

System Security and Toll Fraud

B

Telecommunications fraud is the unauthorized use of another company's telecommunications service. This type of fraud has been in existence since the 1950's when AT&T first introduced Direct Distance Dialing (DDD).

Twenty years later, Remote Access became a target of individuals seeking unauthorized network access. Now, with the added capabilities of voice mail and automated attendant services, customer premises equipment-based toll fraud has expanded as a new type of communications abuse. With its subculture of "hackers" and "phreakers," telecommunications fraud has rapidly become a highly profitable criminal activity.

Protecting Your Voice Messaging System

Voice Messaging toll fraud has risen dramatically in recent years. Now more than ever, it is imperative that you take steps to secure your system. Securing your system means protecting both standard voice messaging and automated attendant applications.

Voice Messaging

There are two types of voice mail fraud. The first type occurs when a hacker takes over a mailbox and uses it to communicate with other hackers. This can be expensive if access is gained to the voice mail system via an 800 number. In this situation, a hacker typically hacks the mailbox password and changes it along with the greeting.

Once thieves transfer to dial tone, they may dial a Trunk Access Code (TAC), Feature Access Code (FAC), or extension number, which is the second type of

abuse. If the system is not properly secured, thieves can make fraudulent long distance calls or request a company employee to transfer them to a long distance number.

Automated Attendant

Auto attendants are used by many companies to augment or replace a switchboard operator. When an auto attendant answers, the caller is generally given several options. A typical greeting is: "Hello, you've reached XYZ Bank. Please enter 1 for Auto Loans, 2 for Home Mortgages. If you know the number of the person you are calling, please enter that now."

In some switches, button 9 is to access dial tone. In addition, when asked to enter an extension, the hacker enters 9180 or 9011. If the system is not properly configured, the auto attendant passes the call back to the PBX. The PBX reacts to 9 as a request for a dial tone. The 180 becomes the first numbers of a 1-809 call to the Dominican Republic. The 011 is treated as the first digits of an international call. The hacker then enters the remaining digits of the telephone number and the call is completed. You, the PBX owner, pay for it. This hacker scenario works the same way with a voice mail system.

Switch Administration

To minimize the risk of unauthorized people using the INTUITY™ AUDIX® system to make toll calls, administer your switch in any of the following ways.

Restrict Outward Dialing

The measures you can take to minimize the security risk of outcalling depend on how it is used. When outcalling is used only to alert on-premises subscribers who do not have AUDIX message indicator lamps on their telephones, you can assign an outward-restricted Class of Restrictions (COR) to the AUDIX voice ports.

Use P010 W3 F19 to assign outward restriction to the voice mail ports' Class of Service (COS).

Assign Low Facilities Restriction Level (FRL)

The switch treats all the PBX ports used by voice mail systems as stations. Therefore, each voice mail port can be assigned a COR/COS with an FRL associated with the COR/COS. FRLs provide eight different levels of restrictions for Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), or World Class Routing (WCR) calls. They are used in combination with calling permissions and routing patterns and/or preferences to determine where calls can be made. FRLs range from 0 to 7, with each number representing a different level of restriction (or no restrictions at all).

The FRL is used for the AAR/ARS/WCR feature to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the FRLs in the AAR/ARS/WCR routing pattern to the FRL associated with the COR/COS of the call originator.

The higher the FRL number, the greater the calling privileges. For example, when voice mail ports are assigned to a COR with an FRL of 0, outside calls are disallowed. If that is too restrictive, the voice mail ports can be assigned to a COR with an FRL that is higher, yet low enough to limit calls to the calling area needed.

⇒ NOTE:
Voice Messaging ports that are outward restricted via COR cannot use AAR/ARS/WCR trunks. Therefore, the FRL level doesn't matter since FRLs are not checked.

FRLs can be assigned to offer a range of calling areas. Choose the one that provides the most restricted calling area that is required.

[Table B-1](#) provides suggested FRL values.

Table B-1. Suggested Values for FRLs

FRL	Suggested Value
0	No outgoing (off-switch) calls permitted.
1	Allow local calls only; deny 0+ and 1-800 calls.
2	Allow local calls, 0+, and 1-800 calls.
3	Allow local calls plus calls on FX and WATS.brtrunks.
4	Allow calls within the home NPA.
5	Allow calls to certain destinations within the continental USA.
6	Allow calls throughout the continental USA.
7	Allow international calling. Assign attendant console FRL 7. Be aware, however, if Extension Number Portability is used, the originating endpoint is assigned FRL 7.

⇒ NOTE:
In [Table B-1](#), FRLs 1 through 7 include the capabilities of the lower FRLs. For example, FRL 3 allows private network trunk calls and local calls in addition to FX and WATS trunk calls.

To set FRLs on G2 and System 85:

- Use P010 W3 F23 to assign FRLs for use with AAR/ARS/WCR trunks. Assign higher FRLs to restricted patterns in P309 than the FRL in the COS for the voice mail ports.
- For G2.2, do not use P314 to mark disallowed destinations with a higher FRL value. P314 W1 assigns a Virtual Nodepoint Identifier (VNI) to the restricted dial string. P317 W2 maps the VNI to the pattern, and P317 W2 shows the pattern preference, with the FRL in field 4.

For earlier releases, use P313 to enter disallowed destinations in the Unauthorized Call Control table.

Restrict Toll Areas

For G2 and System 85:

- Use P311 W2 to establish 6-digit translation tables for foreign NPAs, and assign up to 10 different routing designators to each foreign NPA (area code).
- Use P311 W3 to map restricted and unrestricted exchanges to different routing designators.
- If the unrestricted toll exchanges are in the Home NPA, use P311 W1 to map them to a routing designator.
- If the Tenant Services feature is used, use P314 W1 to map routing designators to patterns. If Tenant Services is not used, the pattern number will be the same as the routing designator number.
- Use P309 W3 to define the restricted and unrestricted patterns. For G3:
- Use change ars analysis to display the ARS Analysis screen.
- Enter the area codes or telephone numbers that you want to allow and assign an available routing pattern to each of them.
- Use change routing pattern to give the pattern preference an FRL that is equal to or lower than the FRL of the voice mail ports.

For G2.2:

- Use P314 W1 to assign a Virtual Nodepoint Identifier (VNI) to the unrestricted dial string.

Map the VNI to a routing pattern in P317 W2, and assign a low FRL to the pattern in P318 W1. If you permit only certain numbers, consider using Network 3, which contains only those numbers.

Block Subscriber Use of Trunk Access Codes

Station-to-Trunk Restrictions can be assigned to disallow stations from dialing specific outside trunks. By implementing these restrictions, callers cannot transfer out of voice mail to an outside facility using Trunk Access Codes.

For G2 and System 85, if TACs are necessary for certain subscribers to allow direct dial access to specific facilities, such as tie trunks, use the Miscellaneous Trunk Restriction feature to deny access to

others. For those stations and all trunk-originated calls, always use ARS/AAR/WCR for outside calling.

⇒ NOTE:

Allowing TAC access to tie trunks on your switch may give the caller access to the Trunk Verification feature on the next switch.

Restrict AMIS Networking Number Ranges

To increase security for AMIS analog networking, including the Message Delivery service, restrict the number ranges that may be used to address messages. Be sure to assign all the appropriate PBX outgoing call restrictions on the AUDIX voice ports.

Subscriber Password Guidelines

To minimize the risk of unauthorized people accessing AUDIX subscriber mailboxes and using them for toll fraud, educate subscribers in the following guidelines for AUDIX passwords.

- When password protection into voice mailboxes is offered, require the maximum number of digits allowed, or a minimum of five digits. Also, be sure that the password length is at least one digit longer than the extension length.
- Make sure subscribers change the default password the first time they log in to the AUDIX system. To insure this, make the default password fewer digits than the minimum password length.
- Establish your password as soon as your AUDIX extension is assigned. This ensures that only YOU will have access to your mailbox, not anyone who enters your extension number and #. (The use of only the “#” indicates the lack of a password. This fact is well-known by telephone hackers.)
- Never have your greeting state that you will accept third party billed calls. A greeting like this allows unauthorized individuals to charge calls to your company. If you call someone at your company and get a greeting like this, point out the vulnerability to the person and recommend that they change the greeting immediately.

- Never use obvious or trivial passwords, such as your telephone extension, room number, employee identification number, social security number, or easily guessed numeric combinations (for example, 999999).
- Change administered default passwords immediately; never skip the password entry. Hackers find out defaults. To change your password, press 5 at the main AUDIX menu. Then press 4.
- Discourage the practice of writing down passwords, storing them, or sharing them with others. If a password needs to be written down, keep it in a secure place and never discard it while it is active.
- Never program passwords onto auto dial buttons.
- If you receive any strange AUDIX messages, or your greeting has been changed, or if for any reason you suspect that your AUDIX facilities are being used by someone else, contact Lucent Network Corporate Security.

INTUITY AUDIX Administration

To minimize the risk of unauthorized people using the INTUITY AUDIX system to make toll calls, you can administer the AUDIX system in any of the following ways.

Outcalling

When outcalling is used for subscribers who are off-site (often the message notification is forwarded to a call pager number), three options exist to minimize toll fraud: 1) the AUDIX voice ports can be assigned to a toll-restricted COR that allows calling only within a local area; 2) the outcalling numbers can be entered into an unrestricted calling list for either ARS or Toll Analysis, or 3) outcalling numbers can be limited to 7 or 10 digits.

- On the Subscriber form, turn off outcalling by using the proper COS for each subscriber.
- On the System Parameters Outcalling form, limit the number of digits that can be dialed for outcalling.



NOTE:

If outcalling is to a pager, additional digits may be required.

Mailbox Administration

- To block break-in attempts, allow a low number of consecutive unsuccessful attempts to log into a voice mailbox. Administer this on the System Parameters Features screen.
- Deactivate unassigned voice mailboxes. When an employee leaves the company, remove the subscriber and, if necessary, reassign the voice mailbox.

- Do not create voice mailboxes before they are needed.
- The INTUITY AUDIX system offers password and password time-out mechanisms that can help restrict unauthorized users. Subscribers can have passwords up to 15 digits for maximum security, and you can specify the minimum length required. Use a minimum of 5 digits, and a length at least one digit greater than the extension number length.

AUDIX callers are given three attempts in one call to correctly enter their mailbox before they are automatically disconnected. You can also specify how many consecutive invalid attempts are allowed before a voice mailbox is locked.

Enhanced Call Transfer

With Enhanced Call Transfer, the AUDIX system uses a digital control link message to initiate the transfer and the switch verifies that the requested destination is a valid station in the dial plan. With Enhanced Call Transfer, when AUDIX callers enter ☐ T followed by digits (or ☐ A for name addressing) and ☐ #, the following steps are performed:

1. The AUDIX system verifies that the digits entered contain the same number of digits as administered on the AUDIX system for extension lengths.

If call transfers are restricted to subscribers, the AUDIX system also verifies that the digits entered match the extension number for an administered subscriber.

NOTE:

When callers request a name addressing transfer, the name must match the name of an AUDIX subscriber (either local or remote) whose extension number is in the dial plan.

2. If Step 1 is successful, the AUDIX system sends a transfer control link message containing the digits to the switch. If Step 1 is unsuccessful, the AUDIX system plays an error message to the caller and prompts for another try.
3. The switch verifies that the digits entered match a valid extension in the dial plan.
 - If Step 3 is successful, the switch completes the transfer, disconnects the AUDIX voice port, and sends a "successful transfer" control link message to the AUDIX system.
 - If Step 3 is unsuccessful, the switch leaves the AUDIX voice port connected to the call, sends a "fail" control link message to the AUDIX system, and then the AUDIX system plays an error message requesting another try.

Coverage Limitations with Enhanced Call Transfer

With Enhanced Call Transfer, the reason for a transfer is included in the control link message that the AUDIX system sends to the switch. For Call Answer calls, such as calls that are redirected to the AUDIX system when an extension is busy or doesn't answer, when a caller enters **0** to Escape to Attendant, the AUDIX system normally reports the transfer to the switch as "redirected."

The switch uses this reason to determine how to proceed with the call. If the reason for the transfer is "redirected," the call will not follow the destination's coverage path or its call forwarding path. This is because the switch will not redirect a previously redirected call.

This restriction may not be acceptable where it is desirable to have the call follow the coverage path of the "transferred-to" station. Enhanced Call Transfer can be administered to allow this type of transfer.

Detecting Voice Mail Fraud

[Table B-2](#) shows the reports that help determine if your voice mail system is being used for fraudulent purposes.

Table B-2. Reports and Monitoring Techniques for the AUDIX system

Monitoring Technique	Switch
Call Detail Recording (SMDR)	All
Traffic Measurements and Performance	All
Automatic Circuit Assurance	All
Busy Verification	All
Call Traffic Report	All
Trunk Group Report	G1, G3, System 75
AUDIX Traffic Reports	All

Call Detail Recording

With Call Detail Recording activated for the incoming trunk groups, you can check the calls into your voice mail ports. A series of short holding times may indicate repeated attempts to enter voice mailbox passwords.



NOTE:

Most call accounting packages discard this valuable security information. If you are using a call accounting package, check to see if this information can be stored by making adjustments in the software. If it cannot be stored, be sure to check the raw data supplied by the CDR.

Review CDR for the following symptoms of voice messaging abuse:

- Short holding times on any trunk group where voice messaging is the originating endpoint or terminating endpoint
- Calls to international locations not normal for your business
- Calls to suspicious destinations
- Numerous calls to the same number
- Undefined account codes



NOTE:

Since CDR only records the last extension on the call, internal toll abusers transfer unauthorized calls to another extension before they disconnect so that the CDR does not track the originating station. If the transfer is to your voice messaging system, it could give a false indication that your voice messaging system is the source of the toll fraud.

For G2:

- Use P275 W1 F14 to turn on the CDR for incoming calls.
- Use P101 W1 F8 to specify the trunk groups.

Call Traffic Report

This report provides hourly port usage data and counts the number of calls originated by each port. By tracking normal traffic patterns, you can respond quickly if an unusually high volume of calls begins to appear, especially after business hours or during weekends, which might indicate hacker activity.

For G2 and System 85, traffic data is available via Monitor I which can store the data and analyze it over specified periods.

Trunk Group Report

This report tracks call traffic on trunk groups at hourly intervals. Since trunk traffic is fairly predictable, you can easily establish over time what is normal usage for each trunk group. Use this report to watch for abnormal traffic patterns, such as unusually high off-hour loading.

ARS Measurement Selection

The ARS Measurement Selection can monitor up to 20 routing patterns for traffic flow and usage.

Automatic Circuit Assurance

This monitoring technique detects a number of short holding time calls or a single long holding time call which may indicate hacker activity. Long holding times on Trunk-to-Trunk calls can be a warning sign. The ACA feature allows you to establish time limit thresholds defining what is considered a short holding time and a long holding time. When a violation occurs, a designated station is visually notified.

When an alarm occurs, determine if the call is still active. If toll fraud is suspected (for example, a long holding time alarm occurs on a Trunk-to-Trunk call), you may want to use the busy verification feature (see [“Busy Verification”](#) below) to monitor the call in progress.

For G2 and System 85:

- Use P285 W1 F5 and P286 W1 F1 to enable ACA systemwide.
- Use P120 W1 to set ACA call limits and number of calls thresholds.
- Choose the appropriate option:
 - To send the alarms and/or reports to a designated maintenance facility, use P497 W3.
 - To send the alarms and/or reports to an attendant, use P286 W1 F3.

Busy Verification

When toll fraud is suspected, you can interrupt the call on a specified trunk group and monitor the call in progress. Callers will hear a long tone to indicate the call is being monitored.

For G2 and System 85:

- Administer a Busy Verification button on the attendant console.
- To activate the feature, press the button and enter the trunk access code and the member number.

AUDIX Traffic Reports

The INTUITY AUDIX system tracks traffic data over various timespans. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, such as heavy call volume on ports assigned to outcalling, they can be investigated immediately. In addition, the AUDIX Administration and Data Acquisition Package (ADAP) uses a PC to provide extended storage and analysis capabilities for the traffic data. You can also use the AUDIX Administration Log and Activity Log to monitor usage and investigate possible break-in attempts.

Lucent Technologies's Statement of Direction

The telecommunications industry is faced with a significant and growing problem of theft of customer services. To aid in combating these crimes, Lucent Technologies intends to strengthen relationships with its customers and its support of law enforcement officials in apprehending and successfully prosecuting those responsible.

No telecommunications system can be entirely free from risk of unauthorized use. But diligent attention to system management and to security can reduce that risk considerably. Often, a tradeoff is required between reduced risk and ease of use and flexibility. Customers who use and administer their systems make this tradeoff decision. They know best how to tailor the system to meet their unique needs and, necessarily, are in the best position to protect the system from unauthorized use. Because the customer has ultimate control over the configuration and use of Lucent services and products it purchases, the customer properly bears responsibility for fraudulent uses of those services and products.

To help customers use and manage their systems in light of the tradeoff decisions they make and to ensure the greatest security possible, Lucent Technologies commits to the following:

- Lucent products and services will offer the widest range of options available in the industry to help customers secure their communications systems in ways consistent with their telecommunications needs.
- Lucent Technologies is committed to develop and offer services that, for a fee, reduce or eliminate customer liability for PBX toll fraud, provided the customer implements prescribed security requirements in its telecommunications systems.
- Lucent's product and service literature, marketing information and contractual documents will address, wherever practical, the security features of our offerings and their limitations, and the responsibility our customers have for preventing fraudulent use of their Lucent products and services.

- Lucent sales and service people will be the best informed in the industry on how to help customers manage their systems securely. In their continuing contacts with customers, they will provide the latest information on how to do that most effectively.
- Lucent Technologies will train its sales, installation and maintenance, and technical support people to focus customers on known toll fraud risks; to describe mechanisms that reduce those risks; to discuss the tradeoffs between enhanced security and diminished ease of use and flexibility; and to ensure that customers understand their role in the decision-making process and their corresponding financial responsibility for fraudulent use of their telecommunications system.
- Lucent Technologies will provide education programs for customers and our own people to keep them apprised of emerging technologies, trends, and options in the area of telecommunications fraud.
- As new fraudulent schemes develop, we will promptly initiate ways to impede those schemes, share our learning with our customers, and work with law enforcement officials to identify and prosecute fraudulent users whenever possible.

We are committed to meeting and exceeding our customers' expectations, and to providing services and products that are easy to use and are of high value. This fundamental principle drives our renewed assault on the fraudulent use by third parties of our customers' communications services and products.

Lucent Technologies Security Offerings

Lucent Technologies has developed a variety of offerings to assist in maximizing the security of your system. These offerings include:


- Security Audit Service of your installed systems
- Fraud Intervention Service
- Individualized Learning Program, a self-paced text that uses diagrams of system administration screens to help customers design security into their systems. The program also includes a videotape and the *BCS Products Security Handbook*.
- Call Accounting package that calls you when preset types and thresholds of calls are established.
- Remote Port Security Device that makes it difficult for computer hackers to access the remote maintenance ports
- Software that can identify the exact digits passed through the voice mail system.

For more information about these services, see the *BCS Products Security Handbook*.

**Lucent Technologies Toll Fraud Crisis
Intervention**

If you suspect you are being victimized by toll fraud or theft of service and need technical support or assistance, call the Lucent Technologies BCS Technical Service Center (TSC) immediately.

DEFINITY®/System 75/85 PBX Repair	800 242-2121
AUDIX Help Line	800 562-8349

 **NOTE:**
These services are available 24 hours a day, 365 days a year. Consultation charges may apply.

Lucent Technologies Corporate Security

Whether or not immediate support is required, please report all toll fraud incidents perpetrated on Lucent services to Lucent Corporate Security. In addition to recording the incident, Lucent Corporate Security is available for consultation on product issues, investigation support, law enforcement, and education programs.

