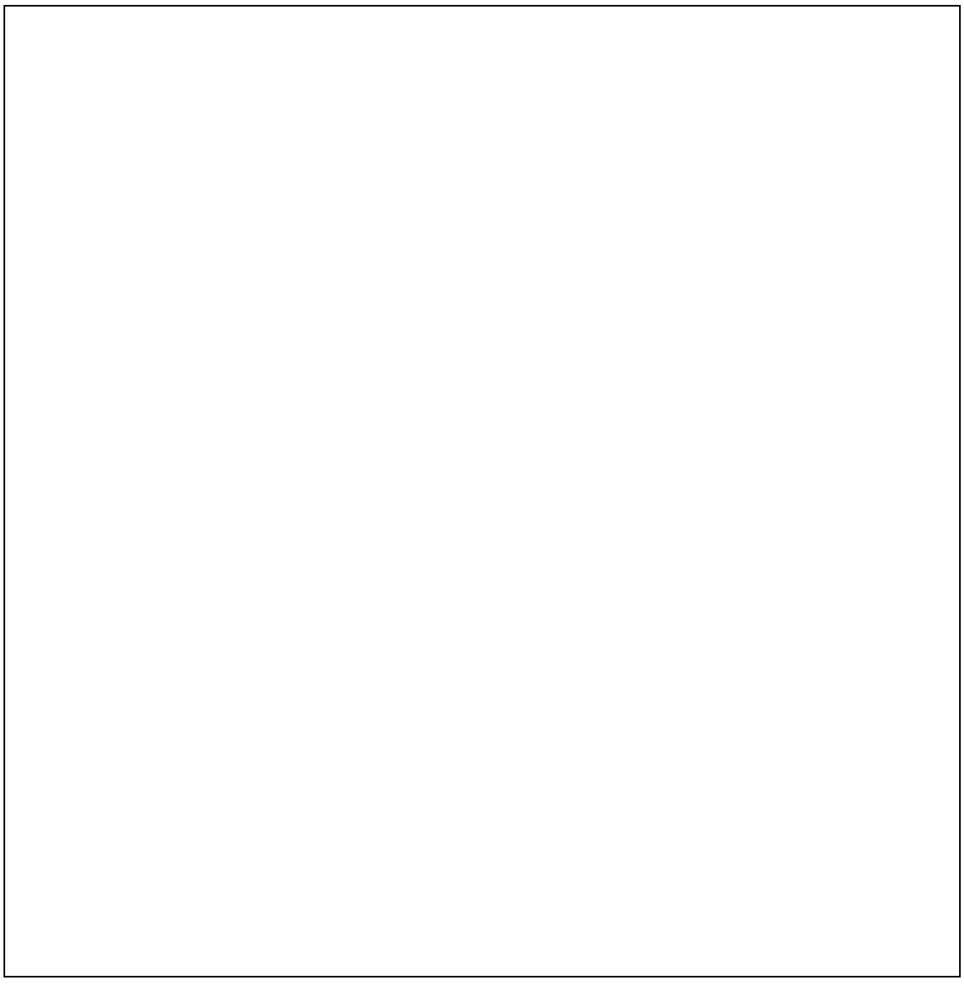
297-1001-132

DMS-100 Family

Blue Box Fraud Detection

Feature Description

BCS22 and up Standard 02.02 March 1991



northern telecom

DMS-100 Family

Blue Box Fraud Detection

Feature Description

Publication number: 297-1001-132
Product release: BCS22 and up
Document release: Standard 02.02
Date: March 1991

Revision history

BCS	Date	Revisions
BCS32	March 1991	Converted document to Interleaf format (style) - content of document is unchanged by this revision.
BCS22	April 1987	Updated format and content of document.
BCS0		Original issue of document.
	Page 1 of 1	

Revision bars in the table of contents identify the sections where information has been changed. Revision bars in the outside margin of a page indicate text that has been added or revised.

About this document

This document describes how the Blue Box Fraud Detection feature (U.S. patent 4,001,513) operates within the DMS-100 family of digital multiplex switches. This document is a general description manual, and as such, it is intended for use by a wide skill-level range of readers.

Applicability of this document

Northern Telecom (NT) software releases are referred to as batch change supplements (BCS) and are identified by a number, for example, BCS29.

This document applies to DMS-100 Family offices that have BCS22. Unless the document is revised, it also applies to offices that have software releases greater than BCS22.

More than one version of this document may exist. To determine which version applies to the BCS in your office, check the release information in *Northern Telecom publications master index,* 297-1001-001.

How to identify the software in your office

Software applicable to a specific DMS-100 Family office is identified by a BCS release number and by Northern Telecom (NT) Product Engineering Codes (PEC). The significance of the BCS number and the PEC is described in *Provisioning,* 297-1001-450 (section 450/32) and in the Office Feature Record D-190.

The *Office feature record D190* lists your current BCS and the NT feature packages that it comprises. To view similar information on screen, enter the following command string at a MAP terminal.

PATCHER;INFORM LIST;LEAVE

How the Blue Box Fraud Detection documentation package is organized

This document is the only document in the Blue Box Fraud Detection documentation package. The Blue Box Fraud Detection documentation package is a subset of the DMS-100 Family Library.

How the Blue Box Fraud Detection documents relate to other documents

Blue Box Fraud Detection documents are intended to be used with other documents in the DMS-100 Family library.

To fully understand the content of the Blue Box Fraud Detection document, you may also require DMS-100 basic documents in the 297-1001 layer. Related documents in the 297-1001 layer are listed below under the headings Prerequisite References and Informative References.

Where to find information

Documents that you require to understand the content of this document are listed below. These documents are also referred to in the appropriate places in the text.

Note: More than one version of these documents may exist. To determine which version of a document applies to the BCS in your office, check the release information in *Northern Telecom publications master index*, 297-1001-001.

Prerequisite References

Document	Title
297-1001-100	*System Description*

Informative References

Document	Title
GFXINDEX	*General Feature Description Index of Document*
297-1001-001	*Master Index of Practices*
297-1001-110	*Maintenance and Administration Position (MAP)*
297-1001-114	*Operational Measurements (OM)*
297-1001-119	*Automatic Message Accounting - Northern T elecom Format*
297-1001-450	*Provisioning*
297-1001-510	*Log Report Manual*

NT and BNR trademarks and the products they represent

The following chart lists all NT and BNR trademarks that occur in this document, and associates them with the products they represent.

Trademark	Product
BNR	*Bell-Northern Research* company involved in scientific research and development in the field on telecommunications
DMS	*Digital multiplex system* telephone switching equipment
DMS-100	*Digital Multiplex System - 100* local digital switch
MAP	*Maintenance and administration position* telecommunications user interface equipment
NT	Northern Telecom *manufacturer of communications switching equipment*

How commands, parameters, and responses are represented

In this document, commands, parameters, and responses are represented according to the following conventions.

Input prompt (>)

An input prompt (>) indicates that the information that follows is a command.

Type the command that follows the input prompt and press the carriage return key.

Capital letters

Capital letters represent commands, fixed parameters, and responses that appear at a MAP.

Enter the command or fixed parameter exactly as it appears on the page.

Lowercase letters

Lowercase letters represent variables.

Brackets [ ] or [ ]

enclose optional parameters. A vertical list enclosed in brackets means that one of the parameters may be selected.

For commands and parameters, enter the letters or numbers that the variable represents. In most instances, the name that is used for the variable indicates clearly what you must enter. Where it does not, further explanations are provided.

In responses (which are presented in capital letters), lowercase letters represent a range of values.

The following example illustrates the command syntax that is used in this document.

Examples of command syntax used in this document

Step	**Action**
1	Post the card in the inactive unit.
input>	**>POST unit_no card_no state**
parameters>	where unit_no is the number of the inactive unit (0 or 1) card_no is the number of the card you replaced (22-27) state is the state of the unit in which you wish to replace the card (Insv, SysB, ManB or Offl)
Example input>	For example: **>POST 7 1 INSV**
Example output>	`CARD 7 IS POSTED IN UNIT 1 OF MSB16`

Contents

Introduction

This document describes the Blue Box Fraud Detection feature and its operation within the DMS-100 Family. A ”blue box” is any device, connected illegally to a subscriber’s line, that can produce both a 2600 Hz tone and multifrequency (MF) digits.

To place a fraudulent call, the perpetrator performs two steps:

1 The perpetrator uses a normal telephone to place a normal call. This call is usually a free or inexpensive call, and uses a Single Frequency (SF) trunk beyond the perpetrator’s billing office.

2 The perpetrator uses a blue box to place the fraudulent call. This call uses the SF trunk seized for the original, normal call.

The perpetrator’s billing office typically does not detect calls placed with a “blue box”, thus the term “blue box fraud.”

The Blue Box Fraud Detection feature discovers fraudulent MF signaling over Centralized Automatic Message Accounting (CAMA) and SuperCAMA trunks. It does not detect fraudulent signaling over Traffic Operator Position System (TOPS) trunks. The Blue Box Fraud Detection feature can alert the operating company of a fraudulent call attempt and either allow billing to be made for the call or disconnect the call.

This feature detects fraudulent MF signaling but does not detect fraudulent SF pulsing. No customer data schema is required, because the feature is activated and deactivated using the Command Interpreter (CI) facilities at the Maintenance and Administration Position (MAP). The feature implements the method of detection of fraudulent telephone calls described in U.S. patent 4,001,513.

Description

The Blue Box Fraud Detection feature allows the DMS-200 to perform three fraud detection functions:

- test for fraudulent calls
- record fraudulent calls
- dispose of fraudulent calls (cut or continue).

Those events are described in the remainder of this chapter

Figure 2-1 describes how a perpetrator initiates a fraudulent call.

Figure 2-1
Fraudulent call setup

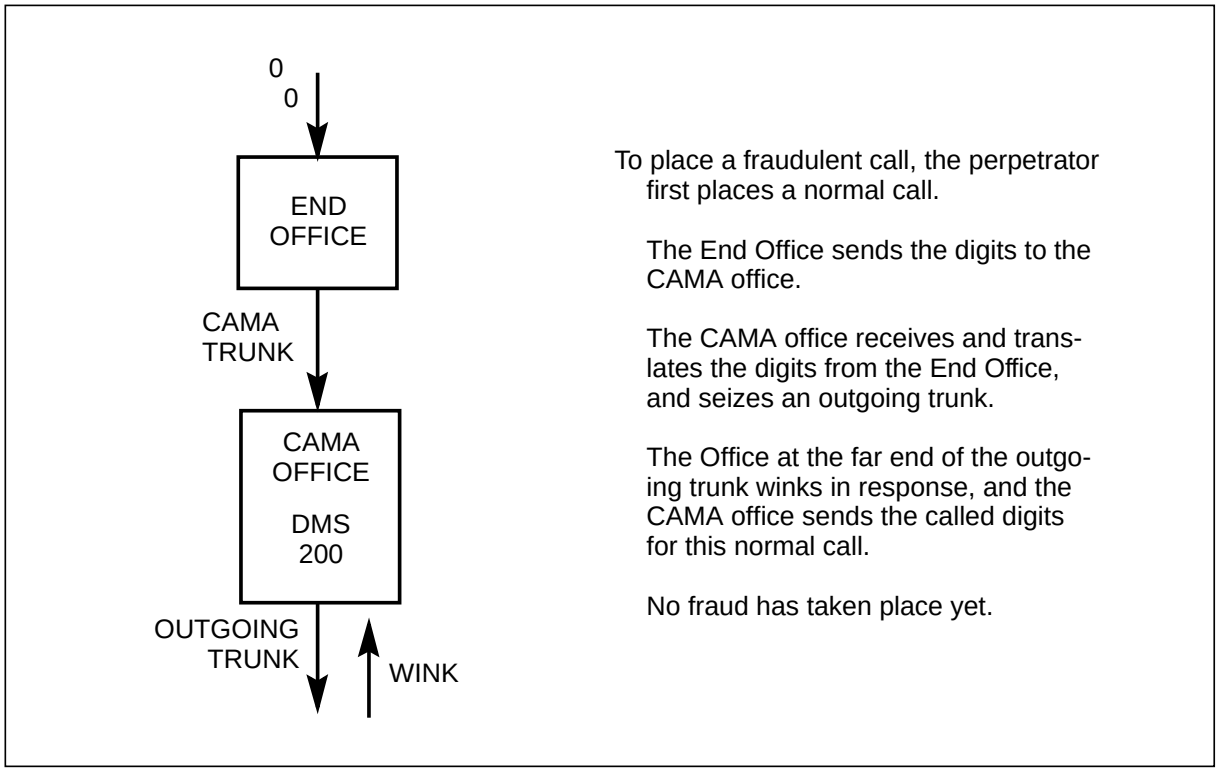
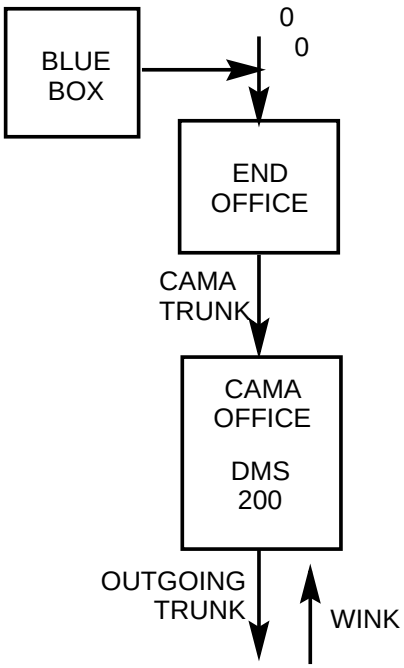


Figure 2-2 describes how the system responds to a fraudulent call, and how the testing procedure is invoked.

Figure 2-2xxx
Fraudulent call system response



To place a fraudulent call, the perpetrator first places a normal call.

The End Office sends the digits to the CAMA office.

The CAMA office receives and translates the digits from the End Office, and seizes an outgoing trunk.

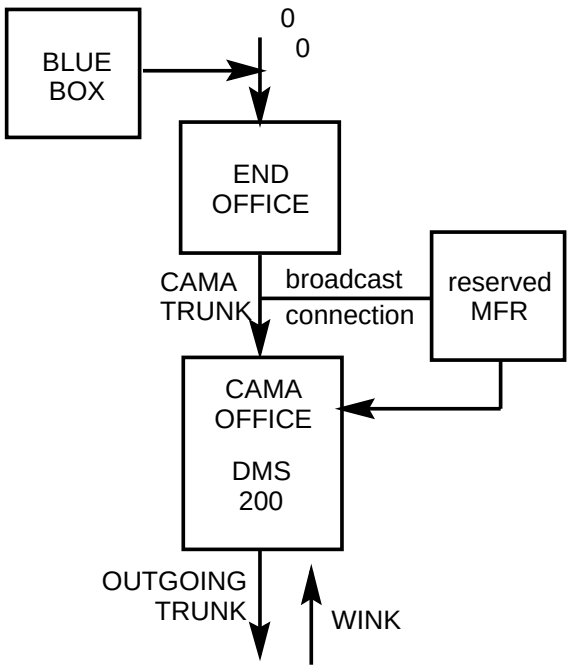
The Office at the far end of the outgoing trunk winks in response, and the CAMA office sends the called digits for this normal call.

No fraud has taken place yet.

Testing for fraudulent calls

Triggered by the unexpected wink, the DMS-200 begins to test the suspected fraudulant call. Figure 2-3 describes how the DMS-200 prepares to test for fraudulent calls.

Figure 2-3xxx
Reserved multifrequency receiver



To test the call, the DMS-200 establishes a broadcast network connection from the suspected incoming CAMA trunk to a reserved MF receiver (MFR).

These MFR are reserved when the feature is activated.

As long as the feature is active, the reserved MFR are not available for standard call processing.

NOTE: The number of MFR set in reserve depends on the number of simultaneous fraud attempts expected. For providing MFR refer to *Provisioning,* 297-1001-450.

Following is a description of the events that occur after the MFR is attached.

Table 2-1 describes the events that occur after the MFR is attached. After attaching the MFR, the DMS-200 waits for one of the events shown in the ”Event” column of Table 2-1 and responds to that event as shown in the ”System response” column of the same table. Table 2-1 also includes an ”Explanation” coulmn to clarify circumstances and conditions surrounding the event being described.

Table 2-1xxx
MFR attachment response

Event	Explanation	System response
Wink	Wink on the same trunk again.	Reset the MFR timeout and continue to wait.
Digits	A fraudulent set of called digits has been received.	Provide the charge utility with these digits and use the Automatic Message Accounting (AMA) Event Information Digit to flag this call as a Blue Box call. Release the MFR. If the CUT option was specified from the MAP, disconnect the call. Refer to Commands on page 4-1 for information about the CUT option.
Call Failure	Mutilated digit(s) detected by the MFR. Several things could cause this: · the call may have released · there may be a real transmission problem · the perpetrator may be using SF pulsing	Release the MFR and assume no fraud has taken place.
MFR Timeout	This time allowed to detect possible fraudulent MF digits has expired.	Release the MFR and assume no fraud has taken place.

Page 1 of 1

Recording fraudulent calls

The DMS-200 performs the following actions after detecting a fraudulent call:

- If the CUT option was not specified, replace the original digits in the charge buffer with the fraudulent digits.

  Note: If the perpetrator places more than one fraudulent call, only the last call appears in the charge buffer.

- Set the AMA event information digit to mark the call as a blue box call. See document *Automatic Message Accounting - Northern Telecom Format*, 297-1001-119.
- If the office is performing AMA recording for this call, generate a log to alert the operating company office that a Blue Box call is in progress.
- See if the ALARM option was specified at the MAP, generate a visual/ audible minor alarm.

Disposing of fraudulent calls

There are two options for disposing of fraudulent calls: Cut the call or continue the call.

Cut the call

To cut a fraudulent call, the DMS-200 performs the following actions:

- releases the MFR
- releases the connection between the originating and terminating agents of the call
- processes the AMA information
- deallocates the terminator
- sets treatment for the originator.

Continue the call

If the CUT option was not specified, the DMS-200 releases the MFR and the call continues. The perpetrator is billed based on the fraudulent digits.

When the subscriber disconnects the call, the system generates a log and turns off the alarm if the ALARM option was specified.

Operational measurements

The Operational Measurement BLUEBOX is associated with the Blue Box Fraud Detection feature (see *Operational Measurements (OM)*, 297-1001-814, for more information). The CI command OMSHOW BLUEBOX will display the contents of each field.

BLUEBOX has the following fields:

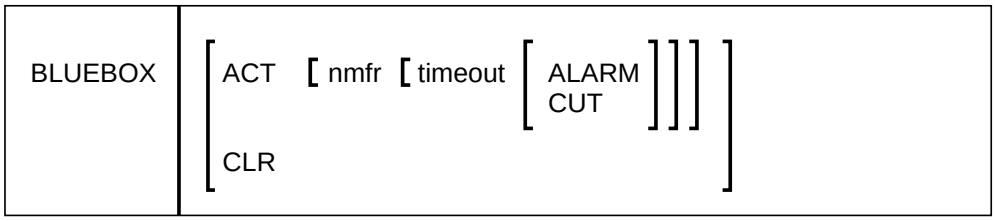
Table 3-1xxx
Blue box fields

Field	Description
BBWinks	Number of unexpected winks detected on incoming CAMA trunks. These winks could indicate fraudulent calls.
BBAttach	Number of successful MFR attachments to suspected trunks.
BBDetect	Number of fraudulent calls detected.

User interface

The Blue Box Fraud Detection feature is activated by a CI command issued at the MAP. The same command can be used to query the status of the feature. The following section describes the syntax and options of the commands.

Commands



activates, clears, or queries the status of the Blue Box Fraud Detection feature. Activating the feature reserves the specified number of MFR. Clearing the feature returns the MFR to the common pool.

Where:

ACT activates the blue box feature and reserves the specified number of MFR.

CLR deactivates the blue box feature and returns the MFR to the common pool.

nmfr specifies the number of MFR to be reserved.

- Range: 1 through 3.
- Default: 1.

timeout specifies the number of seconds the MFR will wait for digits.

- Range: 5 through 35.
- Default: 30.

ALARM specifies that an audible/visual alarm will be generated when a Blue Box call is detected.

CUT specifies that fraudulent calls will be disconnected. If this parameter is not specified, the fraudulent call will continue.

Note: 1 The activation parameters are position-dependent. That is, nmfr must be specified before timeout; both nmfr and timeout must be specified before ALARM or CUT.

Note: 2 The BLUEBOX command issued without any parameters queries the system for the feature status.

Examples:

1 Activate the blue box feature using only the default parameters. The user enters the following CI command:

BLUEBOX ACT

The system responds with the feature status and parameters:

```
Bluebox Fraud Detection Feature Status:
Active.
1 MFR reserved, timeout set to 30 seconds.
```

2 Activate the blue box feature and reserve two MFR. The user inputs the following CI command:

BLUEBOX ACT 2

The system responds with the feature status and parameters:

```
Bluebox Fraud Detection Feature Status:
Active.
2 MFR reserved, timeout set to 30 seconds.
```

3 Activate the blue box feature and reserve three MFR with a timeout of 22 seconds. The user inputs the following CI command:

BLUEBOX ACT 3 22

The system responds with the feature status and parameters:

```
Bluebox Fraud Detection Feature Status:
Active.
3 MFR reserved, timeout set to 22 seconds.
```

4 Activate the blue box feature with the ALARM option. Reserve one MFR with a timeout of 30 seconds. The user inputs the following CI command:

BLUEBOX ACT 1 30 ALARM

The system responds with the feature status and parameters:

```
Blue Box Feature Status:
Active.
1 MFR reserved, timeout set to 30 seconds.
  Detection will report alarm.
```

5 Activate the blue box feature with the CUT option. Reserve two MFR with a timeout of 25 seconds. The user inputs the following CI command:

BLUEBOX ACT 2 25 CUT

The system responds with the feature status and parameters:

```
Bluebox Fraud Detection Feature Status:
Active.
2 MFR reserved, timeout set to 25 seconds.
  Detection will cut off call.
```

6 Determine the status of the blue box feature. The user inputs the following CI command:

BLUEBOX

If the feature is not active, the system responds with:

```
Bluebox Fraud Detection Feature Status:
Inactive.
```

If the feature is active, the system responds with the feature status and parameters:

```
Bluebox Fraud Detection Feature Status:
Active.
2 MFR Reserved, timeout set to 35 seconds.
  Detection will cut off call.
```

7 Deactivate the blue box feature and return the MFR to the common pool. The user inputs the following CI command:

BLUEBOX CLR

The system indicates command execution with the response:

```
Bluebox Detection Feature Cleared.
```

Q	BLUEBOX

queries the system for the syntax of the BLUEBOX command.

Example:

Display the BLUEBOX command syntax.
The user inputs the following CI command:

```
Q BLUEBOX
```

The system responds with the following syntax diagram:

```
Parameters for Bluebox Fraud Detection
Parms: [<Active Status> {CLR,
                         ACT [<Number of MFRs> {1 TO 3}]
                             [<Timeout Value> {5 TO 35}]
                             [<Notification Option> {ALARM,
                                                     CUT}]}]
```

Alarms

If the ALARM option is specified, a minor office alarm is activated whenever a blue box call is detected. The office alarm is deactivated at call disconnect.

Logs

The following six logs are associated with the Blue Box Fraud Detection feature:

- AUDT118
- EXT106
- TRK151
- TRK152
- TRK153
- TRK154.

The following is a brief description and example of each log. See *Log Report Manual*, 297-1001-510, for more detailed information.

Table 4-1xxx
Log description

Log	Description

AUDT118	The Audit subsystem generates this log when Blue Box Fraud Detection feature data is inconsistent with the corresponding MFR data. The identified MFR cannot be used for fraud detection until the problem is cleared.
	
	Example:
	
	`AUDT118 APR12 12:00:00 2112 FAIL BLUEBOX MFR LOST`
	`CKT RCVRMF 1`

EXT106	The External Alarms subsystem generates this log when a fraudulent call is detected and when that call disconnects.
	
	Example:
	
	`*EXT106 MAR14 12:00:00 2112 INFO BLUEBOX ON`
	`CALL DETECTED`

TRK151	The Trunk Maintenance subsystem generates this log when the Bluebox Fraud Detection feature is activated.
	
	Example:
	
	`TRK151 APR11 12:00:00 2112 INFO BLUEBOX DETECTION ACTIVE`
	`# OF MFRS = 2 ALARM ENABLED`
	`CKT RCVRMF 0 CKT RCVRMF 1 CKT RCVRMF 2`

TRK152	The Trunk Maintenance subsystem generates this log when the Bluebox Fraud Detection feature is deactivated. Example: `TRK152 APR04 12:00:00 2112 INFO BLUEBOX DETECTION CLEARED`

Page 1 of 2

Table 4-1xxx
Log description (continued)

Log	Description

TRK153	The Trunk Maintenance subsystem generates this log when the Bluebox Fraud Detection feature is active and a fraudulent call is detected.
	
	Example:
	
	`TRK153 APR16 12:00:00 2112 INFO BLUEBOX CALL DE-TECTED`
	`IC TRUNK = CKT RTP2W 1 CALLING # = 9197811199`
	`OG TRUNK = CKT CARY2W 2 CALLED # = 61247418888`
	`CALLED # REPLACED BY 3152651234`
	`CALLID = 123456`

TRK154	The Trunk Maintenance subsystem generates this log when the Bluebox Fraud Detection feature is active and a fraudulent call is disconnected.
	
	Example:
	
	`TRK154 APR11 12:00:00 2112 INFO BLUEBOX CALL DIS-CONNECT`
	`CKT APEX2W 1`
	`CALLING # = 6133628669 2 CALLED # = 6124741888`
	`CALLID = 123456`

List of terms

AMA

Automatic Message Accounting

Automatic Message Accounting

An automatic recording system that documents all the necessary billing data of subscriber-dialed long distance calls.

Batch Change Supplement

A DMS-100 Family software release.

BCS

Batch Change Supplement

CAMA

Centralized Automatic Message Accounting

Centralized Automatic Message Accounting

A system that produces itemized billing details for subscriber-dialed long distance calls. Details are recorded at a central facility serving a number of exchanges. In exchanges not equipped for automatic number identification, calls are routed to a CAMA operator who obtains the calling number and keys it into the computer for billing.

CI

Command Interpreter

Command Interpreter

A Support Operating System component that functions as the main interface between machine and user. Its principal roles are:

1 To read lines entered by a terminal user.

2 To break each line into recognizable units.

3 To analyze the units.

4 To recognize command item-numbers on the input lines.

5 To invoke these commands.

Maintenance and Administration Position

A group of components that provide a man-machine interface between operating company personnel and the DMS-100 Family systems. A MAP consists of a Visual Display Unit and keyboard, a voice communications Module, test facilities, and MAP furniture. MAP is a trademark of Northern Telecom.

MAP

Maintenance and Administration Position

MF

Multifrequency

MFR

Multifrequency Receiver

Multifrequency

A method that makes use of pairs of standard tones to transmit signaling codes, digit pulsing, and coin-control signals.

Northern Telecom Practice

A document that contains descriptive information about the DMS-100 Family hardware and software Modules, and Performance Oriented Practices for testing and maintaining the system. NTP's are supplied as part of the standard documentation package provided to an operating company.

NTP

Northern Telecom Practice

PEC

Product Engineering Code

Product Engineering Code

An eight character code that provides a unique identification for each marketable product manufactured by Northern Telecom.

SF

Single Frequency

Single Frequency

A signaling method using a 2600 Hz tone to transmit and receive on-/off-hook address and supervisory signals. SF is used in conjunction with E and M signaling on four-wire trunk facilities.

TOPS

Traffic Operator Position System

Traffic Operator Position System

A toll operator’s position consisting of a video display and keyboard for monitoring call details and entering routing and billing information. TOPS is a trademark of Northern Telecom.

DMS-100 Family

Blue Box Fraud Detection

Feature Description

Publication number: 297-1001-132
Product release: BCS22 and up
Document release: Standard 02.02
Date: March 1991

Published simultaneously in Canada and the United States by Northern Telecom.