

**Asst. Director of U.S. Secret Service  
(Office of Investigations)**

**Deputy Special Agent in Charge, U.S.S.S.  
Special Services Director**

**Director, Technical Security, MCI**

**Director, Information Security, IBM**

**Deputy Chief Counsel, U.S. Secret Service**

**Network Development Engineer, MCI**

**Asst. Director FBI (Intelligence Div.)**

**Director of Investigations, MCI**

**Corporate Industrial Hygienist, PEPCO**

**V.P. Systems Integrity, MCI**

**Network Systems Planning Engineer, MCI**

**Chief, Superfund Site Investigations Section, EPA**

**Director, Federal Systems Div. Security, IBM**

**Director, Security & Safety,**

**Special Assistant, U.S. Attorney, U.S. Dept. of Justice**



## **A Wealth of Experience**

Members of the MCI Systems Integrity team draw upon key skills and experience derived from a wide variety of previous positions, as well as that gained in *advanced training and on the job.*

This multi-disciplinary team is built on the experience and skills of systems analysts, engineers, safety officers, security experts and former law enforcement officials, investigators and prosecutors. Operating nationwide, they use every possible means to prevent or minimize a wide range of potential business problems such as telecommunications fraud, information protection, physical security and environmental issues.

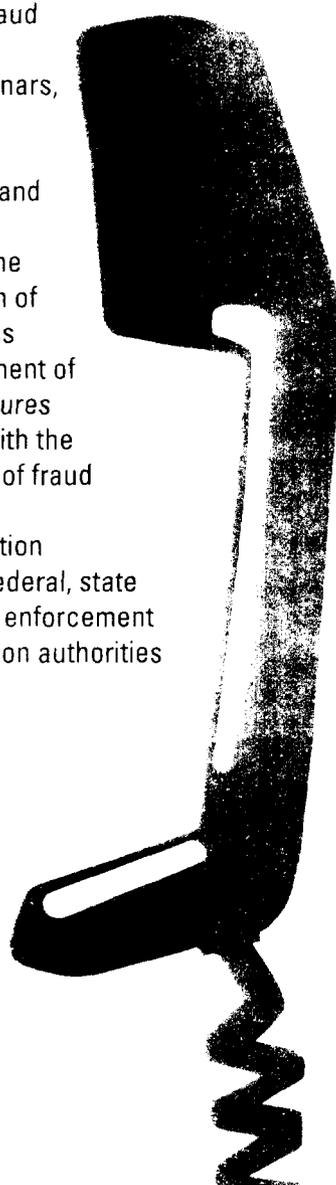
As appropriate, the talent, knowledge and experience of the MCI Systems Integrity team is available to support certain customer efforts in these areas. We will share our considerable experience, assist in minimizing fraud, and offer consultative support to help establish or enhance customer programs. Our team is ready to be a part of your team.



## Telecommunication Fraud Prevention

This is a major focus of the MCI Systems Integrity Customer Support program. Efforts are aimed at preventing or reducing the costs of fraud occurring through the abuse of CPE equipment and calling cards.

Steps range from prevention of unauthorized access to identification of fraud perpetrators and include:

- the evaluation, selection and/or recommendation of access control and monitoring equipment and systems
  - development of MCI network-based fraud prevention, detection and control systems
  - increasing fraud awareness through seminars, literature, publicity, consultation and other steps
  - assisting in the determination of fraud methods and development of countermeasures
  - assistance with the identification of fraud perpetrators
  - risk identification
  - liaison with federal, state and local law enforcement and prosecution authorities
- 

## Information Security

Many of the steps needed for the prevention of telecommunications fraud are also used in information security, particularly security for electronically transmitted or stored information. The Systems Integrity group has expertise in the protection of data, text, voice, image and materials which may be in use, storage or transit that contain proprietary information.

In addition to many of the steps listed under telecommunications fraud, the MCI Systems Integrity group offers experience in these and other areas:

- electronic and physical access controls and monitoring
- computer virus prevention and detection
- disaster recovery
- security organization and planning
- employee, vendor and consultant security issues

## Physical Security

The Systems Integrity group also has expertise in the physical security of corporate personnel and property. Certain of these skills may also relate to telecommunications fraud control.

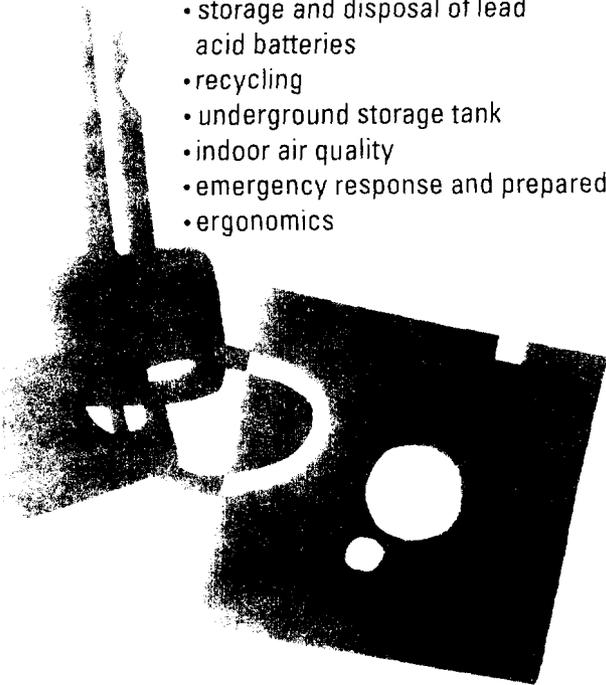
- officers and electronic monitoring systems
  - key control
  - electronic and physical access management
  - crisis management and executive protection
  - threats and/or acts of violence
  - fire and safety training
- 



## Environmental Program

MCI has experience in addressing a wide area of environmental compliance issues. Among these are:

- compliance, evaluation, training and awareness program
- hazardous materials management
- storage and disposal of lead acid batteries
- recycling
- underground storage tank
- indoor air quality
- emergency response and preparedness
- ergonomics

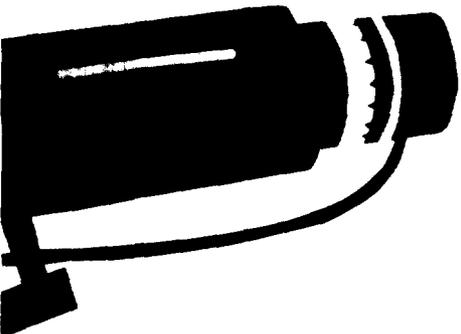


## Available Through Your MCI Representative

The services of the MCI Systems Integrity Customer Support Program are available to MCI customers at no cost or on an actual expense basis. They are offered by MCI to supplement and support customer telecommunications fraud control and related programs on a resource as available basis.

Discuss your needs with your MCI Representative.

MCI stands ready to work with you.



Since 1988, MCI has operated a highly sophisticated Corporate Systems Integrity Organization. Its mission... to insure that the telecommunications networks of MCI and its customers are as free as possible from unauthorized access and fraud... to protect against loss or damage to corporate information and records... to maintain the physical security of properties, equipment and personnel... and to insure compliance with environmental and safety standards.

The MCI logo consists of the letters "MCI" in a bold, sans-serif font. A horizontal line is positioned above the "M" and "C", extending from the left side of the "M" to the right side of the "C".

**MCI**

have been put in place. They will also enable out-dialing features that do not normally exist on the PBX. These situations can be difficult to detect. Hackers have been known to change the system at 8:00 pm to allow fraud calls. Then, at 3:00 am the next morning, they re-program the system back to its original configuration. A telecom manager who reviews the configuration in the morning will not be looking at the configuration that was abused. This can lead to delays in resolving the abuse.

#### **FRAUD SOLUTION(S):**

To solve this problem a Security Access Unit (SAU) should be placed in front of the maintenance port. SAUs provide another level of user ID and password protection. This ID and password should be controlled by the PBX owner and not any vendor. In addition, SAUs can be set up to further validate a user via callback or various token devices. While somewhat expensive, there are products which use voice validation for authentication.

### **LOOPING**

---

#### **FRAUD METHOD(S):**

Looping is a method which call-sell operators use to circumvent restrictions that IXCs put in the networks to control calling card fraud. Looping is also used to avoid identification of the origination of the calls. As an example, all carriers block calling card calls bound for the Dominican Republic that originate in NYC. If a call-sell operator is able to obtain a dial tone from a PBX but is not able to dial 809 or 011 call directly, they will revert to looping. They could dial an 800 number outbound from the PBX. The 800 number could be to another PBX or could be a calling card or operator access number. They could also dial 950 carrier access numbers. Lastly, they can dial various 10XXX carrier access codes. In any case they can still use the PBX to place a fraud call. If the PBX is not in NYC they can use the calling card. Use of the 10XXX codes could allow for direct billing to the PBX.

#### **FRAUD SOLUTION(S):**

Many times a PBX owner will also take proactive actions to minimize the risk of fraud. These actions include:

- Blocking of 011 or 809 dialing.
- Block 10XXX codes if possible.
- Block 950 access if possible.
- Monitor 10XXX, 950 and 800 calling on the system to identify possible looping.

## Typical PBX Fraud Methods and Summary Solutions

M C I Systems Integrity

The  
**MCI Network**  
*Means*  
**BUSINESS**

**MCI**

COMNET '93

## DISA

### FRAUD METHOD(s):

DISA is designed to allow remote access to a PBX and then originate an outbound call. As a result of this design, many PBX owners use DISA in lieu of Calling Cards; however, it is also used by call-sell operators in placing fraudulent calls.

The hackers are able to locate the DISA feature with the use of a "war dialer." The "war dialer" dials telephone numbers randomly, generally 800 numbers, until a modem or dial tone is obtained. After a number is found, hacking software is then used to search for valid authorization codes (auth codes). Codes are "frequently" but not always distributed to pirated voice mail systems and computer bulletin boards. The codes are usually distributed to a network of call-sell operators and may also be posted on bulletin boards and voice mail systems.

### FRAUD SOLUTIONS(s):

There are many steps a PBX owner can take to prevent hackers from obtaining and fraudulently using the DISA feature. To begin, auth codes should be made as long as possible. At very least, a factor of 10,000 should exist between the active codes. For example, if there are 10 users the code should be at least 5 digits long ( $10 \times 10,000 = 100,000$  or 5 digits). Auth codes should be randomly scattered throughout the possible range but not easily defined (i.e. 1234 or 1111). Class of service restrictions should be applied to the auth codes. Only users with a truly legitimate need should be allowed International dialing through the DISA. A monitoring system should be set up to record DISA usage. Monitoring reports should show the number of times and minutes an auth code is used in a day. If possible, the dollar value of those calls should also be noted on the reports.

## VOICE MAIL BOXES (VMB)

### FRAUD METHOD(s):

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

### FRAUD SOLUTIONS(s):

To protect against a VMB being pirated the following steps should be taken:

- Do not allow administrative access via the phone. If a telecom person can add, delete and change boxes via the phone, so can a hacker.
- Do not have active mailboxes that do not have an owner.
- Passwords should be at least 6 digits long.
- If possible, passwords should expire every 30-90 days.

## VOICE MAIL BOXES (VMB)

### FRAUD METHOD(s)

The second type of abuse involves garnering a PBX dial tone via the VMB. This is accomplished in two ways. Both methods can transfer out of the VMB to a phone on the system. If the PBX is not set up properly the transfer can be made directly to dial tone. In other instances the caller transfers to an extension. In some cases the extension may be on another PBX and require transmission over a tie line. If the tie line is not properly secured, dial tone can be retrieved and fraudulent calls placed. Finally, all PBXs have Trunk Access Codes (TACs) or Facility Access Codes (FACs). Technicians use these codes to make test calls. If allowed, a hacker can transfer out of the VMB to the TACs or FACs.

### FRAUD SOLUTION(s):

Steps to prevent this type of fraud include:

- Disabling the transferring out feature. This would restrict use to only receiving and retrieving messages.
- Limiting access to only 4 digit extension, if transferring is allowed.
- Blocking 8 & 9 access (8 & 9 generally being draw dial tone numbers).
- Prohibiting trunk-to-trunk access from tie lines.
- Disallowing TAC and FAC access from the VMB.

## CALL ATTENDANT

### FRAUD METHOD(s):

Call attendants are used by many companies to replace a switchboard operator. When a call attendant answers, the caller is generally given numerous options. A typical greeting would be, "Hello, you've reached ABC 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 many call attendants, option nine would be allowed on outbound calls. In addition, when asked to enter an extension the call-sell operator will enter 9180 or 9011. If the system is not properly configured, the call attendant will pass the call back to the PBX. The PBX will react to the 9 as a request for a dial tone. The 180 would become the first numbers of a 1-809 call to the Dominican Republic. The 011 would be treated as the first digits of an International call.

### FRAUD SOLUTION(s):

- Ensure muted features are disabled. In the above example the caller has been offered options 1 and 2. The other options have been muted. They must be shut off to guarantee that the muted features are not active and cannot be accessed.
- Allow only line side access to any calls passed by the call attendant to the PBX.
- Disallow TAC and FAC access to the call attendant trunks.
- Configure the call attendant so that only valid extensions are transferred back to the PBX.

## MAINTENANCE PORTS

### FRAUD METHOD(s):

Maintenance ports are the most recent type of abuse. In this scenario a hacker finds a maintenance port number with his "war dialer." He/she then hack out the user ID and password. At this point they have access to all the features and controls within the PBX. They will program out any restrictions that

## Using Your Vnet Card Is As Easy As 1-2-3 . . .

When calling from the U.S. and Canada:

1. **Dial 1-800-950-1111.**
2. **When you hear the tone,**  
**Dial 0 + area code + number; or**  
**Dial 01 + country code + city code + number**  
**(for international calls); or**  
**Dial 8 + seven-digit private dialing plan**  
**number (if used by your company).**
3. **When you hear the second tone,**  
**Dial your authorization code (the number**  
**on the front of your Vnet Card).**

To make additional calls, you don't have to start over with your access number—simply press the # sign for a full second instead of hanging up, and then repeat step 2. (You don't even have to dial the authorization code again!)

If you dial a wrong number, press the # sign for a full second, then dial the correct number. If it is the first call, dial the authorization code at the second tone. If not, there's no need to redial the authorization number.

- If you are calling from a rotary phone, dial the access number and wait for an operator to assist you.
- If you are calling from a payphone, please check the instructions on the payphone for making an "800" call; you may need to dial 0 800-950-1111.
- If you are calling from a hotel phone, use the hotel's instructions for making an "800" call, dial 1-800-950-1111 and follow steps 2 and 3 to complete the call. (You may still be billed a surcharge by the hotel.)

 Vnet™

**MCI**

MCI Telecommunications Corporation  
© 1992  
1-800-950-1111

**Use The**

**Vnet Card**

**To Stay**

**In Touch**

■ **One number is all you need**—from either a touch-tone or rotary phone. When you're traveling, convenience and efficiency are critical. When it comes time to make a call, you don't have time to look up a lot of numbers.

■ **All the benefits of your company's phone network—when you're on the road!** If your company has a seven-digit private dialing plan, the same number you use to call your colleagues from your office can be used with the Vnet Card<sup>SM</sup>. You also get the benefit of other network services, such as having your call automatically forwarded, or receiving special "help-messages" when there's any kind of change or problem.

### Or More Convenient . . .

■ **Once you access the system, you can make as many calls as you want.** When your conversation is finished, instead of hanging up, simply press the # key and you can place another long distance call.

■ **It's also easy to call from an ever expanding list of other countries**—all instructions are contained in the wallet-sized, easy-to-follow Vnet Card Global Reach<sup>SM</sup> Pocket Guide.

### Or More Practical.

■ **The Vnet Card offers your company considerable cost savings.** Every call you make using the Vnet Card contributes to your company's savings plan with MCI<sup>®</sup>—the more you use it, the more your company will save! When you use your Vnet Card to call your office or any of your company's major facilities, you save even more because you'll be going through your company's private network. The Vnet Card's fast connections will save you time too!

**If you have a problem with your Vnet Card . . .** Call customer service to report the problem (the number is written on the carrier in which you received your Vnet Card). For your convenience, you can write this number in the space provided on the back of your card.

**If your card is lost or stolen . . .** You should immediately call the customer service number.

**If you dial a wrong number . . .** You can receive immediate credit. Simply dial 1-800-950-1111, wait for the operator, and explain that you want credit.

**If you get a recording that says you are not authorized to call the number you dialed . . .** See your manager. To increase security in case of a lost or stolen Vnet Card, your company can specify calling privileges for each card. The area covered is determined by where you do business. If you need to make calls outside of the area set for your card, your manager can make the changes to permit such calls.

**If you need to make calls from outside the U.S. or Canada . . .** Instructions for using your Vnet Card are provided in your Vnet Card Global Reach Pocket Guide, which you received with your card. MCI is continuously adding countries in which you can use your Vnet Card. Before your next business trip abroad, call 1-800-444-4141 to get the most recent list of countries and the free-phone (toll-free) numbers for each one.

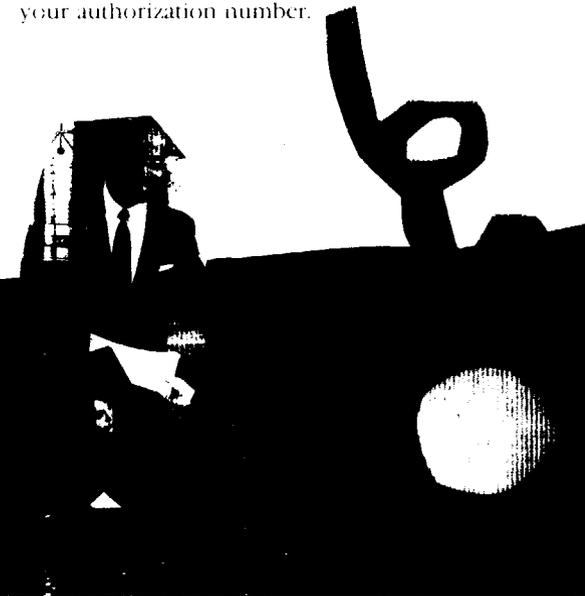
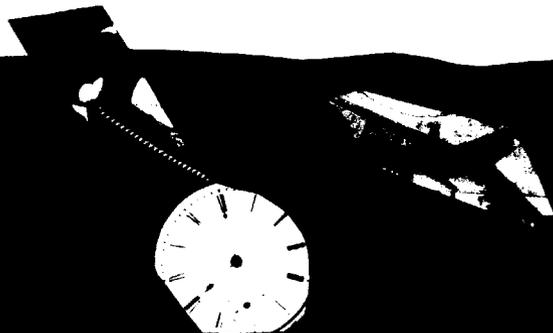
**If you are trying to access Vnet<sup>®</sup> from any phone in the U.S. . . .** Dial the "800" access number for all types of calls from all types of phones. (Other companies require several different access numbers depending on the type of call and the payphone carrier.) This access number allows you to make multiple calls.

## Use Your Vnet Card With Care

Your Vnet Card can help you and your company fight the fraudulent use of credit cards by programming your card to cover only those areas where you actually do business. Should your card be lost or stolen, the risk of fraud is significantly reduced because your Vnet Card will only operate within designated areas.

Here are some other ways you can help combat fraud:

- **If your Vnet Card is lost or stolen,** report it to customer service (the number written on the Vnet Card carrier) as soon as you become aware of it.
- **Don't share your Vnet Card with other people**—protect it as you would any credit card.
- **Try to memorize your Vnet Card authorization code** (the number on the front of the card). The less you take it out in public, the less likely it is that someone will steal it or copy down the number.
- **Be aware of people loitering around payphones.** If you have not memorized your number, try to prevent others from seeing your Vnet Card when you take it out to use it.
- **When placing operator-assisted calls, speak directly into the phone in a normal tone of voice**—be careful not to allow anyone to hear your authorization number.



## For more information

The National Fraud Information Center provides information to consumers about current telephone frauds and tips for avoiding fraud. Center staff is available from 10:00 a.m. to 4:00 p.m. to answer questions, provide information and names, and addresses of agencies and organizations that offer assistance to consumers. Recorded information is available 24 hours a day. Calls requiring personal assistance, when received after hours, will be returned as soon as possible.

### National Fraud Information Center

Consumer Assistance 1-800-876-7060

TDD 202-737-5084

This brochure was produced on behalf of the National Fraud Information Center by MCI Consumer Markets and MCI Systems Integrity.

**NATIONAL  
FRAUD**  
INFORMATION CENTER

**MCI**

AVOIDING PHONE FRAUD

A MESSAGE FROM MCI



# P H O N E F R A U D

## NEW TECHNOLOGY, OLD SCAMS

The telephone offers American consumers an inexpensive, efficient way to communicate directly with family, friends and businesses. New telephone technologies, from increasingly versatile 800 and 900 number services to fax machines and cellular telephones, have changed the way we communicate with each other.

To use calling cards or 800 and 900 numbers, callers do not have to understand the technologies and databases that make these kinds of services possible. Following a few simple steps, callers learn quickly to complete these calls with a minimum of effort.

Unfortunately, con artists have learned to use the telephone to promote confusion and deceive consumers. Using the communications tools of legitimate businesses, they sell everything from fraudulent investments, loans and travel bargains to boats that turn out to be inflatable rafts. Like burglars stealing through the night, they use telephones to become "invisible".

**American consumers can outsmart the telephone scam artists.** By following some rules for telephone shopping, callers can make sure that they don't give a criminal a chance.

## OBSERVE A FEW BASIC PRECAUTIONS WHEN MAKING PURCHASES BY TELEPHONE

Telephone shopping is so popular with Americans that con artists recognized an opportunity to deceive consumers. They could sell their valueless products or phony securities while hiding behind the anonymity of the

telephone. These con artists started out by simply calling consumers and pressing them into buying their worthless wares. After this approach stopped working, they often used newspaper and cable advertising, postcards and other types of mail to urge their "unsuspecting prospects" to call them. Their techniques are sometimes a near-perfect imitation of the techniques of legitimate businesses.



**"I was really excited—I received a postcard in the mail telling me I'd won a free prize if I called a certain number. I ended up sending the company money for some merchandise, and never received anything."**

## **AVOID FRAUD — FOLLOW THESE SIMPLE PROTECTIVE MEASURES**

- 1. Make sure that you know the company with which you are dealing, whether the company calls you or you make the call.** The company should be willing to provide its name, address and phone number.
- 2. If you need more information about a company, check it out with the consumer protection office or the office of the attorney general where the business is located.**
- 3. Do not give credit card or checking account information over the telephone unless you know the company and are making a purchase.**
- 4. Ask for written information about sales transactions.** You should expect to receive a written confirmation of costs, and terms and conditions of purchase transactions. Ask about price, including all fees, delivery charges, sales tax. Insist on a detailed description of the goods and services that you are considering for purchase.
- 5. Ask about guarantees and refunds, and make sure you have them in writing before you make a financial commitment.**
- 6. Do not agree to send cash by mail.**
- 7. Resist high-pressure tactics.**
- 8. Be skeptical of offers that sound too good to be true.**

## **USING A CALLING CARD**

Thieves do not need the calling card itself to use it for fraudulent purposes. They need only to learn the 14 digit authorization code to "steal" your card from you. Important do's and don'ts include:

- 1. Do memorize your calling card number.** Memorization of your card number reduces the risk of the number being stolen as you use the card.
- 2. Do be aware of people loitering around the phone.** People may pretend to be having a conversation on a nearby payphone, to place themselves in a good position

to copy down your authorization code while you are making your call. Stand directly in front of the phone while pressing the authorization code numbers. Also, use a normal conversational tone when reciting the number to an operator.

**3. Don't give your calling card number to telephone security or others.** Any legitimate telephone representatives already have your authorization code and will not need to ask you for it.

**4. Don't share your calling card number with others.** Your calling card number can be abused just like any credit card; guard the number as you would a Visa or MasterCard number.

**5. Do report lost or stolen cards.** Report the loss to the appropriate long distance company as soon as possible to minimize the risk of abuse by thieves.

## **DON'T ACCEPT THIRD-PARTY CALLS FROM PEOPLE YOU DON'T KNOW**

Third-party calls are calls billed to your telephone, by someone calling outside your home or office. Operators, before placing third-party calls, must obtain permission from the party who will be billed for the call. It is appropriate to approve such calls when you know the person calling, and wish to pay for the call. Do not give permission to unknown parties to bill calls to your number.

## **900 NUMBERS: CONSUMER SAFEGUARDS IN PLACE**

Many companies and organizations provide information about their products or services, take orders, or offer advice or educational messages via 900

**"What happens when I call a 900**



**"Someone charged calls on my calling card number. How can that happen when the calling card was never out of my wallet?"**

long distance service. Most businesses serving consumers who use their 900 number lines. Federal rules and long distance company regulations require providers of 900 service to protect consumers by preceding the billable part of the call with a statement or preamble, explaining:

- 1. The cost of the call per-minute or the flat rate, if it will exceed \$2.00.** The name of the information provider and a description of the information or service to be provided must be clearly indicated.
- 2. The exact point when billing will begin (for example, a beep tone might show when the charges start for the call).** The program must allow you to disconnect before that point without charge.
- 3. If the program is directed toward minors, it must warn them that they must obtain parental permission to complete the call.**

Federal rules require long distance carriers to provide the name, address and customer service telephone number of the information provider, at no charge. Local telephone companies must offer a free (for the first request) 900 service block option to residential customers. Local phone companies may not disconnect local phone service for non-payment of interstate 900 pay-per-calls.

In addition to further protect consumers, long distance carriers impose additional restrictions on the uses of 900 programs for which they will perform the billing and collection.

## **USING 800 NUMBERS**

When 800 service was first introduced, it was widely advertised as toll-free. The intent of the long distance carriers is to continue to promote and protect toll-free 800 service. In some short-lived scams, con artists distorted the 800 service by confusing consumers and charging for calls that they expected would be free.

To protect callers, long distance carriers prohibit charging callers for information carried on 800 numbers unless the caller has an established billing relationship with the 800 information service or uses a credit card to pay for the service. For example, a caller could dial an 800 number to reach a stock information service which charges a fee, but would be required to have a billing relationship with the service or use a credit card to receive the service. The 800 information service CANNOT bill the customer's phone number or permit charges by a third party with whom the consumer has no business relationship.

If you call an 800 number and are asked to call another long distance number or to receive a collect call to obtain additional information, you may be charged for the collect or additional call. The collect or additional call is not a part of the original 800 call.

**number? When do the charges begin?"**





**TYPICAL PBX FRAUD METHODS  
AND  
SUMMARY SOLUTIONS**

**MCI  
SYSTEMS INTEGRITY**

**OUTLINE**

- DISA
- VOICE MAIL BOXES(VMB)
- CALL ATTENDANT
- MAINTENANCE PORTS
- LOOPING

# DISA

## **FRAUD METHOD(s):**

DISA is designed to allow remote access to a PBX and then originates an outbound call. As a result of this design, many PBX owners use DISA in lieu of Calling Cards; however, it is also used by call-sell operators in placing fraudulent calls.

The hackers are able to locate the DISA feature with the use of a "war dialer". The "war dialer" dials telephone numbers randomly, generally 800 numbers, until a modem or dial tone is obtained. After a number is found, hacking software is then used to search for valid authorization codes (Auth Codes). The Auth Codes are then distributed via bulletin boards or pirated Voice Mail boxes.

## **FRAUD SOLUTION(s):**

There are many steps a PBX owner can take to prevent hackers from obtaining and fraudulently using the DISA feature. To begin, Auth Codes should be made as long as possible. At very least a factor of 10,000 should exist between the active codes. An example, if there are 10 users the code should be at least 5 digits long ( $10 \times 10,000 = 100,000$  or 5 digits). Auth Codes should be randomly scattered throughout the possible range but not easily defined (i.e. 1234 or 1111). Class of service restrictions should be applied to the Auth Codes. Only users with a truly legitimate need should be allowed International dialing through DISA. A monitoring system should be set up to record DISA usage. Monitoring reports should show number of times and minutes an Auth Code is used in a day. If possible, the dollar value of those calls should also be noted on the reports.

# VOICE MAIL BOXES (VMB)

## **FRAUD METHOD(s):**

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

## **FRAUD SOLUTIONS(s):**

To protect against a VMB being pirated the following steps should be taken:

- Do not allow administrative access via the telephone. If a telecom person can add, delete and change boxes via the telephone, so can a hacker.
- Do not have active mailboxes that do not have an owner.
- Passwords should be at least 5 digits long.
- If possible, passwords should expire every 30-90 days.

(Continued)

## VOICE MAIL BOXES (VMB)

### **FRAUD METHOD(s)**

The second type of abuse involves garnering a PBX dial tone via the VMB. This is accomplished in two ways. Both methods can transfer out of the VMB to a telephone on the system. If the PBX is not set up properly the transfer can be made directly to dialtone. In other instances, the caller transfers to an extension. In some cases the extension may be on another PBX and require transmission over a tie line. If the line is not properly secured, dial tone can be retrieved and fraudulent calls placed. Finally, all PBX have Trunk Access Codes (TAC's) or Facility Access Codes (FAC's). Technicians use these codes to make test calls. If allowed, a hacker can transfer out of the VMB to the TAC's or FAC's.

### **FRAUD SOLUTION(s):**

Steps to prevent this type of fraud include:

- Disabling the transferring out feature. This would restrict use to only receiving and retrieving messages.
- Limiting access to only 4 digit extensions, if transferring is allowed.
- Blocking 8 & 9 access (8 & 9 generally being draw dial tone numbers).
- Prohibiting trunk-to-trunk access from tie lines.
- Disallowing TAC and FAC access from the VMB.

## CALL ATTENDANT

### **FRAUD METHOD(s):**

Call attendants are used by many companies to replace a switchboard operator. When a call attendant answers, the caller is generally given numerous options. A typical greeting would be, "Hello, you've reached Nations Bank, please enter one for Auto Loans, two for Home Mortgages. If you know the extension of the person you are calling, please enter it now." In many call attendants, option nine would be allowed on outbound calls. In addition, when asked to enter an extension the call attendant will enter 9180 or 9011. If the system is not properly configured the call attendant will pass the call back to the PBX. The PBX will react to the 9 as a request for a dial tone. The 180 would become the first numbers of a 1-809, call the Dominican Republic. The 011 would be treated as the first digits of an international call.

### **FRAUD SOLUTION(s):**

- Ensure muted features are disabled. In the above example the caller has been offered options 1 and 2. The other options have been muted. They must be shut off to guarantee that the muted features are not active and cannot be accessed.
- Allow only line side access to any calls passed by the call attendant to the PBX.
- Disallow TAC and FAC access to the call attendant trunks.
- Configure the call attendant so only valid extensions are transferred back to the PBX.

## MAINTENANCE PORTS

### **FRAUD METHOD(s):**

Maintenance ports are the most recent type of abuse. In this scenario a hacker finds a maintenance port number with his "war dialer." They then hack out the user identification and password. At this point, they have access to all the features and controls within the PBX. This will program out any restrictions that have been put in place. They will also enable outdialing features that do not normally exist on the PBX. These situations can be difficult to detect. Hackers have been known to change the system at 8:00 pm, to allow fraud calls. Then, at 3:00 am the next morning they re-program the system back to its original configuration. A telecom manager who reviews the configuration in the morning will not be looking at the configuration that was abused. This can lead to delays in resolving the abuse.

### **FRAUD SOLUTION(s):**

To solve this problem, a Security Access Unit (SAU) should be placed in front of the maintenance port. SAU's provide another lever of user identification and password protection. This identification and password should be controlled by the PBX owner and not the vendor. In addition, SAU's can be set up to further validate a user via callback or numerous token devices. While still a bit expensive there are products which use voice validation for authentication.

## LOOPING

### **FRAUD METHOD(s):**

Looping is a method which call sell operators use to circumvent restrictions that IXC's put in the networks to control calling card fraud. All carriers block calling card calls bound for the Dominican Republic that originate in NYC. If a call sell operator is able to obtain a dialtone from a PBX but is not able to dial 809 or 011 call directly, they will revert to looping. They could dial an 800 number outbound from the PBX. The 800 number could be to another PBX or could be a calling card or operator access number. They could dial 950 carrier access numbers. Lastly, they can dial various 10XXX carrier access codes. In any case, they can still use the PBX to place a fraud call. If the PBX is not in NYC they can use the calling card. Use of the 10XXX codes could allow for direct billing to the PBX.

### **FRAUD SOLUTION(s):**

Many times a PBX owner will also take proactive actions to minimize the risk of fraud. These actions include:

- Blocking of 011 or 809 dialing.
- Block 10XXX codes if possible.
- Block 950 access if possible.
- Monitor 10XXX, 950 and 800 calling on the system to identify possible looping.

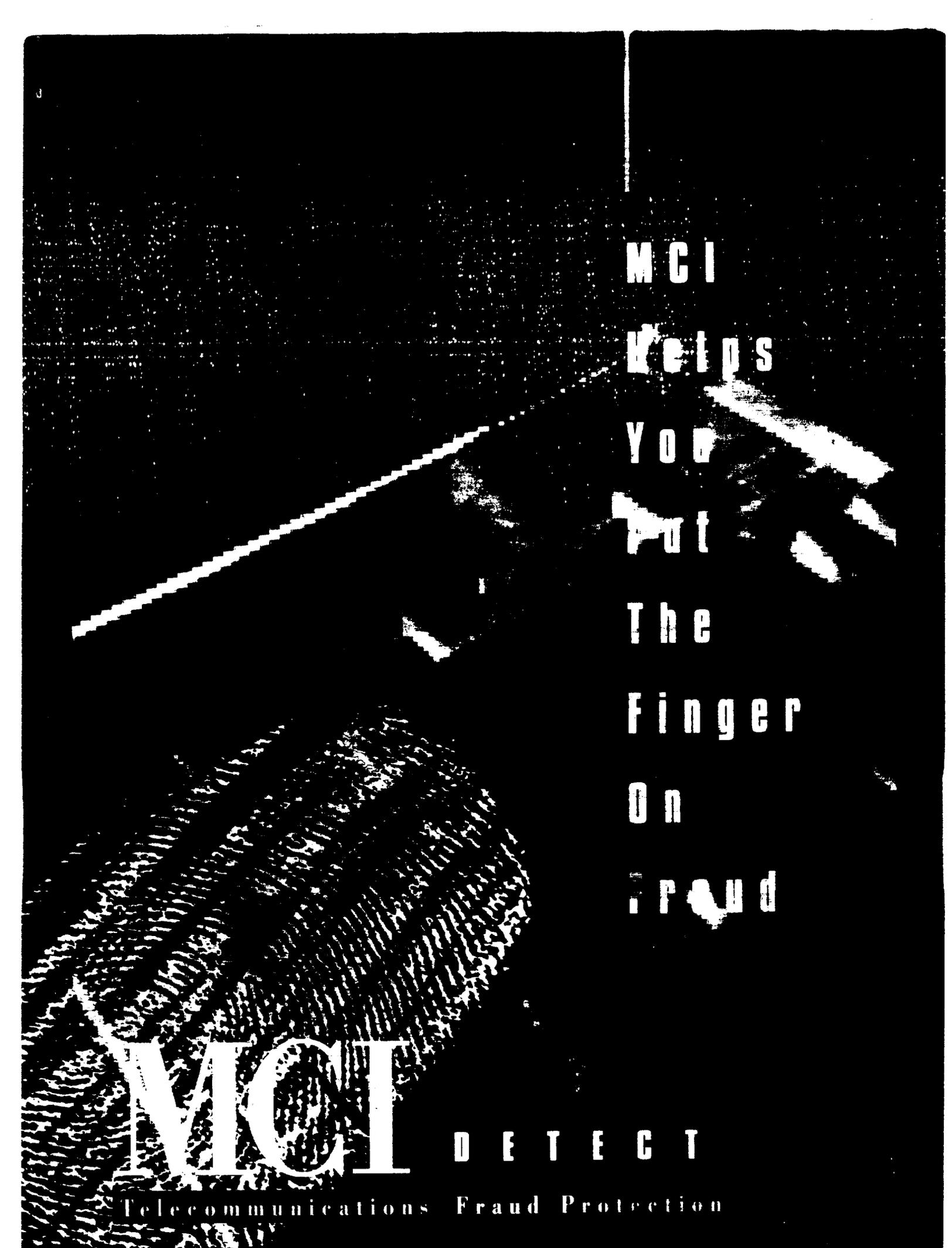
## **ATTACHMENT B**

**ATTACHMENT B**

The United States Department of Treasury  
The United States Secret Service  
The United States Department of Justice  
The Federal Communications Commission  
Cable & Wireless Communications, Incorporated  
Octel Communications Corporation  
The Tennessee Valley Authority  
Sandia National Laboratories  
Sprint  
The Central Intelligence Agency  
Southern Bell  
The United States Coast Guard  
Intel Corporation  
The Orange County Transportation Authority  
Indiana University  
Rolm  
KDD  
The Massachusetts Department of Revenue  
The Securities and Exchange Commission  
Kemper National Insurance Companies  
Mellon Bank  
The United States Department of Commerce  
The University of Texas  
Northern Telecom  
The National Aeronautics and Space Administration  
US West Communications  
The United States Air Force  
The State of Ohio (Auditor of State)  
The United States Department of the Navy  
Bell Atlantic  
Seattle Post-Intelligencer Newspaper  
National Association of State Telecommunications Directors  
Coopers & Lybrand  
Switching Systems Division, Rockwell International Corporation  
American Airlines  
Teleconnect Magazines  
Discover Card Services  
GTE Mobilenet  
AT&T  
National White Collar Crime Center

RECEIVED  
JAN 14 1994  
FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

**ATTACHMENT A**



MCI  
Helps  
You  
Put  
The  
Finger  
On  
Fraud

**MCI** D E T E C T

Telecommunications Fraud Protection

# YOUR PARTNER IN TELECOMMUNICATIONS FRAUD PREVENTION

## CPE-RELATED FRAUD...A COSTLY, GROWING PROBLEM

CPE-related fraud, the illegal use of private telecommunications systems, can be a serious problem for owners of Customer Premises Equipment (CPE) such as PBX and voice mail systems. Surreptitiously tapping into systems through electronic "hacking" or by stealing access codes, thieves are able to use someone else's phone lines to place costly international calls.

Many of them sell overseas calls at bargain rates to street customers...others use the access for their own purposes, such as making non-traceable calls to drug dealers in foreign countries. It's not until weeks later, when unauthorized long-distance calls show up on phone bills, that unsuspecting companies find out that they've been victimized.

## MCI DETECT: A MULTI-DISCIPLINARY APPROACH

MCI has developed MCI Detect, a multi-disciplinary attack on the problem of fraud. This value-added approach for our customers is provided at no additional cost. It includes:

Customer Awareness and Education

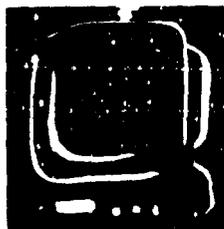
CPE Fraud Detection Equipment

Analysis of Customer Traffic

Third-Party Insurance

These elements are now being implemented and shared with our customers. Working with you as part of your fraud control plan, MCI will do as much as we can to help you limit your exposure and financial loss. To find out what you can do to control fraud, take advantage of the MCI Detect program now.

## CUSTOMER AWARENESS AND EDUCATION



Exclusive fraud awareness video for MCI customers.

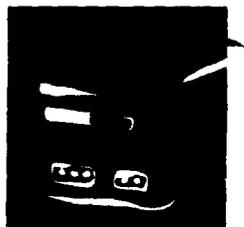
- Exclusive fraud awareness video for MCI customers
- Manual on easily compromised CPE features
- Newsletter on latest fraud control techniques

### Securing Your CPE...the First Line of Defense

Awareness of fraud potential is critical to its detection. A new fraud awareness video presentation, "Invisible Criminals," is available to all MCI customers. MCI has played a leading role in educating customers of fraud potential and in ways to identify and control it. Over the past three years, fraud workshops have been held for more than 2,000 participants.

The first and most important battle in the fight against telephone fraud is to secure your CPE. The MCI Detect newsletter will keep you up-to-date on the latest techniques, technology and ideas. A manual for MCI customers explaining the features of CPE which are vulnerable to attack will be available in 1993. MCI can also provide security consulting assistance on a special-use basis for customers who have more complex systems.

## CPE FRAUD DETECTION EQUIPMENT THROUGH AFFILIATES PROGRAM



20% discount on recommended CPE-attached hardware.

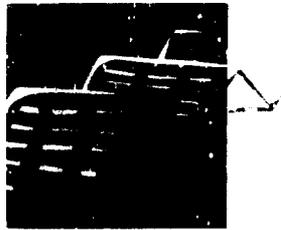
- 20% discount on recommended CPE-attached hardware
- Monitoring of PBX traffic on a real-time basis

### The First Signs of Fraud Can Be Costly

Usually, the first signs of fraud are unexplained spikes in telephone usage along with a sudden rise in calls to certain areas. But these indicators often become apparent weeks after the fact, when much of the damage has already been done. A more timely, continuous analysis of traffic can be accomplished with PBX add-on equipment.

State-of-the-art access control and ground traffic monitoring are available through equipment manufactured by MicroFrame and Xiox. These units monitor PBX traffic on a real-time basis. When thresholds are triggered, the equipment sends alarms and can even take the ultimate measure of shutting down the abused facility without human intervention. MCI currently uses both MicroFrame and Xiox equipment on its own office PBXs. MCI has arranged a 20% discount on CPE-attached hardware units for MCI customers.

## ANALYSIS OF CUSTOMER TRAFFIC



- Analysis of outbound international and inbound 800 traffic to determine fraudulent usage patterns
- Customer notification of suspected fraud
- Assistance with identifying how CPE was compromised

### MCI Program Helps Spot Possible Fraud

Fraud can still occur, no matter how carefully access to long distance lines is controlled. A hacker can get lucky, new technology may be able to subvert yours, disgruntled employees may sell codes...the possibilities are endless.

A program of recording and analyzing customers' usage in an effort to detect traffic with high-fraud-potential allows MCI to spot suspicious calling patterns and advise customers before the charges appear on their bills. There is no charge to the customer for this service and gradual extension is planned as technology permits. It's another part of MCI's commitment to our customers.

MCI monitoring  
program helps spot  
possible fraud.

## THIRD-PARTY INSURANCE



- True insurance that transfers risk
- Coverage of any long distance carriers' traffic

Industry efforts have been made to limit fraud loss through service guarantees that function similarly to insurance coverage. However, these plans are limited to specific carriers and require specific volume traffic commitments.

MCI has a working relationship with an insurance broker, Henry Ward Johnson & Company, Inc.; and a major insurance company for the introduction of an insurance policy which transfers fraud risk without these shortcomings. MCI does not view insurance as a sales tool. We want all our customers, no matter how many carriers they may be using, to have maximum protection and minimum loss.

MCI works  
for non-restrictive  
fraud insurance.

### FOR MORE INFORMATION, TALK TO YOUR MCI REPRESENTATIVE.

We'll work with you in every way possible to reduce the risk of CPE-related fraud loss. Through MCI Detect, MCI makes its expertise on CPE-related fraud available to its customers at no additional charge.

As an MCI customer, MCI Detect will help you plan and implement a fraud prevention program tailored expressly to your needs. We will keep you abreast of new developments, emerging technologies, fresh ideas and effective solutions. We'll do everything we can to help you make your own program effective and cost-efficient.

**MCI** **DETECT**  
Telecommunications Fraud Protection

**W**orking with our customers and the industry, since 1988, MCI has created a long history of leadership in prevention, detection and identification of telecommunications fraud problems. Our goal is to assist our customers in every way possible. When it comes to telephone fraud, MCI has zero tolerance.

MCI has played key roles in the apprehension of fraud perpetrators, in improving telecommunications security, and in helping to develop fraud resistant systems. Sharing our knowledge, skills and experience with our customers, we have helped such diverse organizations as insurance companies, manufacturers, unions, governmental organizations, and computer manufacturers and banks to stem this costly flow.

**MCI:** **telecommuni-**  
**cations.**

**MCI**

WE'RE ALWAYS READY TO

# MCI **DETECT**

Telecommunications Fraud Protection

## MCI Helps You Put the Finger on Fraud

### Customer Awareness and Education

- Exclusive fraud awareness video for MCI customers
- Manual on easily compromised CPE features
- New letters on latest fraud control techniques

### CPE Fraud Detection Equipment Through Affiliates Program

- 20% discount on recommended fraud detection equipment
- Monthly newsletter on fraud control techniques

### Analysis of Customer Traffic

- Identification of high and international calling patterns
- Identification of international fraud patterns
- Identification of suspected international fraud CPE

### International Insurance

- International transfer and long distance services

**MCI**