REPORT!** Tell your Communications Manager and your Communications Carrier what has happened. In nearly all cases, the calls originate from a payphone or unknown numbers. Although the fraudster is often impossible to find, Carriers are pooling information in an effort to combat fraud and prosecute the perpetrators.

**PREVENT!** Make changes in your telephone system that may prevent access to well known fraud destinations. You can request an international block from your carrier or certain country code blocks from your telephone equipment vendor. Operator Services can be blocked at the local carrier level to avoid unauthorized charges made through the Operator Service Provider.

Call your vendor and inquire about the security of your current system: Is there access from the outside world into your system or voicemail? Are all systems password protected? Have default passwords been changed? Are features not in use turned off, such as out dialing? Are all vacant voice mailboxes deleted? Read your telephone bills! Inquire about suspect activity to international countries or calls placed outside normal business hours.



### **Internet Dialer Fraud, Modem Hijacking, or Internet Modem Switch Fraud**

Internet dialer fraud, also known as modem hijacking or Internet modem switch fraud, occurs when a "Dialer" software program is downloaded without your knowledge from an Internet site to your computer. Such a dialer is designed to disconnect your current Internet connection and dial out to a different, reprogrammed number. Often the numbers dialed from your computer are expensive long distance, international, or 900 numbers.

Several things may occur if an attempt to establish a connection is made:

1. A dialer box pops up on your screen and indicates that it is dialing when you did not direct it to.
2. Your computer makes an audible noise like it is trying to reconnect.
3. The current site you are browsing doesn't respond to your commands and freezes up.

If you are a victim of Internet dialing fraud or modem hijacking, the FTC offers a complaint form at [www.ftc.gov](http://www.ftc.gov), or contact the FTC toll-free at 1.877.HELP (1.877.382.4357). The FTC works with consumers to prevent fraudulent practices and will enter the information into a secure online database that is available to law enforcement agencies in the United States and abroad.

You may be able to prevent this type of fraud by taking these steps:

1. Have international and 1010 dial around blocks placed onto your phone line if you do not normally need to dial these types of calls. These blocks may not be available in all areas.
2. Remove your telephone line from your modem when you are not actively using your computer. Shut off your computer when it is not in use.
3. Increase the security settings on your operating system software and install a firewall.
4. Be cautious when surfing the Internet or closing pop-up boxes especially if it indicates "no credit card is needed" or a product or service is "free".
5. Install and run up-to-date anti-virus software and spyware removal tools.

### **Preventing Calling Card Fraud**

CCT Telecomm offers the following tips to ensure your protection from calling card fraud:

1. Make sure no one is watching you enter your calling card number or listening as you give your number to an operator. If a "shoulder surfer" sees or hears you enter your card number and PIN (Personal Identification Number) on a pay phone, you may become the next victim of fraud. Block the view of the keypad and speak directly into the phone. When possible, use a phone that reads your card automatically.
2. Do not use your calling card as an identification card. Use your driver's license or some other form of ID.
3. Memorize your calling card and PIN number. Select a PIN that you can easily remember. Ask that your PIN not be printed on your card.



4. Beware of anyone who calls you requesting calling card verification. Telephone companies will NEVER call you to ask for your calling card number. Give out your card number ONLY when placing a call through an operator.
5. If you do not make international calls, request a calling card for domestic use only.
6. Report a lost or stolen card immediately. Notify your calling card provider the moment you suspect your calling card has been lost, stolen or otherwise compromised.

### **Don't Get Slammed**

Slamming is used by some long distance companies to enlarge their customer base by switching the subscriber's long distance carrier without the subscriber's consent or knowledge.

The Federal Communications Commission (FCC) has taken action against companies known to use slamming as it is an illegal practice. The FCC order clearly outlines requirements for the content and format of Letters of Agency (LOAs) in an attempt to reduce or eliminate unauthorized Primary Inter-exchange Carrier (PIC) changes. All rules apply to both residential and business PIC change requests.

In order to prevent your service from being slammed, simply contact your local telephone company business office and ask for a PIC freeze. A PIC freeze indicates that no carrier selection changes can be made unless you notify them by phone or in writing. Only when a customer has authorized a change in carriers is a change allowed to be made to the account.