Security

A

Overview

No telecommunications system can be entirely free from risk of unauthorized use. However, diligent attention to system management and to security can reduce that risk considerable. Customers know best how to tailor the system to meet their unique needs and are therefore in the best position to protect the system from unauthorized use. Because the customer has the ultimate control over the configuration and use of the Lucent Technologies services and products it purchases, the customer properly bears responsibility for fraudulent uses of those services and products.

Lucent Technologies, however, is committed to help customers use and manage their system to ensure the greatest security possible.

This chapter highlights some of the things you can do to secure your messaging system against fraudulent use.

Purpose

The purpose of this chapter is to alert the customer to the dangers of telecommunications fraud. This chapter also provides some guidelines on how to administer a messaging system to prevent unauthorized use. For a complete discussion, see the *BCS Products Security Handbook*, 555-025-600.

Protecting Your Voice/Fax 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. This means protecting your standard voice messaging and automated attendant applications.

NOTE:
No security issues exist that are unique to fax messaging. Voice messaging security issues generally apply also to fax messaging.

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. Typically a hacker hacks the mailbox password and changes both it and 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 used 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 phone 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.

MERLIN LEGEND Switch Administration

The measures you can take to minimize the security risk of owning a telecommunications system depend on how the telecommunications system is used and how any associated voice messaging or automated attendant system is used.

To minimize the risk of unauthorized persons using the voice messaging or automated attendant systems to make toll calls, administer the voice ports on your switch in any of the following ways:

Restrict Outward Dialing

A voice port with outward restriction cannot make *any* outside calls unless an allowed number list is used for specific area codes and/or exchanges that can be called. Outward restriction prevents or limits outcalling and AMIS networking.

Restrict Toll Areas

A voice port with toll restriction cannot make toll calls, but it can still make local calls. Toll restriction may prevent or limit outcalling and AMIS networking. An allowed number list can be used for specific area codes and/or exchanges that can be called.

Create Disallowed Number Lists

When a voice port is unrestricted, or has no toll restriction, a disallowed number list can be used to prevent calls to specific numbers, specific exchanges within all area codes, or specific numbers. There can be a maximum of eight disallowed lists in the MERLIN LEGEND system with a maximum of ten numbers on each list. Each voice port can be assigned any or all of the disallowed number lists.

Create Allowed Number Lists

When a voice port is outward or toll restricted, an allowed number list can be used to allow calls to specific area codes and/or exchanges. When outcalling or AMIS networking is required, using outward or toll restriction in combination with an allowed number list limits the risk of unauthorized persons using the voice messaging or automated attendant systems to make toll calls because calls can only be made to the specified area codes and/or exchanges. There can be a maximum of eight allowed lists in the MERLIN LEGEND system with a maximum of ten numbers on each list. Each voice port can be assigned any or all of the allowed number lists.

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. If possible, also place outward or toll restriction on the voice ports and use an allowed number list.

Switch Administration

To minimize the risk of unauthorized people using the 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 phones, you can assign an outward-restricted Class of Restrictions (COR) to the AUDIX voice ports.

For G1, G3, and System 75:

- Use **change cor** to display the Class of Restriction screen, and then create an outward restricted COR by entering **outward** in the Calling Party Restriction field.
- Assign the outward restricted COR to the voice ports.

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 A-1 provides suggested FRL values.

Table A-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 trunks.
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 A-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 G1, G3 and System 75:

- Use **change cor** for the voice mail ports (vs. subscribers) to display the Class of Restriction screen.
- Enter the FRL number (**0** through **7**) in the FRL field. Assign the lowest FRL that will meet the outcalling requirements. The route patterns for restricted calling areas should have a higher FRL assigned to the trunk groups.
- Use **change route-pattern** to display the Route Pattern screen.
- Use a separate partition group for ARS on the outcalling ports and limit the numbers that can be called.

NOTE:

For G3, the Restricted Call List on the Toll Analysis Table can also be used to restrict calls to specified areas.

Restrict Toll Areas

A reverse strategy to preventing calls is to allow outbound calls only to certain numbers. For G1 and System 75, you must specify both the area code and the office code of the allowable numbers. For G3, you can specify the area code or telephone number of calls you allow.

For G1 and System 75:

- Use **change ars fnpa xxx** to display the ARS Foreign Numbering Plan Area (FNPA) Table, where **xxx** is the NPA that will have some unrestricted exchanges.
- Route the NPA to a Remote Home Numbering Plan Area (RHNPA) table (for example, **r1**).
- Use **change rhnpa r1:xxx** to route unrestricted exchanges to a pattern choice with an FRL equal to or lower than the originating FRL of the voice mail ports.
- If the unrestricted exchanges are in the Home NPA, and the Home NPA routes to **h** on the FNPA Table, use **change hnpa xxx** to route unrestricted exchanges to a pattern with a low FRL.

  NOTE:
  If assigning a low FRL to a pattern preference conflicts with requirements for other callers, use ARS partitioning to establish separate FNPA/HNPA/RHNPA tables for the voice mail ports.

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.

NOTE:
For G3, the Unrestricted Call List (UCL) on the Toll Analysis Table can be used to allow calls to specified numbers through ARS/WCR. The COR for the voice mail ports should show “all-toll” restriction and access to at least one UCL.

Create Restricted Number Lists (G1, G3, and System 75 Only)

The Toll Analysis screen allows you to specify the toll calls you want to assign to a restricted call list (for example, 900 numbers) or to an unrestricted call list (for example, an outcalling number to a call pager). Call lists can be specified for CO/FX/WATS, TAC, and ARS calls, but not for tie TAC or AAR calls.

Create Allowed and Disallowed Number Lists (MERLIN LEGEND Only)

When a voice port is unrestricted or toll restricted, you can prevent (disallow) calls to specific numbers or exchanges within area codes. If a voice port is outward or toll restricted, you can list the specific area codes or exchanges subscribers are allowed to call. Refer to Appendix A in *Intuity AUDIX Integration with MERLIN LEGEND*, 585-310-231, for complete MERLIN LEGEND security information.

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. The password length should be 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.
- Administer Password Aging on the System Parameters Features screen. Password Aging requires subscribers to change their password at an interval defined by the system administrator. Password Aging enhances overall system security and helps protect against toll fraud by making the INTUITY AUDIX system less vulnerable to break-ins.
- Create your own 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, then enters $\boxed{\#}$. (The use of only a , indicating the lack of a password, is well-known by telephone hackers.)
- Never have your greeting state that you will accept third party billed calls (this allows unauthorized individuals to charge calls to your company). If someone at your company has a greeting like this, point out the vulnerability to the person and recommend they change the greeting immediately.

- Never use obvious or trivial passwords, such as your phone 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 $\boxed{5}$ at the main AUDIX menu. Then press $\boxed{4}$.
- 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.

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 profile 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 subscribers. 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.

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 to a pager is allowed, additional digits may be required.

Basic Call Transfer (5ESS, DMS-100, MERLIN LEGEND, and Non-Lucent Switches)

With Basic Call Transfer, after an AUDIX caller enters $\boxed{*}$ + $\boxed{T}$, the AUDIX system does the following:

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.

2. If step 1 is successful, the AUDIX system performs a switch-hook flash, putting the caller on hold.

   NOTE:
   If step 1 is unsuccessful, the AUDIX system plays an error message and prompts the caller for another try.

3. The AUDIX system sends the digits to the switch.
4. The AUDIX system completes the transfer.

With Basic Call Transfer, a caller can dial any number, provided the number of digits matches the length of a valid extension. So, if an unauthorized caller dials an access code followed by the first digits of a long-distance telephone number, such as $\boxed{9}$ $\boxed{1}$ $\boxed{8}$ $\boxed{0}$ $\boxed{9}$, the AUDIX system passes the numbers on to the switch. (This example shows a 5-digit plan.) The switch interprets the first digit ($\boxed{9}$) as an access code, and the following digits as the prefix digit and area code. The caller then enters the remaining digits of the phone number to complete the call.

If call transfers are restricted to subscribers, a caller cannot initiate a transfer to an off-premises destination unless the digits entered match an administered subscriber’s mailbox identifier (for example, 91809). To ensure the integrity of the “subscriber” restriction, do not administer mailboxes that start with the same digit(s) as a valid switch trunk access code.

Enhanced Call Transfer (System 75, G1, G3)

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.

Intuity AUDIX FAX Messaging

No fax-specific security issues exist. However, since Intuity AUDIX FAX Messaging requires that AMIS Analog Networking be turned on, be sure that outgoing AUDIX voice ports have the appropriate PBX calling restrictions

Detecting Voice Mail Fraud

Table A-1 shows the reports that help determine if your voice mail system is being used for fraudulent purposes.

Monitoring Technique	Switch
Call Detail Recording (or 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*

* MERLIN LEGEND supports only these monitoring techniques

Call Detail Recording (or SMDR)

With Call Detail Recording (CDR) activated for the incoming trunk groups, you can find out details about the calls made into your voice mail ports. This feature is known as Station Message Detail Recording (SMDR) on some switches including MERLIN LEGEND.

NOTE:
Lucent’s optional Call Accounting System (CAS) may be installed on the Intuity AUDIX system, allowing you to create customized reports with your G1, G3, or MERLIN LEGEND CDR/SMDR data. The optional Lucent Hacker Tracker program works in conjunction with CAS Plus Version 3 to alert you to abnormal calling activities. Call 800 521-7872 for more information.

Most other call accounting packages discard 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 normally used by your business
- Calls to suspicious destinations
- Numerous calls to the same number

- Undefined account codes

For G1, G3, and System 75:

- Use **change system-parameters features** to display the Features-Related System Parameters screen.
- Administer the appropriate format to collect the most information. The format depends on the capabilities of your CDR analyzing and recording device.
- Use **change trunk-group** to display the Trunk Group screen.
- Enter **y** in the SMDR/CDR Reports field.

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 G1, G3, and System 75, traffic data reports are maintained for the last hour and the peak hour.

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.

SAT, Manager I, and G3-MT Reporting

Traffic reporting capabilities are built-in and are obtained through the System Administrator Tool (SAT), Manager I, and G3-MT terminals. These programs track and record the usage of hardware and software features. The measurements include peg counts (number of times ports are accessed) and call duration. Traffic measurements are maintained constantly and are available on demand. However, reports are not archived and should therefore be printed to monitor a history of traffic patterns.

For G1, G3, and System 75:

- To record traffic measurements:
  - — Use **change trunk-group** to display the Trunk Group screen.
  - — In the Measured field, enter **both** if you have a Basic Call Management System (BCMS) and a Call Management System (CMS), **internal** if you have only BCMS, or **external** if you have only CMS.
- To review the traffic measurements, use **list measurements** followed by a measurement type (**trunk-groups, call-rate, call-summary**, or **outage-trunk**) and timeframe (**yesterday-peak, today-peak**, or **arrestor**).
- To review performance, use **list performance** followed by a performance type (**summary** or **trunk-group**) and timeframe (**yesterday** or **today**).

ARS Measurement Selection

The ARS Measurement Selection can monitor up to 20 routing patterns (25 for G3) for traffic flow and usage.

For G1, G3, and System 75:

- Use **change ars meas-selection** to choose the routing patterns you want to track.
- Use **list measurements route-pattern** followed by the timeframe (**yesterday, today**, or **last-hour**) to review the measurements.

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 set 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 that follows) to monitor the call in progress.

For G1, G3, and System 75:

- Use **change system-parameters features** to display the Features-Related System Parameters screen.
- Enter **y** in the Automatic Circuit Assurance (ACA) Enabled field.
- Enter **local**, **primary**, or **remote** in the ACA Referral Calls field. If **primary** is selected, calls can be received from other switches. **Remote** applies if the PBX being administered is a DCS node, perhaps unattended, where ACA referral calls go to an extension or console at another DCS node.
- Use **change trunk group** to display the Trunk Group screen.
- Enter **y** in the ACA Assignment field.
- Establish short and long holding times. The defaults are 10 seconds (short holding time) and one hour (long holding time).
- To review, use **list measurements aca.**

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 G1, G3, and System 75:

- Use **change station** to display the Station screen for the station that will be assigned the Busy Verification button.
- In the Feature Button Assignment field, enter **verify**.
- To activate the feature, press the **Verify** button and then enter the trunk access code and member number to be monitored.

AUDIX Traffic Reports

The INTUITY AUDIX system tracks traffic data over various time spans. 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'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 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. However, diligent attention to system management and to security can reduce that risk considerably. Often, a trade-off is required between reduced risk and ease of use and flexibility. Customers who use and administer their systems make this trade-off decision. They know best how to tailor the system to meet their unique needs and are therefore 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 trade-off decisions they make and to ensure the greatest security possible, Lucent 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 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 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 trade-offs 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 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 subscribers 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 Security Offerings

Lucent 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,* 555-025-600.

Lucent 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 one of the following numbers immediately.

DEFINITY/System 75/System 85 — Lucent BCS Technical Service Center (TSC)	800 242-2121
MERLIN LEGEND — Lucent BCS National Service Assistance Center (NSAC)	800 628-2888
Lucent Corporate Network Security	800 821-8235
AUDIX Help Line	800 562-8349

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

Lucent 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.