ELCOTEL INC.

TELECOMMUNICATIONS SYSTEMS

December 18, 1989

Dear Elcotel Customer:

Many of you are quite aware of "Fraudulent Calling". A practice which has become widespread in the country, and a problem that no payphone owner is immune to.

Elcotel would like to put a halt to such calling practices by continuing to provide our customers with proper configurations, programming methods and security features. Therefore, we would like you to take an extra minute to familiarize yourself with the attached document that will describe certain set-ups to help prevent a fraudulent call from being placed.

To alert our Customers of certain fraud situations as they come to our attention, we also have available an electronic bulletin board called, "The Elcotel Troubleshooter". It can be accessed by our Customers via a personal computer equipped with a modem communications package. Both technical and marketing bulletins are available using this method.

Please contact Customer Service for fraud related questions, or if you would like to be entered into our electronic bulletin board database.

6428 Parkland Drive, Sarasota, Florida 34243

813-758-0389 • 800-ELCOTEL • FAX 813-755-1085

Marketing 813-751-7588 • Order Proc. 813-751-7580 • Customer Serv. 813-751-7585 • Purchasing 813-751-7590

PAYPHONE FRAUD AND SECURITY

OVERVIEW OF THE ISSUES.

Payphone fraud generally occurs when a free call (usually toll) is placed. The owner of the phone remains liable for the cost of the call and no revenue is received or billed for the call. Many fraud methods have been used from slugs to pocket dialers. Today, payphones block the known methods of fraud other than those committed by tapping onto the line. However, there are some current issues which are addressed in this document to insure that each phone is properly installed and programmed.

ORGANIZED GROUPS FIND AND COMMUNICATE FRAUD METHODS.

Some recent payphone fraud schemes have been traced to organized groups. The primary issue with organized groups is their communications distribution. When a new way to defraud phones is found, the speed and extent of disseminating the information results in rapid abuse. The fraud problem is industry wide. No one manufacturer, carrier, or system is singled out or overlooked.

WHAT CONTRIBUTES TO FRAUD.

There are factors which contribute to the possibility of frauding payphones. The payphone manufacturers are aware of these and provide as much protection as possible at the time of manufacture and in software up-dates. The key factors that make it possible to fraud payphones are discussed below.

PROPER CONFIGURATION OF THE PAYPHONE.

The proper configuration of the payphone normally inhibits attempts to fraud. However, the payphone must be configured correctly. Options designed to provide high security are overlooked at times. Also some of the more convenient options may be turned off to improve access security. Altering a macro for a call type should be by the manufacturer's direction as this can result in improper operation or in overriding the payphone's controls.

NOTIFICATION OF FRAUD.

When a new fraud method is discovered - notification is (1) by letter, (2) the "Elcotel Trouble Shooter" bulletin, and (3) posted on the Elcotel's "electronic bulletin board". This information may recommend payphone settings which prevent fraud and it should be followed. This information should be used to override the editor settings until a new PNM can be issued.

SECONDARY DIAL TONE / CHAIN DIALING.

Secondary dial tone represents a major opportunity for fraud. This secondary dial tone from the local central office can result in chain dialing. Chain dialing is possible when the called party goes on-hook and the caller remains off-hook. Dial tone is then returned from the central office. The caller enters digits for the next call and a free call is made. Payphones have total control of access in making the first call and dialing the called party. Disabling the keypad and monitoring for any touch tone signals injected into the mouthpiece after the destination number has been dialed will stop chain dialing.

However, today with answer machines, voice mail, and automated attendants, it is desirable to allow touch tone signaling to these devices after the destination number has been dialed.

This issue of allowing secondary signaling when secondary dial tone is returned is a major fraud opportunity. Wink and other methods deal with this and are discussed below.

HOW TO STOP CHAIN DIALING.

The best method to prevent chain dialing is for the central office not to return secondary dial tone. This product is not available to the private sector, even though the telcos use the feature for their equipment.

Wink is the next best method of stopping chain dialing, (assuming the keypad must be active after dialing the destination number). Wink is the term used for an interruption in loop current flow at the completion of a call. Most central offices will provide this short interruption in loop current and the payphone reliably interprets this signal, disables the keypad, and prevents chain dialing.

SET-UP TO STOP CHAIN DIALING.

Keypad is enabled until Wink is received at call termination.

Software 4.2.X and above:

- Keypad enabled after dialing destination - 145 ON.
- Wink Enabled - 126 ON.
  Closes keypad at Wink.

Later versions of software, 4.2.4 and 4.3.X have Wink width adjustments. See software release information or manuals for details.

INADEQUATE CALL SCREENING.

Inadequate call screening can result in charges to the payphone and no revenue collected. Screening can be provided by the LEC and to some extent the IXC. Not all locations or IXCs provide the same level of screening. The simplest test is to dial an 0+ call. When the operator asks, "How would you like to pay for this call?" Say "Bill it to this number". The operator will instruct the caller to dial 1 next time, however, the call is put through. Proper screening will stop this. In addition to 0+ calls, screening should include international 01+ calls, third party, and collect calls to the payphone.

FOR COMPLETE SET-UP INFORMATION, PLEASE CONSULT TECHNICAL MANUAL

10XXX DIALING AND NO SCREENING.

Dialing 10XXX to an IXC (Inter-Exchange Carrier) bypasses screening at the LEC if the IXC operator becomes involved. Payphone patron dialing of 10XXX-1+ must be blocked at the payphone. However, it may be necessary for the payphone to dial 10XXX-1+ to access the IXC for lowest cost routing of calls. In this case, the IXC should provide international call screening. Dialing 10XXX-0+ must also have screening to prevent billing to the originating phone. Dialing 10XXX-0+ appears to be a weak link. If the caller dials 10288-0+ and waits for the operator, it is very easy to bill the call to the payphone. Test calls must be made to ensure the correct Telco screening is being accepted.

ALLOWING 800 and 950 ACCESS TO IXC.

Allowing 800 and 950 access to IXC in locations with secondary dial tone can also present problems. This has to do with the ready tone returned to the caller when the IXC is reached. This tone is often dial tone, at which point the caller is to enter the destination or authorization number for the IXC use. This type of ready tone prevents the use of dial tone detection for terminating secondary touch tone signalling.

To allow touch tone signalling after 1-800 or 950 access to the IXC is fine in locations with no secondary dial tone. Locations that provide Wink can allow touch tone signalling even with secondary dial tone present. The Wink will close the keypad and prevent additional dialing. However, this type access presents a problem in locations with no Wink and secondary dial tone. For this IXC access, timed keypad control must be used if touch tone signalling is required in locations with no Wink and secondary dial tone. Timed control does not provide the same level of protection as Wink and should be used only when absolutely required by the site.

SET-UP FOR 1-800 and 950 IXC ACCESS AND NO WINK.

- o Keypad disabled - 145 OFF
- o OCC access through local call - 123 ON.
- o OCC keypad on at 1st ring back - 127 ON.
- o Macro 03 - must be used in place of Macro 02.

TAMPERING.

Another method of allowing free calls is by gaining access to a payphone and tamper with its operational configuration. While the possibility of "hacking" an entry in theory is possible, tamper fraud may come from ex-employees. The payphone can be secured with the use of high security access and limiting remote access to payphone control from touch tone phones.

SET-UP TO STOP TAMPERING.

- o High security on local voice telemetry - 135 ON.
  This requires an upper housing key and the owner by-pass code.
- o Remote voice telemetry off - 129 OFF.
  This prevents access to the payphone from a remote touch tone phone.
- o Change owner bypass code regularly - register 230.

FOR COMPLETE SET-UP INFORMATION, PLEASE CONSULT TECHNICAL MANUAL

IN SUMMARY

WHAT ARE THE BEST METHODS TO PREVENT FRAUD.

- o No secondary dial tone.
- o Call screening at the LEC and IXCs.
- o High security access features of the payphone.

OTHER PAYPHONE FRAUD AND SECURITY FEATURES.

There are many other security features built into the payphone that continually provide monitoring and protection. Obviously it would not be wise to detail all these features. However, here are a few security features and their function.

- o Access attempt limit to prevent hacking.
  The payphone ignores access when a number of unsuccessful attempts have been made to gain access to the payphone.
- o No back-door access.
  Back-doors are accesses in a product for the manufacturer. These are not present in Elcotel payphones after 4.2.0 software.
- o Monitor for dialing patterns after destination number.
  Even when secondary touch tone signalling is required the payphone monitors the signal for certain dialing combinations.
- o Remote telemetry password and protocol security.
  The modem access to the payphone uses passwords and a protocol. This combination will limit access to the payphone.
- o Local telemetry password.
  A separate and easily changed owner by-pass is required for local access to the payphone control.
- o High security access.
  High security for local access requires an upper housing key and the owner by-pass code to gain access.
- o Coin box collection bypass.
  Coin collector use a separate code when collecting the coin box. This reports the collection and amount without access to the payphone control. Available in 4.2.4 and above.