

System Security and Toll Fraud



Telecommunications fraud is the unauthorized use of another company's telecommunications service. This type of fraud has been in existence since the 1950's with the introduction of 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 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. Callers into the voice messaging/automated attendant system may transfer to an outgoing trunk if adequate security measures are not implemented. Callers who have unauthorized access to a voice mailbox can use it as a message drop for communications at your expense on your 800 numbers. Securing your system means protecting the switch, protecting the voice messaging system, and protecting any automated attendant applications.

Switch Security

The only tool a criminal needs to breach an inadequately secured system is a touch-tone telephone. If criminals can gain access to an inside dial tone, they will attempt to gain access to an outside line by using normal switch functions such as:

- Automatic Routing System (ARS) access codes
- Pool Access Codes

Security Tips

To help prevent toll fraud at the switch, follow these guidelines:

- Assign toll restrictions to voice messaging system and automated attendant ports.
- If you do not to use the outcalling features of the voice messaging system, restrict the outward calling capability of all voice ports.
- Use a dial plan that does not allow extensions beginning with the same digits as ARS, TAC, or verification and test codes.
- Inform all system operators that they are not to dial outside calls. Request that operators report all attempts to bypass switch restrictions to the telecommunications department for repairs or to the corporate security office for investigation.
- Restrict the numbers for outcalling and AMIS with a disallowed list.

Voice Messaging System Security

With regard to toll fraud, voice messaging systems have two areas of weakness:

- Codes that transfer to inside or outside dial tone
- Mailboxes that can be used as message drops

Once thieves transfer to inside dial tone, they have access to any unprotected switch features. Preventing this type of abuse requires security at both the switch and at the voice messaging system.

Once thieves break into a mailbox, they can use it as a message drop for untraceable calls or for illegal activities. If you have 800 lines that can connect to your voice messaging system, they can use them to pass stolen information around at your expense. If you have user-administrable outcalling, they can pass stolen information around at your expense automatically. Preventing this type of abuse requires security at the voice messaging system and on the part of your subscribers.

- Cellular telephones can be monitored. If a subscriber enters a mailbox number and a password on a cellular telephone, the mailbox number and the password will be known to anyone listening.
- To break a password, every word in a computerized 100,000 word-processor spelling checker or dictionary can be tried in just a few minutes. In a slightly longer time, every digit combination from 1 to 100,000 can be tried.

Security Tips

To help prevent toll fraud at the voice messaging system, follow these guidelines:

- Do not create voice mailboxes before they are needed.
- Deactivate unassigned mailboxes. When an employee leaves the company, close or reassign the mailbox.

- Do not have permanent “guest” mailboxes (mailboxes without a physical extension that are loaned to outsiders for the duration of a project). If you need a guest mailbox, assign it when it is needed and deactivate or change its password immediately after it is no longer needed. Do not reassign a guest mailbox without changing the password.
- Lock out multiple unsuccessful attempts to enter a voice mailbox on a single call. (Allow no more than two or three attempts on the same call.)
- Do not use default initial passwords that follow any scheme. Have a list of random passwords and select one when you create the mailbox. Require that the mailbox owner personally appear at the corporate security office or telecommunications office to obtain the initial password. Go over the subscriber password guidelines with the subscriber when you give out the initial password.
- Make sure subscribers change the initial password the first time they log in to the INTUITY AUDIX LX system by making the initial password shorter than the minimum password length.
- Use the password-aging feature so that users must change their passwords monthly.
- Discourage the practice of writing down passwords, storing them, or sharing them with others.
- Restrict the use of outcalling to personnel who actually need it.
- Restrict the number of digits that can be used for outcalling to seven or ten if possible. (Outcalling to pagers may require more.)
- Inform all system operators that they are not to dial outside calls. Request that operators report all attempts to bypass switch restrictions to the telecommunications department for repairs or to the corporate security office for investigation.
- Inform users that programming passwords onto auto-dial buttons is a breach of corporate security.
- Inform employees on how to report suspected toll fraud to the corporate security office.
- Monitor call detail recording (SMDR) reports, call traffic reports, INTUITY AUDIX LX traffic reports, and other available reports regularly.

Automated Attendant System Security

Automated attendants are used by many companies to augment or replace a switchboard operator. When an automated attendant answers, the caller is generally given several options that are appropriate to the company's business.

- There may be other unstated options such as a code for dial tone or a code for transfers that allow criminals to access unanticipated parts of the telecommunications system.

- Pressing ☐, ☐ 7 (☐, ☐ T) will cause a transfer from the automated attendant to the voice messaging service.
- Even anticipated transfers may cause problems if they are not well thought out.
- Naive operators may dial an outside call for someone who has dialed 0 and complains of trouble making a call.

In some automated attendant systems, option ☐ 9 is to access dial tone.

Security Tips

To help prevent toll fraud at the automated attendant, follow these guidelines:

- Do not allow transfers to inside or outside dial tone.
- Restrict transfers to subscribers only.
- Inform all system operators that they are not to dial outside calls. Request that operators report all attempts to bypass switch restrictions to the telecommunications department for repairs or to the corporate security office for investigation.
- Inform employees on how to report suspected toll fraud to the System Administrator.
- Monitor call detail recording (SMDR) reports, call traffic reports, INTUITY AUDIX LX traffic reports, and other available reports regularly.

Password Guidelines

To minimize the risk of unauthorized persons accessing subscriber mailboxes and using them for toll fraud, inform all system users of these guidelines for voice messaging system passwords.

- Mailbox passwords are required.
- Require that passwords be as long as feasible, with a minimum of five digits, and a length that is at least one digit longer than the maximum extension length.
- System users must change the initial password the first time they log in to the voice messaging system. To ensure this, the initial password should have fewer digits than the minimum password length.
- Never have greetings that state you will accept third party billed calls. A greeting like this allows unauthorized individuals to charge calls to your company. If a user calls somebody within the company and receives a greeting like this, they should 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 the birthday of any family member. Also avoid easily guessed numeric combinations such as [1], [3], [9], [7] and [2], [4], [8], [6] (geometric pattern on the dial), [9], [9], [9], [9], [9], [9] (repeated digits), and [7], [2], [7], [7], [9], [6], [7], [3] ("password" spelled out on the dial).
- Passwords should not be written down, stored, or shared with others.
- Passwords must not be programmed into auto-dial buttons. Violation will result in an entry in the employees permanent personnel record.
- If subscribers receive any strange voice mail messages, find that their greeting or password has been changed, or suspect for any reason that their voice mailbox is being used by someone else, they should contact the System Administrator immediately.

Switch Administration

The measures you can take to minimize the security risk of owning a telecommunications system depend on how the telecommunications system and 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 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/MAGIX 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/MAGIX 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.

INTUITY AUDIX LX Administration

To minimize the risk of unauthorized persons using the Intuity AUDIX LX system to make toll calls, administer the Intuity AUDIX LX system in any of the following ways:

Outcalling

Outcalling uses the voice messaging ports. If mailbox security is broken, unauthorized persons can use outcalling to transfer messages at your expense. If you need outcalling, restrict it as far as possible to eliminate the possibilities for theft of services.

- Do not enable outcalling at all if you do not need it.
- Do not enable outcalling for subscribers who do not need it.
- If outcalling is used only to ring in-house telephones that do not have message waiting lamps, restrict the number of digits to the maximum length of extensions.
- If possible, restrict outcalling to the local area (7 digits) or North America (10 digits).
- If outcalling must be allowed to pagers, use pagers that have individual DID numbers so that pager identification digits are not required and restrict any additional digits for caller identification to the minimum possible.
- If a limited number of pagers are in use, consider putting the pager numbers on an unrestricted calling list so that outcalling can be effectively limited to only those numbers.

Mailbox Administration

The use of Intuity AUDIX LX system security features in combination with mailbox administration can help reduce the risk of unauthorized use of mailboxes.

- Use the longest feasible password length. The Intuity AUDIX LX system allows passwords up to 15 digits, and you can specify the minimum number of digits required. Use a minimum of five digits, and a length at least one digit longer than the extension number.

- Lock out multiple consecutive attempts to enter a voice mailbox. The Intuity AUDIX LX system has a password time-out feature that allows callers three attempts in one call to correctly enter their password before they are automatically disconnected. You can also specify how many consecutive invalid attempts are allowed before a voice mailbox is locked.
- Deactivate unassigned voice mailboxes. When an employee leaves the company, close or reassign the voice mailbox.
- Do not create voice mailboxes before they are needed.
- Avoid or closely monitor the use of “guest” mailboxes.

Basic Call Transfer

With Basic Call Transfer, when a caller enters *, , the Intuity AUDIX LX system processes the call as follows:

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

If call transfers are restricted to system users, the Intuity AUDIX LX system also verifies that the digits entered match the extension number for an administered user.

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

NOTE:

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

3. The Intuity AUDIX LX system sends the digits to the switch.
4. The Intuity AUDIX LX 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. If an unauthorized caller dials 9x11 (where “x” is 1 through 9), the call may go outside. Therefore extension numbers of the form 9x11 should not be used for mailboxes or for system users.

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

Detecting Toll Fraud

Some of the Intuity AUDIX LX system reports are valuable in determining if your voice messaging or automated attendant systems are being used for fraudulent purposes.

Call Detail Recording

With Station Message Detail Recording (SMDR) activated for incoming calls, you can check the calls in to your voice mail ports. A series of short holding times may indicate repeated attempts to enter voice mailbox passwords.

Review SMDR reports for the following symptoms of voice messaging abuse:

- Short holding times on calls where voice messaging is the originating 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:

The MERLIN LEGEND/MAGIX system only records the last extension on the call. Internal toll abusers transfer unauthorized calls to another extension before they disconnect so that the SMDR 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.

Review the Call Accounting System (CAS) and HackerTracker documentation on how to use SMDR reports.

Intuity AUDIX LX Traffic Reports

The Intuity AUDIX LX 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 Data Acquisition Package (ADAP) uses an external PC (running MS-DOS) 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.

Avaya Inc. 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, Avaya 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 Avaya 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, Avaya commits to the following:

- Avaya 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.
- Avaya 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.
- Avaya'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 Avaya products and services.
- Avaya 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.
- Avaya 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.

- Avaya 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 customer's 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.

Avaya's Security Offerings

Avaya 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 *GBCS 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 *Avaya Products Security Handbook*.

Avaya 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 Avaya National Service Assistance Center (NSAC) immediately.

MERLIN LEGEND/MAGIX Communications System Repair (NSAC)	800 628-2888
AUDIX Help Line	800 562-8349

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

Avaya Corporate Security

Whether or not immediate support is required, please report all toll fraud incidents perpetrated on Avaya services to Avaya Technologies National Service Assistance Center (NSAC) at 800-288-2888. In addition to recording the incident, Avaya services are available for consultation on product issues, investigative support, law enforcement, and education programs.