Notice to our customers regarding Toll Fraud

- **Beware of Toll Fraud.**

- **Toll Fraud is a crime against you. Bizfon isn't responsible for your Toll Fraud.**

- **You need to take steps to protect yourself from Toll Fraud.**

- ***IMPORTANT*: INCIDENTS OF TOLL FRAUD INCREASE DURING THE YEAR-END / HOLIDAY SEASONS. READ THE FOLLOWING INFORMATION ABOUT TOLL FRAUD AND TAKE MEASURES TO REDUCE YOUR RISK**

What exactly is toll fraud?

"Toll fraud" is the unauthorized use of your phone lines, equipment, or services to make long distance calls that are charged to you. Toll fraud is an illegal activity similar to computer hacking. It is a global, industry-wide problem totaling over a billion dollars annually. Toll fraud takes many forms including fraud involving mobile phones, calling cards, pay phones, and long-distance fraud on calls placed through phone systems. It is a large enough problem that many of the major providers of long distance telephone service have a separate department specifically for identifying and handling toll fraud issues.

Historically, the primary target for toll fraud has been larger companies with expensive and powerful telephone systems. Smaller phone systems possessing much of the power of the larger phones systems are now available, making these systems potential targets. The BIZFON phone system has powerful features including call forwarding and remote access to qualified outside (remote) users. Passwords are not required to be used to access the BIZFON system, but they are required to gain access as a remote user (e.g. checking voicemail). If an unauthorized person obtains the password for an extension, they may be able to log into the system and make unauthorized phone calls to outside numbers or change the phone system's settings.

Understand your liability.

Under most long distance carrier agreements, if a call has originated with, or passed through a customers' equipment, that customer is 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. Learn how to prevent toll fraud because you have the final responsibility for securing both your BIZFON system and any networked equipment.

BIZFON DOES NOT WARRANT THAT ITS PRODUCTS ARE IMMUNE FROM OR WILL PREVENT TOLL FRAUD. BIZFON WILL NOT BE RESPONSIBLE FOR ANY CHARGES, LOSSES, OR DAMAGES THAT RESULT FROM TOLL FRAUD.

Plan ahead.

While a good security program will vastly reduce your risk, it cannot guarantee you won't be hit. Develop procedures to be followed if you suspect your system has been breached. Establish it now, because if you are hit, the toll meter may continue to run while you decide what to do.

Knowledge and prevention are your best defense.

BIZFON wants to arm you with as much information as possible to help you avoid toll fraud. These guidelines will not completely eliminate the risk, but they can help reduce your chances of becoming a victim of toll fraud.

If an incident of toll fraud is discovered:

1. **Take immediate steps to block remote access to your phone system. See the following paragraphs for suggestions. If you're having trouble making these changes, call BIZFON at 603-870-9400.**
2. **Contact your long-distance provider immediately.**
3. **Report the incident to your local police authority.**

While BIZFON is not responsible for toll fraud on your system, if you are a BIZFON owner, we will be happy to discuss what protective measures you can take and help you make any necessary changes to your system.

Here are two emergency techniques which could help should you find yourself the victim of toll fraud:

- **Technique 1. Unplug all of your telephone lines from the Bizfon 680 ports labeled "Incoming Telephone Lines". This should temporarily halt the toll fraud, and give you time to continue with the rest of the suggestions. Alternately, you could leave one phone line plugged in, as remotely forwarded calls through the Bizfon 680 require two phone lines. This would give you access to one phone line for calls. Now reset all extensions (no matter how many phones you have) one at a time to factory default through the General Settings. Don't forget to reset all of the Virtual Extensions including the 0 (Operator). If the "hacker" has made changes to your extension settings, this should remove them. Note that you will lose any extension voicemails and personal extension greetings, so you may want to clear out**

voicemails and write down the greetings first. When you set the extensions back up, make sure to follow the other suggestions in this document concerning the use of extension passwords.

- Technique 2. Unplugging the BIZFON 680 phone system's AC power will disconnect all calls and prevent anyone from dialing through the phone system. Since valid calls will also be unable to get through, you could temporarily wire around the system until the problem can be resolved by connecting the individual phone lines directly to BizTouch 1 or 2 or generic analog phonesets. An alternate temporary workaround after unplugging the 680's AC power would be to plug an analog phone into the emergency port on the Bizfon 680. This would give you the ability to use Line 1 only.

How could an unauthorized person gain access to your long-distance service?

There are many possibilities. Thieves or hackers can:

- **Break into your voice-mail system and take over mailboxes, and/or steal long distance by obtaining an outside line, or by programming mailboxes to accept third party billed calls.**
- **Use your Toll Free (800, 888, or 877) numbers and make calls that you didn't intend to or want to pay for.**
- **Call your office and guess easy passwords or con your employees into giving out passwords while posing as telephone company personnel. Once they have a password, they may gain access to your system. Please note that neither Bizfon employees nor telephone company employees have any need to ask for your passwords.**
- **Use your company calling card numbers to place international calls.**
- **Go through your trash - commonly known as 'dumpster diving' - searching for codes.**
- **Use your printed internal telephone directory to try & "recruit" your employees.**
- **Con your switchboard and reception staff into accepting collect calls or connecting them to long distance trunks - a technique known as "social engineering."**

- Bill international calls to your telephone number by employing a third number billing scam.
- "Shoulder surf" in airports or other public locations to obtain calling card or other access numbers and authorization codes by looking over callers' shoulders as they use them.

What are some warning signs that could indicate toll fraud?

- Calls (especially international) you don't recognize on your telephone bill.
- Warnings from your telephone company regarding unusual call activity not matching your typical call profile.
- Increases in calls after business hours.
- Phone lines in use for extended periods when no one else is on the phone (including valid remote users).
- Complaints by incoming callers getting busy signals or outside lines not being available when the office isn't using all the phone lines (can be caused by other issues like call forwarding settings, or lack of disconnect signals from the telephone service provider).

Secure your Systems.

Voice-mail systems:

- Either don't use any passwords (disables remote extension log-in), or assign and change passwords regularly.
- Increase password length, and prohibit the use of trivial, simple passwords such as 222 or 123 or extension numbers.
- Prohibit the sharing or posting of passwords, or entering them into programmable keys or speed dial buttons.
- Delete all inactive mailboxes.
- Restrict out-calling.

Long-distance calling (through your local/long-distance telephone service provider(s):

- Block all toll calls at night, on weekends and on holidays.

- Block or limit access to overseas calls. If your company has no requirement to call overseas, block overseas calls completely.
- Review carefully all billing information to identify unauthorized calling patterns.
- Block access codes to alternate long-distance carriers (10-10-220, etc.)

General Security Policies.

- Secure telephone equipment rooms and/or wiring frames, and allow access only to authorized personnel.
- Secure all system documentation, including manuals, configuration records and system printouts.
- Require positive ID checks from supplier staff and maintain an entry log.
- Delete a code immediately when an employee leaves your company, and do not reassign it to a new employee.
- Ensure cards and passwords are returned when an employee leaves your company.
- Keep telephone numbers private.
- Impress upon your staff that your telephone number plan must never be discussed outside the company.
- Eliminate the paper trail and foil "dumpster divers." Shred call detail reports and records and destroy obsolete internal telephone directories.
- Establish policies about the accepting of collect calls and providing access to outside lines.
- If you use cellular phones, never discuss or give out system access codes or calling card numbers over the cellular network.
- If you own a cellular phone, ensure that all calls billed to you were in fact made from your telephone. Thieves may "clone" or copy your phone and have their calls billed to you. To minimize the risk, keep your cellular phone off when not required.
- Protect your calling card number and PIN at all times. Retain in a secure place, or destroy the backing sheet to which your calling card is attached when it is mailed.
- When employees leave the company, cancel their calling card or change the PIN.

- When using your calling card in public, be aware that people near you may be "shoulder surfing" to observe the card information for their use.
- Never leave your calling cards unattended; protect them and keep them confidential; treat them like your personal credit cards.
- Review security procedures regularly.
- Always check your monthly statement.

Educate your staff.

- Brief your staff on security procedures and toll fraud detection regularly (i.e. warning signs, alarms).
- Warn staff about "shoulder surfing" and ensure they know who to notify if they believe their company calling card or access codes have been compromised.
- Warn switchboard operators, receptionists, and employees about "social engineering," i.e. con-artists impersonating security investigators, phone company installers, or telecom managers trying to obtain calling access or be transferred to an outside telephone line through your phone system.
- Establish procedures for staff to report suspected security breaches immediately.
- Establish procedures for calling cards or access codes that are misplaced, lost, stolen, or compromised.

Where can I find more information?

The foregoing information about toll fraud is also available on our website, http://www.bizfon.com. Check our website for updated information about toll fraud form time to time. You should also ask your long distance carrier about its policies related to toll fraud and prevention efforts. The following link is to the Federal Communication Commission's website with additional information about toll fraud: http://www.fcc.gov/cgb/consumerfacts/businesstfrd.html