2013 Phone Bill Fraud Prevention Checklist

Published by Telecom Association at BusinessPhoneNews.com

About This Checklist: This checklist is produced by Telecom Association ("TA"), a membership organization of 3,800 independent telecom solution partners and their technology vendors. The guide is published for business owners and managers to help them understand what kind of phone bill fraud their business is exposed to and how they can minimize risk.

How to Use This Checklist: Read about the different types of phone bill fraud and evaluate which types your business is exposed to. After identifying your major vulnerabilities take appropriate action to reduce risk and then educate your employees about their responsibilities to minimize phone bill fraud risk. Include content about "reducing phone bill fraud" with each new employee indoctrination and provide all employees with phone bill fraud refresher training once per year. If you need to be referred to a recommended phone phone bill fraud consultant please check our "partner" directory at BusinessPhoneNews.com or ask for a customized referal for you specific needs by sending a detailed email to Dan@BusinessPhonenews.com.

Overview

Phone bill fraud occurs when a phone company bills your firm for long distance phone calls that were made on your telephone equipment that you do not want to pay for because they are not authorized business phone calls. These phone calls can be made by strangers or your own employees. Owners of business phone call equipment must take necessary precautions to prevent phone bill fraud as the phone companies that bill you for the calls will not forgive the charges just because they were not authorized business calls.

As the cost of international calls comes down, many business owners are focusing on the losses they are suffering from the loss of paid employee time due to employees making unauthorized personal calls on company time.

Business owners need to understand that the phone and computer equipment that they provide to employees can be used to make phone calls over different phone company networks, both the networks that the business subscribes to and other networks that both employees or hackers can access using the company equipment but is not authorized to be used - but is not blocked from use.

Business owners will want to work with their phone equipment vendors to ensure that all alternate phone networks are blocked and no phone calls (or possibly any communications) can be made unless they are made over the authorized network that the business owner can track and record. In addition, owners will want to work with their authorized network providers to ensure that only certain types of phone calls can be completed.

Phone Call Fraud Prevention Checklist

1. **Know what sorts of phone calls your company normally makes and in what volume using both regular office phone systems, mobile phones and Internet "VoIP" phones.**

   The best way to do this is to review all telecommunications invoices and their related

Edited by Dan Baldwin, 951-251-5155, Dan@BusinessPhoneNews.com

contracts. The fine print must be examined to determine if all charges are flat-rate or usage sensitive. For any contracts that are usage sensitive, determine if there is a billing cap. If there is no cap work with your network provider to either install a cap or put a usage exception report in place so that abnormal monthly usage is quickly flagged.

2. **Understand if there are any ways to gain remote access to any of your phone equipment for the purpose of making direct or "transferred" phone calls.**

   Just because you do not use all your phone system's outward dialing abilities does not mean they don't exist or have been properly blocked. Many older business PBX phone systems are still DISA ("direct inward system access") enabled. DISA is a"calling card" PBX feature which allows outside employees to call a phone number that rings into the PBX and then get a second dial tone to then make an outbound call.

   Modern IP-PBXs use Internet VoIP technologies to allow remote, work at home employees to make calls through the main business phone system. These same systems have sophisticated auto-attendants and voice mail systems that allow callers to press a number to be connected to an employee's cell phone or home office number.

   Hackers look for both old and new phone systems that they can secretly access to setup a new voicemail box or auto-attendant option to clandestine callers. Once their hack is complete they turn around and sell "free calls to Russia" that will be paid for by the PBX owner at the end of the month.

3. **Understand what sorts of unauthorized calls that employees may be making or assisting others to make.**

   Once you understand all the different ways that anyone can make direct or "transferred" phone calls through your phone system you need to spend a little time thinking like a hacker or a disgruntled employee. Make a list of all the different sorts of unauthorized calls that can be made through a compromised phone system.

4. **Understand what resources are available to block unauthorized phone calls and how long it takes to block or unblock certain types of calls.**

   For most businesses, local and domestic outbound calls are all that need to be made for business purposes. All international calling can be blocked by either by the PBX or the contracted phone company. For most businesses the most secure route to blocking unauthorized and expensive calls is to simply have their phone company block all international calls. This prevents expensive calls even if the PBX is hacked. If some international countries do need to be called and the phone company can not block some countries and allow others then ask your PBX vendor if they can create a custom dialing plan that blocks international countries that do not need to be called.

5. **Understand what resources are available to track, measure and/or record phones calls.**

   If your phone company does not normally provide call detail records (CDRs) because of flat rate billing, ask if it is an option. If it is not an option, ask your PBX vendor what sort of call accounting packages or add-ons are available and if it includes recording of individual or all calls.

6. **Establish a company policy about what sorts of phone calls are authorized and if any or all business calls are to be recorded.**

Once you know what all the phone fraud risks are you can decide what steps you want to take to control or eliminate them. Be sure to publish the policy and review it regularly with your communication vendors to ensure that new threats are recognized and then incorporated into your company fraud prevention policy.

7. **Educate employees on a regular basis about company authorized phone call policy and the various ways that employees can assist with reducing fraudulent calls.**

   Ask your human resources department to include the training for all new hires and during any annual HR refresher courses that are required. Many employers feel that monitored employees are more productive. If this is indeed the case then it seems that the productivity comes from the employee fully understanding that all communications are monitored and/or recorded to prevent phone fraud.
8.

Recommended Phone System TA Partners & Vendors

The following TA partners and vendors are specifically recommended for their phone system design expertise and system integration solutions by business end-users that have selected them and then reviewed their performance within the past year. Listing are ranked by review points.

Phone System Selection Blog Updates

Recent phone system selection articles at TA's BusinessPhoneNews.com blog

Other Useful Resource Links

The following phone system selection resource links may help end users and consultants fine tune prospective bandwidth management solutions.

Comprehensive Mobile Phone Spy Software To monitor what employees do with company cell phones.

Call Monitoring Software Improves Your Overall Business Productivity Business phone systems recording solution

Workplace Privacy and Employee Monitoring What's legal and what's prohibited

Fraudulent Business Calls Telecom Security & Fraud Prevention Verizon resource pages

This Dad Got Hit With A $10,000 Bill For Letting His Kids Watch Netflix On The Road

What You Should Do Before Traveling Abroad With Your Cell Phone

Verizon Customer Racks Up $1,500 Cell Phone Bill In 12 Days

Edited by Dan Baldwin, 951-251-5155, Dan@BusinessPhoneNews.com

[How Telephone Companies Use 'Plain English' To Rob You Blind]

[PBX Fraud Prevention Tips]

[TelePacific Fraud Prevention Checklist]

Edited by Dan Baldwin, 951-251-5155, Dan@BusinessPhoneNews.com