Temporary Document TD3/11- Ottawa(99) - ___

ITU-Telecommunication Standardization Sector

Ipswitch October 12, 2000

QUESTIONS:	Q24/4
SOURCE:	Q24/4 Rapporteur group
	LIASON TO ETSI FOR FORWARDING TO 3GPP TSG-SA3

APPROVAL:	Not yet Approved by Working Party 5/4
FOR:	Information and Response
DEADLINE for REPLY:	January 2001
CONTACT:	G. Caryer BT The Chestnuts Rose Hill Grundisburgh Suffolk IP13 6TD, UK Tel: +44 1473 738108 Fax: +44 1473 227884 Email: geoff.caryer@btinternet.com

---

Thank you, for your response liaison "Use of the Fraud Information Gathering System" dated September 2000.

ITU-T Study Group 4 is currently developing a series of Recommendations for the X interface between IMT2000 operators belonging to different 3rd generation families. We are also considering a broader work programme for the future, on the application of TMN to 3rd generation mobile systems.

We attach the latest revision of the draft M3210.1 recommendations which address the requirements and analysis (Stage 1 and Stage 2) for the management information to be exchanged between Visited and Home Service Providers for the management of the prevention of fraud. Please note that the above requirements are protocol and implementation neutral, therefore not influenced by CAMEL or SS No.7.

However, we understand your comments and agree that this current version does not address GPRS and IP domain issues. Handling data service related information will be considered after the approval of the current draft in January 2001. We look forward for your input on the topic.

We would appreciate your suggested additions and enhancements for discussion at our next Q24/4 experts meeting which will be held during January 2001.

(Attach Draft Recommendations M.3210.1)

* Co-Issue Managers:	John Visser	Geoff Caryer
	Nortel Networks, Canada	British Telecom, UK
Phone	+1-613-763-7028	+44-1473-738108
Fax	+1-613-765-5598	+44-1473-227884
Email	jvisser@nortelnetworks.com	geoff.caryer@btinternet.com

DRAFT NEW RECOMMENDATION M.3210.1

CONTENTS

DRAFT NEW RECOMMENDATION M.3210.1

TMN MANAGEMENT SERVICES FOR IMT2000 SECURITY MANAGEMENT

Summary

This recommendation is one of the series of M.3200 TMN Management Service recommendations that provide description of management services, goals and context for management aspects of IMT2000 networks. This recommendation provides a profile for fraud management in an IMT2000 mobile network. This recommendation builds on the function sets identified in Recommendation M.3400 by defining new function sets, functions and parameters and adding additional semantics and restrictions.

Keywords

-Telecommunications Management Network (TMN)
-TMN Management Service
-International Mobile Telecommunications: IMT - 2000
-Security Management
-Fraud Detection and Containment
-Third Generation Wireless – 3G Systems

1 Introduction

Recommendation M.3210.1 provides Requirements and Analysis of the Security management (Administration) of IMT2000. The emphasis is on the X interface between two service providers and the management services needed between the two service providers to detect and prevent fraud. The methodology used in this document is based on ITU-T Recommendation M.3020.

1.1 Purpose and Scope

This recommendation describes a subset of Security Management services, identified in Recommendation M.3200 as a TMN managed area, for IMT2000 management. It describes the Requirements and Analysis of operating the Fraud Information Gathering System (FIGS) between service providers. FIGS provides the means for the Wireless service provider to monitor a defined set of subscriber activities. The aim is to enable service providers/network operators to use FIGS to limit their financial exposure to large unpaid bills produced on subscriber accounts whilst the subscriber is roaming outside their home areas.

Verification of the authenticity of the Home Network—FDS and the Visited Service Provider is beyond the scope of this management service.

2 References

1. ITU-T Recommendation Q.1701 “Framework of IMT2000 Networks”
2. ITU-T Recommendation Q.1711 “Network Functional Model for IMT2000 ”
3. ITU-T Recommendation Q.1721 “Information Flows for IMT-2000”
4. ITU-T Recommendation M.3010 “Principles for a Telecommunications Management Network”
5. ITU-T Recommendation M.3020 “TMN Interface Specification Methodology”
6. ITU-T Recommendation M.3200 “TMN Management Services”
7. ITU-T Recommendation M.3400 “TMN Management Functions”

3 Definitions, abbreviations and conventions

3.1 Definitions

The following terms are used in this Recommendation:

Visited Network	The foreign or Visited Network which provides subscriber with roaming service.
Home Network	The home network to which the wireless subscriber contracts service.
Home Network – FDS	The Fraud Detection System operated by the home network.
Service Provider	A general reference to an entity who provides telecommunications services to customers and other users either on a tariff or contract basis. A SP may or may not operate a network.
Network Operator	An organization that operates a telecommunications network. A network operator may be a Service Provider and vice versa. A network operator may or may not provide particular telecommunications services
Fraud Report	A Fraud report is the set of potential violations that the subscriber has performed that may indicate potential fraud. This typically captures threshold violations from the subscribers’ normal patterns or criteria like calling countries, high usage limits)

3.2 Abbreviations

FDS	Fraud Detection System
FIGS	Fraud Information Gathering System
GDMI	Guidelines for the Definition of TMN Management Interface
IMT2000	International Mobile Telecommunications 2000
ITU	International Telecommunications Union
MS	Management Services
N/A	Not Applicable
NML	Network Management Layer
SML	Service Management Layer
TMN	Telecommunications Management Network

3.3 Conventions Used in this Document

Symbol	Explanation
m	Mandatory
m (=)	The recipient must provide the same value in the response as provided in the request by the requestor.
o	Optional, Optionality is subject to definition according to the agreement between the two service providers, i.e., a parameter listed as optional may be made mandatory.
o (=)	Return of the value by the responder is optional; however, if the responder elects to return the value, it must be the same value supplied by the requestor in the request. Responder is not allowed to alter this field.
c	Conditional Parameter, Definition of the Condition will be specified in the notes column. A numeric suffix is used to enable reuse of the conditional statements.
c (=)	If the value is provided in the request by the requestor, the responder must provide the same value in the response.
Blank	A blank implies that the parameter is not applicable.

4 Security Management Service

4.1 Security Issues

Modern telecommunications networks, particularly mobile networks provide the potential for fraudsters to make use of telecommunication services (Voice, Data, Fax etc.) without the intent to pay. A number of different scenarios are exploited and it is up to the network operator or service provider to detect misuse where it occurs and to stop it at the earliest possible opportunity.

The scale of frauds (per day on a single account) can be substantial, especially when International or Premium rate numbers are called. The most common types of fraud that effect 3G networks are related to the ability to sell calls at below market price using stolen air-time/equipment where the user of the equipment does not intend to pay the network operator or service provider. Fraudulent subscribers often avoid payment by obtaining a handset and a subscription to a network by fraudulently giving details and justifications to the network operators/service provider. If there are not good controls within the network the subscriber can make a large volume of calls to expensive destinations and accumulate a large bill.

4.2 Management Service Description

With wireless subscribers roaming from one network operator to another (and with multiple service providers), Security Management Service becomes of paramount importance. This recommendation specifies the Security Management related information exchanged over the x reference point between two TMN Operating System (OS) s (the Visited Network and the Home Network.)

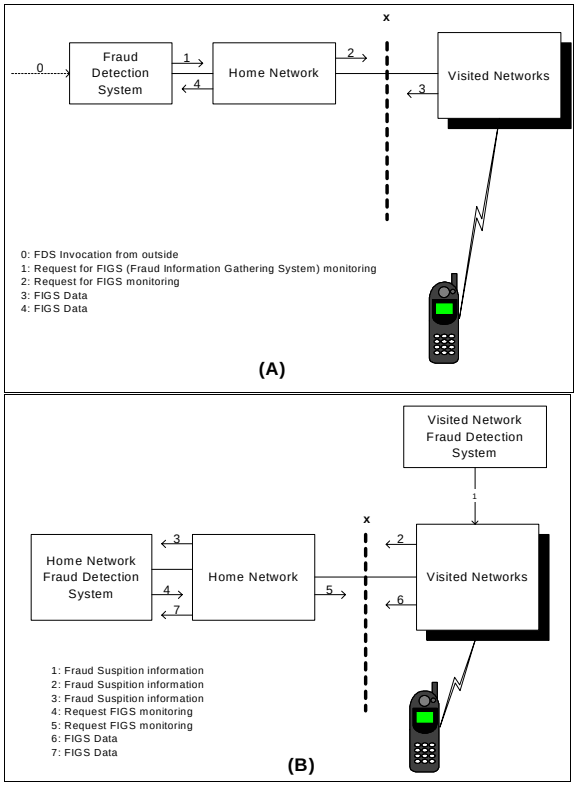

Figure 1: IMT2000 Security Management Service: Fraud Information Gathering collaboration diagrams.~~1~~

TMN relationships for IMT-2000 Security Management Service: Fraud Information Gathering are depicted in Figure 1. It shows the wireless subscriber roaming to a network of a visited service provider.

In Figure 1-A, The Home Network Fraud Detection System (FDS) requests the Visited Network to supply certain information about a subscriber from the time the subscriber registers in that Visited Network to the time the last of the monitored activities is finished in that Visited Network, which can be after the subscriber's ~~de-~~ de-registration from the Visited Network. The information received by the Home Network shall be passed to the Home Network —FDS. Analysis of this information may lead to further instructions transmitted to the Visited Network to act in an appropriate way.

Figure 1-B actions are comparable to those of Figure 1-A except that invocation of the activities is initiated by the visited service provider.

5 Management High Level Requirements

The Home Network—FDS or the Visited Network can take preventive actions to control and prevent fraudulent activities, according to the security policies. The security management services described ~~here~~in this Recommendation are applicable, across different service providers operating different or similar wireless networks. This management service provides the Visited Network and the Home Network—FDS with the capability to exchange and to control the exchange of information related to potential fraudulent activities in the Visited Network.

The Fraud Information Gathering System capabilities are categorized in the following table:

~~lated to potential fraudulent activities in the Visited Network.~~

~~In most cases,~~

~~the Visited Network obtains requests from the Home~~

~~Network—FDS~~

~~for monitoring suspicious subscriber activities. In some cases, it is conceivable that~~

~~the Home Network—FDS receives unsolicited subscriber alerts from the Visited Network, especially if the roaming subscriber continues to obtain service from the Visited Network for extended periods of time.~~

The following minimum capabilities are required:

Scope	Reference	Requirement
System Wide Capabilities	1.	FIGS Monitoring should be activated by: 1- the Visited Network obtains requests from the Home Network—FDS for monitoring suspicious subscriber activities. 2- the Home Network—FDS receives unsolicited subscriber alerts from the Visited Network, especially if the roaming subscriber continues to obtain service from the Visited Network for extended periods of time.
	2.	FIGS should not modify the Visited Network service.
	3.	FIGS should not alter any standard 3G Wireless functionality seen by the customer or affect the service quality.
	4.	FIGS Monitoring feature applies to all subscribed Bearer Services (e.g., Circuit, IP, etc.), TeleServices and Supplementary Services of the subscriber. It is not possible to apply FIGS independently to individual Services.
	5.	The information should be transferred from the Visited to the Home Network—FDS over existing communication links (e.g., TMN X Interface, SS7 signalling links).

Scope	Reference	Requirement
	6.	A mechanism is required whereby a Visited Network can charge an Home Network—FDS for the bulk data transfer made to that Home Network—FDS.
Home Network Capabilities	7.	Fraud information gathering is controlled by the Home Network—FDS and can be activated and deactivated by the Home Network—FDS only.
	8.	The Home Network shall indicate the level of fraud monitoring required: **Level 1** accelerated accounting procedure, associated with a mechanism such as real time/near real time Billing **Level 2** partial call information is gathered, but only at the beginning and the end of the call. **Level 3** full call information on subscriber activities, i.e. call start and end times, and partial call records. Notification of the invocation of Explicit Call Transfer, Call Deflection, Call Forwarding, Call Hold and Multi Party Service is also given.
	9.	The Home Network—FDS shall be able to specify whether it would like call information on Mobile Originated sessions, Mobile Terminated sessions, or both.
	10.	The Home Network should not permit the marking of new subscribers if the support of FIGS is causing overload within the Visited Network. The Visited Network should therefore handle up to a realistic limit any requests for marking of subscribers and be able to support the associated data transfer. The setting of this limit is outside the scope of this recommendation.
	11.	The Home Network should Mark a subscriber as being under FIGS monitoring.
	12.	The Home Network should receive FIGS Data from the Visited Network.
	13.	The Home Network ceases the FIGS monitoring of a subscriber's activities.
Visited Network Capabilities	14.	Based on roaming agreements, the Visited Network should advise the Home Network—FDS of information that suggests fraudulent activities.
	15.	If the Visited Network does not have the resources to support a FIGS request, it should respond accordingly to the Home Network—FDS.
	16.	Each Visited Network should limit the number of subscribers that each Home Network—FDS may request to be monitored using FIGS. Otherwise an Home Network—FDS may take more than its "fair share" of the FIGS processing capability of

Scope	Reference	Requirement
		a Visited Network.
	17.	Information should be transferred from the Visited Network to the Home Network—FDS within two minutes of the occurrence of a FIGS-monitored event. This is because up to date information is a critical part of any fraud information system. The sooner data is transferred to the Home Network—FDS; the sooner fraud can be stopped.
	18.	Based on roaming agreements, to transmit FIGS Data to the Home Network—FDS based on: 1. Frequency requested by Home Network—FDS, 2. Events specified by Home Network—FDS, and/or 3. On demand.

~~1.Fraud information gathering is controlled by the Home Network—FDS and can be activated and deactivated by the Home Network—FDS only.~~

~~2.The Home Network shall indicate the level of fraud monitoring required.~~

~~Level 1—accelerated accounting procedure, associated with a mechanism such as real time/near real time Billing~~

~~Level 2—partial call information is gathered, but only at the beginning and the end of the call.~~

~~Level 3—full call information on subscriber activities, i.e. call start and end times, and partial call records. Notification of the invocation of Explicit Call Transfer, Call Deflection, Call Forwarding, Call Hold and Multi Party Service is also given.~~

~~3.This network feature applies to all subscribed Bearer Services (e.g., Circuit, IP, etc.), TeleServices and Supplementary Services of the subscriber. It is not possible to apply FIGS independently to individual Services.~~

~~4.The Home Network—FDS shall be able to specify whether it would like call information on Mobile Originated sessions, Mobile Terminated sessions, or both.~~

~~5.The following service conditions shall apply:~~

~~□FIGS should not modify the Visited Network service,~~
~~□FIGS should not alter any standard 3G Wireless functionality seen by the customer or affect the service quality;~~
~~□If the Visited Network does not have the resources to support a FIGS request, it should respond accordingly to the Home Network—FDS.~~

~~6.Information should be transferred from the Visited Network to the Home Network—FDS within two minutes of the occurrence of a FIGS-monitored event This is because up to date information is a critical part of any fraud~~

information system. The sooner data is transferred to the Home Network – FDS; the sooner fraud can be stopped.

7. The information should be transferred from the Visited to the Home Network – FDS over existing communication links (e.g., TMN X Interface, SS7 signalling links).

FIGS system

8. should not permit the marking of new subscribers if the support of FIGS is causing overload within the Visited Network. The Visited Network should therefore handle up to a realistic limit any requests for marking of subscribers and be able to support the associated data transfer. The setting of this limit is outside the scope of this recommendation.

9. Each Visited Network should limit the number of subscribers that each Home Network – FDS may request to be monitored using FIGS. Otherwise an Home Network – FDS may take more than its "fair share" of the FIGS processing capability of a Visited Network.

10. A mechanism should be required whereby a Visited Network can charge an Home Network – FDS for the bulk data transfer made to that Home Network – FDS.

Within the Home Network to:

- Mark a subscriber as being under FIGS monitoring,

Receive

- from the Visited Network FIGS Data,
- Cease monitoring of a subscriber's activities,

Within the Visited Network:

11. Based on roaming agreements, to transmit FIGS Data to the Home Network – FDS based on:

- Frequency requested by Home Network – FDS,
- Events specified by Home Network – FDS, and/or
- On demand.

Based on roaming agreements, to advise the Home Network – FDS of information that suggests fraudulent activities.

5.1 Management Service Overview

Security Management includes the following function set groups according to M.3400

- Prevention
- Detection
- Containment and recovery
- Security Administration.

Among the function set groups of M.3400, this recommendation only addresses aspects of Detection Function Set Groups in order to detect wireless fraud.

A key list of management requirements for “Security – Audits: Counts of Fraudulent Use” includes the following:

- Determination of security related events,
- Recording of security related events
- Reporting of security related events.

Several sources of detecting security violations in a wireless network exist. The processes in place in Home Network—FDS and the Visited Network use various factors such as billing usage and pattern analysis to produce security reports. The reports and events that are exchanged between the two service providers form the basis of the detection aspects of this recommendation. The potential information contained in these reports may include: Time & date stamp, Deviation usage data, Usage data records, Alarm event reports, Subscriber Information.

5.2 Telecommunications Resources

5.2.1 Fraud Information Gathering System (FIGS)

The Home Network—FDS is provided with data on the activities of subscribers in a Visited Network by the way of using the Fraud Information Gathering System. The Home Network—FDS can make inferences about what the subscriber is doing and then take decisions on what the subscriber should be allowed to do. The following operations maybe invoked in FIGS as described in the use cases:

1. Fraud Alert: The Visited Network invokes this operation when fraud is suspected.
2. Activate information gathering: This operation starts up the process of monitoring a particular subscriber activities,
3. Report FIGS: This operation is invoked by the Visited Network to relay gathered information.
4. Deactivate information gathering: This operation concludes the process of monitoring the subscriber's activities,
5. Modify FIGS report: This operation alters the monitoring level and/or schedule of delivering subscriber activities,
6. Advice suspend FIGS Monitoring: This operation is invoked by the Visited Network to inform the Home Network—FDS that information gathering has been suspended.
7. Advise Resume FIGS Monitoring: This operation is invoked by the Visited Network to inform the Home Network—FDS that information gathering has been resumed after it was suspended.

5.2.2 Visited Network

A Visited Network (Visited Service Provider) can receive FIGS monitoring requests. A Visited Network can then perform some of the following actions:

- Activate FIGS monitoring for the requested roaming subscriber. The Home Network—FDS is then notified with reports as a result of the monitoring activities.

- The Visited Network may be overloaded, the request is suspended until monitoring capacity is restored and then FIGS monitoring is activated for the roaming subscriber requested.

5.2.3 Home Network Fraud Detection System (FDS)

The Home Network—FDS request FIGS monitoring from Visited Networks to start collecting data about particular subscriber activities.

The HN-FDS then schedules receipt of security event reports, as specified in an agreed upon time interval. Alternatively, the Home Network—FDS requests security event reports at any time from the Visited Network. In either case, security information should be delivered in as close to real time as possible.

5.3 Fraud Information Gathering Use Cases

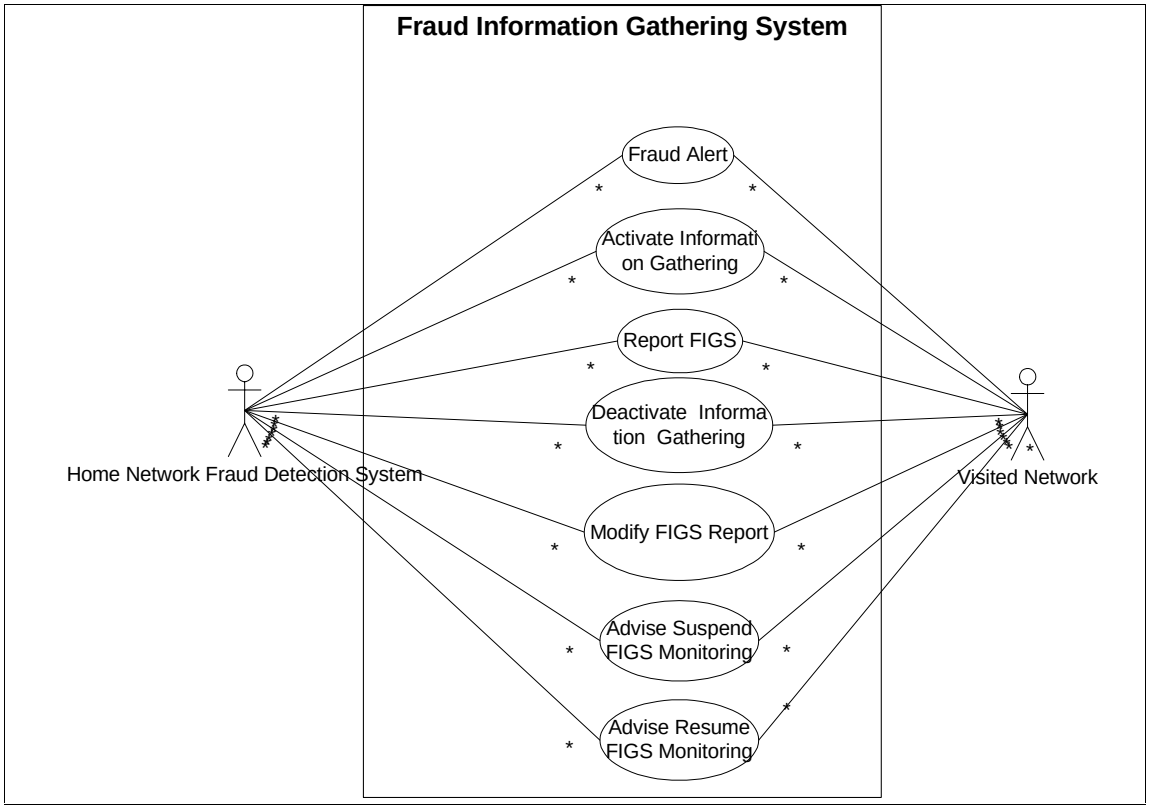

Figure 2: FIGS Use cases

5.3.1 Fraud Alert Use Case

Name	Fraud Alert
Summary	This operation is invoked by the Visited Network suspecting fraud to inform Home Network—FDS of need to initiate FIGS monitoring
Actor(s)	1. Home Network—FDS 2. Visited Network
Pre-Conditions	Subscriber Fraud suspected
Begins When	Subscriber roams to Visited Network
Description	After a particular subscriber roam in a Visited Network, the Visited Network may inform the subscriber Home Network—FDS that it suspects fraudulent use. This alert may be the result of the roaming subscriber following an unusual usage pattern, for example.

Name	Fraud Alert
Ends When	N/A
Exceptions	N/A
Post-Conditions	FIGS Monitoring requested Fraud no longer suspected Subscriber device deactivated
~~**Traceability**~~	~~This use case fulfils the following requirements: 1, and 14~~
Traceability	This use case fulfils the following requirements: 1

5.3.2 Activate Information Gathering Use Case

Name	Activate Information Gathering
Summary	This operation initiate the request to start up the process of monitoring a particular subscriber activities
Actor(s)	Home Network—FDS Visited Network
Pre-Conditions	Subscriber Fraud suspected
Begins When	Receive request from either: Home Network—FDS Visited Network request
~~**Description**~~	~~Request is accepted and passed to the Visited Network~~
Description	The Home Network—FDS may find it necessary to monitor a particular subscriber. This decision may be in response to the Visited Network Fraud Alert message.
Ends When	Home Network—FDS request to terminate subscriber monitoring
Exceptions	Visited Network is unable to initiate monitoring
Post-Conditions	Fraud no longer suspected Subscriber device deactivated
Traceability	This use case fulfils the following requirements: 1, 8, 9, 10, 12 and 15 ~~1, 2, 3, 4, 7, 8 and 14~~

5.3.3 Report FIGS Use Case

Name	Report FIGS
Summary	This operation is invoked by the Visited Network to relay gathered information to the Home Network—FDS
Actor(s)	1. Home Network—FDS 2. Visited Network
Pre-Conditions	Subscriber Fraud suspected
Begins When	Subscriber roams to Visited Network
Description	The Visited Network accumulates information about roaming subscriber usage for the Home Network—FDS. This information is only gathered based on the Home Network request to activate the subscriber monitoring. This information is then transmitted to the home network based on the set criteria.
Ends When	When FIGS monitoring is deactivated or FIGS is suspended because of Visited Network overload.
Exceptions	N/A
Post-Conditions	Fraud no longer suspected Subscriber device deactivated
Traceability	This use case fulfils the following requirements: 2, 3, 4, 5, 6, 7, 12, 13, 14, 15, 17 and 18.~~2, 5, 6, 9, 11, 13, and 14~~

5.3.4 Deactivate Information Gathering Use Case

Name	Deactivate Information Gathering
Summary	This operation is invoked by the Home Network—FDS to request terminating the process of monitoring the visiting subscriber's activities
Actor(s)	~~3.~~1. Home Network—FDS ~~4.~~2. Visited Network
Pre-Conditions	Either case is reached: • Subscriber Fraud not suspected • Subscriber finished roaming
Begins When	Receive request from the Home Network—FDS
Description	Request is accepted and passed to the Visited Network
Ends When	N/A
Exceptions	N/A
Post-Conditions	Fraud no longer suspected Subscriber device deactivated
Traceability	This use case fulfils the following requirements: 7, and 13 ~~1, 4, 7, 8, 10 and 12~~

5.3.5 Modify FIGS Report Use Case

Name	Modify schedule for delivering Fraud Information

Name	Modify schedule for delivering Fraud Information
Summary	The Home Network – FDS sends request to the Visited Network asking to modify the frequency of delivering monitoring reports.
Actor(s)	~~5.~~1. Home Network—FDS ~~6.~~2. Visited Network
Pre-Conditions	• FIGS monitoring is in progress for a ~~S~~subscriber • Home FDS requires subscriber activities to be monitored at a different level or on a different schedule than identified in the roaming agreement.
Begins When	Receive request from the Home Network—FDS
Description	The Home Network—FDS may find it necessary to change: a) the schedule of delivering the monitoring reports of a particular subscriber, b) the level of fraud monitoring required. ~~Request is accepted and passed to the Visited Network~~
Ends When	Request is accepted and passed to the Visited Network
Exceptions	Visited System cannot process request
Post-Conditions	New delivery schedule or monitoring level is established
Traceability	This use case fulfils the following requirements: 8 and 18. ~~1, 2, 4, 5, 6, 10 and 13~~

5.3.6 Advise Suspend FIGS Monitoring Use Case

Name	Advise Suspend FIGS Monitoring
Summary	This operation is invoked by the Visited Network to inform the Home Network—FDS of suspending the collection of FIGS information because of resource shortage.
Actor(s)	~~7.~~1. Home Network—FDS ~~8.~~2. Visited Network
Pre-Conditions	Subscriber ~~F~~fraud suspected and Visited Network resources are short.
Begins When	Visited Network resources cannot meet the demand to monitor existing roaming subscribers
Description	The Visited Network monitoring resources may suffer from resource shortage. This may be the result of increased activities of a large number of roamers being monitored, for example. Consequetly, a message is send to some of the subscribers' Home Network informing them that monitoring is being suspended.
Ends When	Visited Network normal condition is restored and a message advising the Home Network of resuming the monitoring gets sent.
Exceptions	N/A
Post-Conditions	Fraud no longer suspected Subscriber device deactivated

Name	Advise Suspend FIGS Monitoring
Traceability	This use case fulfils the following requirements: 10, 15 and 16. ~~1, 2, 4, 7 and 8~~

5.3.7 Advise Resume FIGS Monitoring Use Case

Name	Advise Resume FIGS Monitoring
Summary	This operation is invoked by the Visited Network to inform the Home Network—FDS of the resumption of collecting FIGS information.
Actor(s)	1. Home Network—FDS 2. Visited Network
Pre-Conditions	Subscriber Fraud suspected
Begins When	Subscriber roams to Visited Network
Description	Visited Network resources are restored and can resume monitoring existing tagged roaming subscribers
Ends When	Subscriber monitoring is ended or Visited Network FIGS System overload reoccurs.
Exceptions	N/A
Post-Conditions	Fraud no longer suspected Subscriber device deactivated
Traceability	This use case fulfils the following requirements: 10, 15 and 16. ~~1, 2, 4, 7 and 8~~

6 Management Functions Analysis

This section provides the high level description for the FIGS Security Management service. That is, it provides the messages needed to support the management functions for requesting and collecting security related information between service providers.

6.1 Fraud Information Gathering Function set

FIGS function set supports a service provider request and reporting of usage data from other service provider. Table 1 lists FIGS functions to illustrate the management activity originator and recipient.

	Function	Originator	Responder
1.	Fraud Alert function	Visited Network	Home Network—FDS
2.	Activate Information Gathering function	Home Network—FDS	Visited Network
3.	Report FIGS function	Visited Network	Home Network—FDS
4.	Deactivate Information Gathering function	Home Network—FDS	Visited Network
5.	Modify FIGS reporting schedule function	Home Network—FDS	Visited Network
6.	Advise Suspend FIGS Monitoring function	Visited Network	Home Network—FDS

	Function	Originator	Responder
7.	Advise Resume FIGS Monitoring	Visited Network	Home Network—FDS

Table 1: FIGS function sets interactions

6.2 Object Classes and State Chart

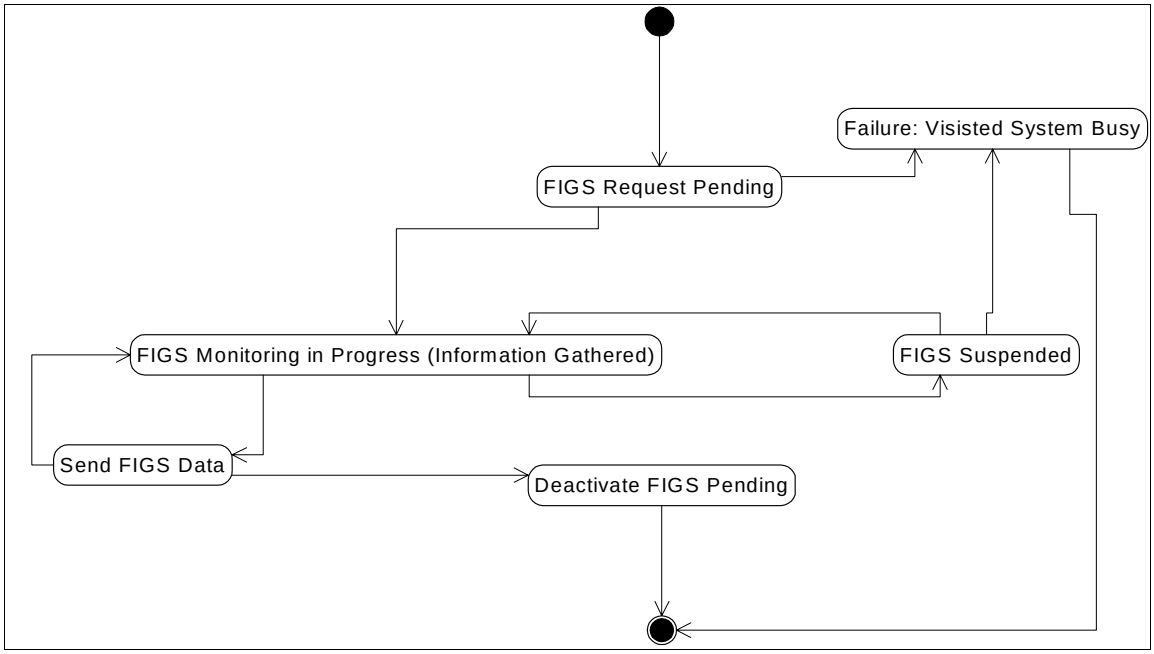

Figure 3: FIGS State Diagram

The state machine describing FIGS related interaction is illustrated in the diagram in Figure 3. As messages are exchanged between the Visited Network and the Home Fraud Detection System, the message link between them may be situated in one of the states listed.

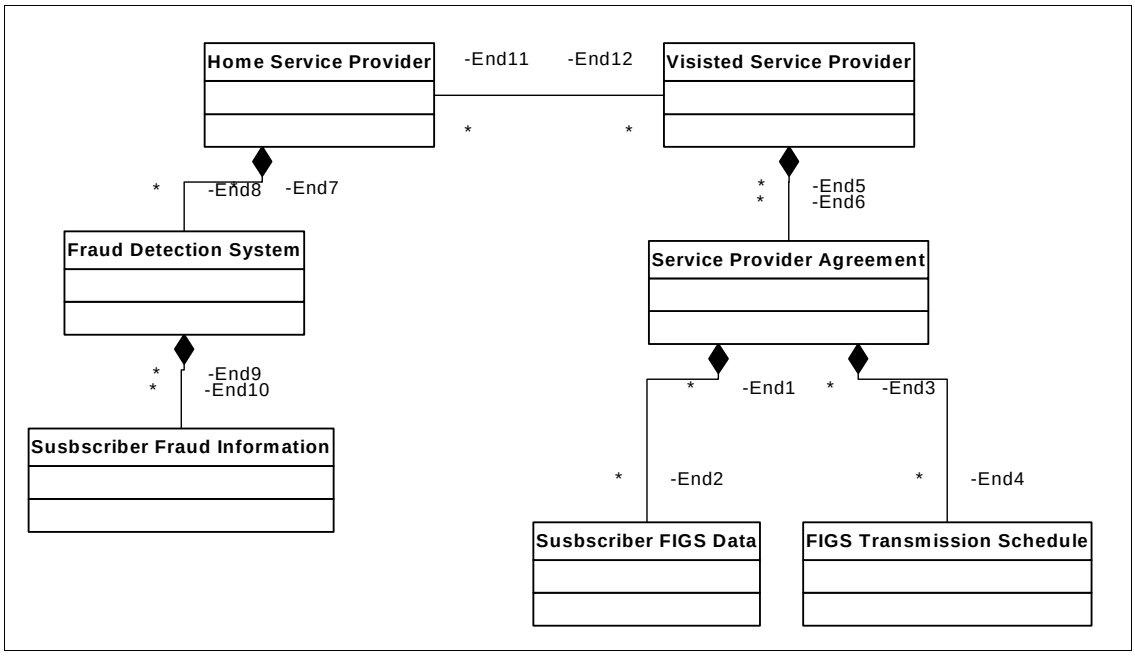

Figure 4: FIGS Class Diagram

6.3 Fraud Information Gathering Functions and Sequence Diagrams

6.3.1 Fraud Alert Function

After a particular subscriber roam in a Visited Network, the Visited Network may inform the subscriber Home Network—FDS that it suspects fraudulent use. This alert may be the result of the roaming subscriber following an unusual usage pattern, for example.

Figure 5: Alert Message flow

Consequently, the Home Network—FDS is informed. In this scenario, shown in Figure 5, the Visited Network informs the Visited Network of particular roaming subscriber.

6.3.1.1 Information Flow

	Home Network FDS	Visited Network	Notes
3G User Identification List		m	List of unique identification of the wireless subscriber e.g. (International Mobile Subscriber Identity(IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number		m	The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.

Table 2: Fraud Alert exchanged information

The information exchanged for Fraud Alert is detailed in Table 2.

6.3.2 Activate Information Gathering Function

The Home Network—FDS may find it necessary to monitor a particular subscriber. This decision may be in response to the Visited Network Fraud Alert message for example. In this scenario, the Home Network—FDS requests from the Visited Network to monitor a particular roaming subscriber. The Visited Network is required to acknowledge the receipt of this request.

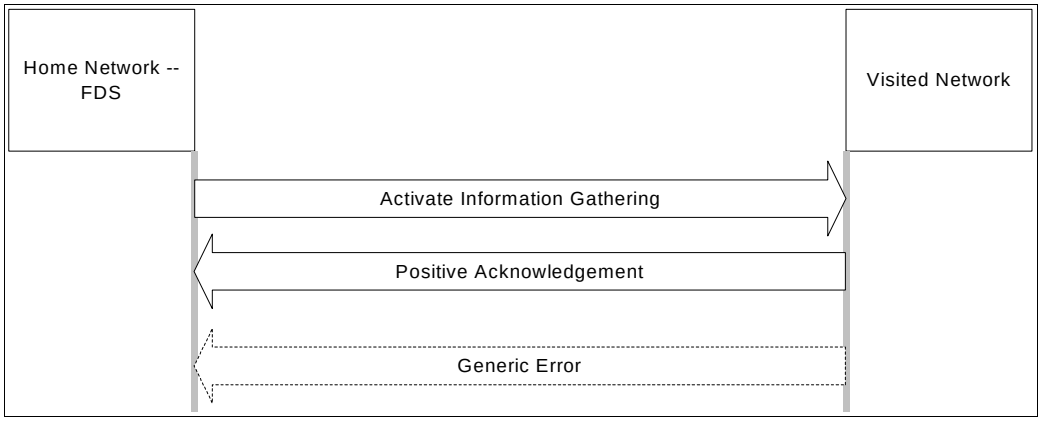

Figure 6: Message flow to Activate FIGS

The request to activate information gathering is only initiated by the Home Network FDS and transmitted to the Visited Network as shown in Figure 6.

6.3.2.1 Information Flow

	Home Network FDS	Visited Network	Notes
3G User Identification List	m		List of unique identification of the wireless subscriber e.g. (International Mobile Subscriber Identity(IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number	m		The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
Activate FIGS reason	c		Reason Code : - Fraud is suspected, - Other.
Level of Monitoring Required	m		Level of Monitoring Level 1 – (near) real time billing Level 2 – partial call records Level 3 - full call records
Confirmation		m	Result code: R0: other R1: Success R2: Unknown subscriber(s)

Table 3: Activate FIGS exchanged information

The information exchanged for ~~Fraud Alert~~ Activate FIGS is detailed in Table 3.

6.3.3 Report FIGS Function

The Visited Network accumulates information about roaming subscriber usage for the Home Network—FDS. This information is only gathered based on the Home Network request to activate the subscriber monitoring.

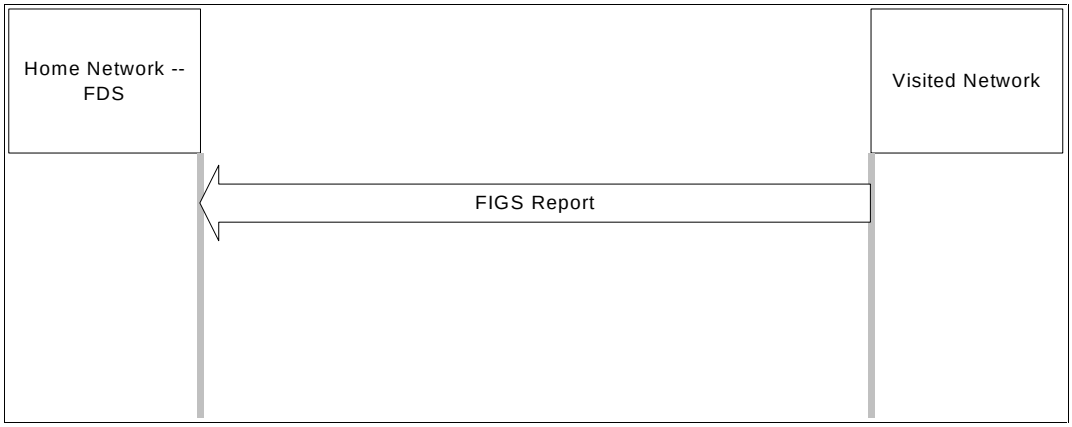

Figure 7: Message flow to send information

In this scenario, shown in Figure 7, the Visited Network sends the Home Network—FDS particular roaming subscriber information periodically.

6.3.3.1 Information Flow

	Home Network FDS	Visited Network	Notes
3G User Identification List	m		List of unique identification of the wireless subscriber e.g. (International Mobile Subscriber Identity(IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number	m		The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
FIGS Report	c		Reason Code : - Fraud is suspected, - Other.
Confirmation		m	Result code: R0: other R1: Success R2: Unknown subscriber(s)

Table 4: Report FIGS information

The Report FIGS information ~~exchanged for Alert~~ is detailed in ~~Table 3~~ Table 4.

6.3.4 Deactivate Information Gathering Function

The Home Network—FDS may find it necessary to terminate monitoring a particular subscriber. This decision may be a result of determining that a subscriber usage pattern is verified to be ordinary. In this scenario, the Home Network—FDS requests from the Visited Network to terminate the monitoring of a particular roaming subscriber. The Visited Network is required to acknowledge the receipt of this request and to terminate the monitoring.

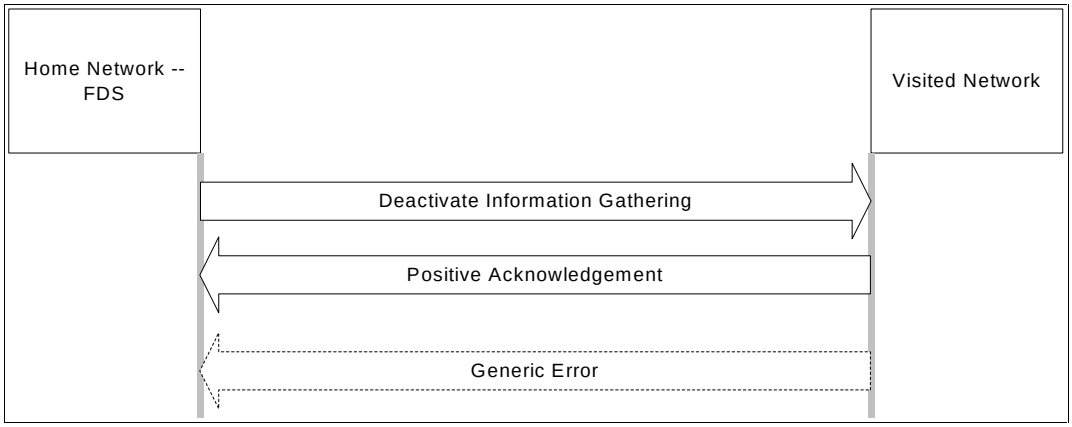

Figure 8: Message flow to deactivate FIGS

The request to deactivate information gathering is only initiated by the Home Network FDS and transmitted to the Visited Network as shown in Figure 8.

6.3.4.1 Information Flow

	Home Network FDS	Visited Network	Notes
3G User Identification List	m		List of unique identification of the wireless subscriber e.g. (International Mobile Subscriber Identity(IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number	m		The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
Deactivate FIGS reason	c		Reason Code : 1. Fraud is detected – Subscriber suspended, 2. No Fraud is concluded.
Confirmation		m	Result code: R0: other R1: Success R2: Unknown subscriber(s)

Table 5: Deactivate FIGS exchanged information

The Deactivate FIGS information exchanged is detailed in Table 5.

6.3.5 Modify FIGS Report Function

The Home Network—FDS may find it necessary to change the schedule of delivering the monitoring reports of a particular subscriber. This decision may be a result of overload condition.

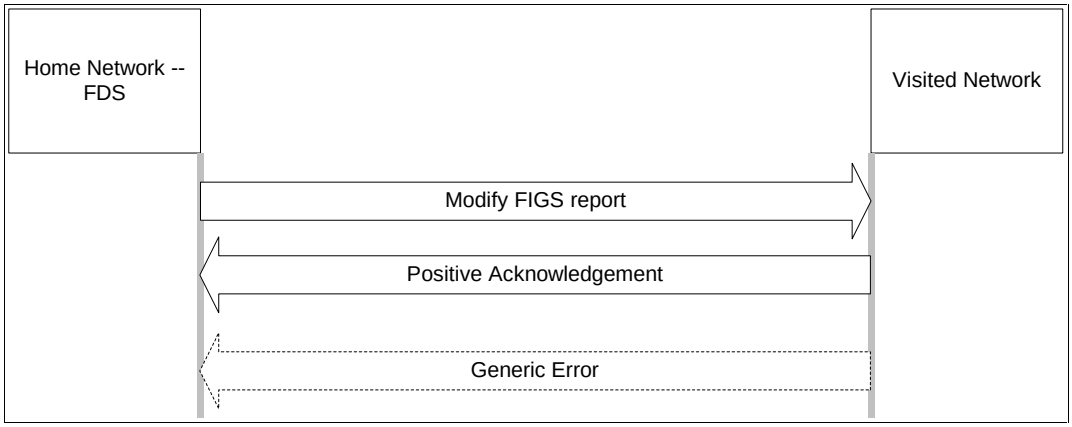

Figure 9: Message flow to change reporting schedule

In this scenario, shown in Figure 9,the Home Network—FDS requests from the Visited Network to change the reporting schedule. The Visited Network is required to acknowledge the receipt of this request and to alter the reporting schedule.

6.3.5.1 Information Flow

	Home Network FDS	Visited Network	Notes
3G User Identification List	m		List of unique identification of the wireless subscriber e.g. (International Mobile Subscriber Identity(IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number	m		The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
New Schedule	c		If the modification request is for a change of schedule, this element is mandatory Choice of: - Time Interval, - Absolute times.
New Monitoring Level	c		If the modification request is for a change of monitoring level, this element is mandatory Choice of: Level 1 Level 2 Level 3
Confirmation		m	Result code: R0: other R1: Success R2: Unknown subscriber(s)

Table 6: Modify FIGS Reporting ~~Schedule~~ exchanged information

The Modify FIGS Reporting exchanged information is detailed in **Table 6**.

6.3.6 Advise Suspend FIGS Monitoring Function

The Visited Network monitoring resources may suffer from shortage. This may result the increased activities of a large number of roamers being monitored, for example.

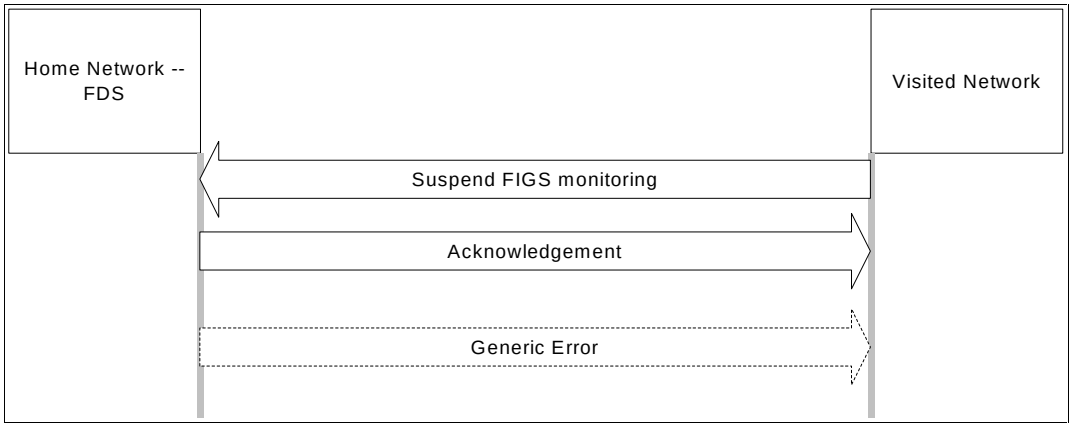

Figure 10: Message flow to Suspend FIGS

Consequently, as shown in Figure 10, selected subscribers monitoring may be suspended and the Home Network—FDS is informed. In this scenario, the Home Network—FDS informs the Visited Network of its decision to suspend the monitoring of particular roaming subscriber information.

6.3.6.1 Information Flow

	Home Network FDS	Visited Network	Notes
3G User Identification List	m	m=	List of unique identification of the wireless subscriber e.g. (International Mobile Subscriber Identity(IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number	m	m=	The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
Suspend service code	m		Reason code : - System Problems - Other
Confirmation		m	Confirmation code : r0: other r1: Success r2: Unknown subscriber

Table 7: Advise suspend FIGS exchanged information

The information exchanged between the Home Network—FDS and the Visited Network to suspend the monitoring of a roaming subscriber detailed in Table 7.

6.3.7 Advise Resume FIGS Monitoring Function

When the Visited Network monitoring resources are restored after shortage, monitoring of suspended roaming subscribers is resumed. The Home Network—FDS is informed.

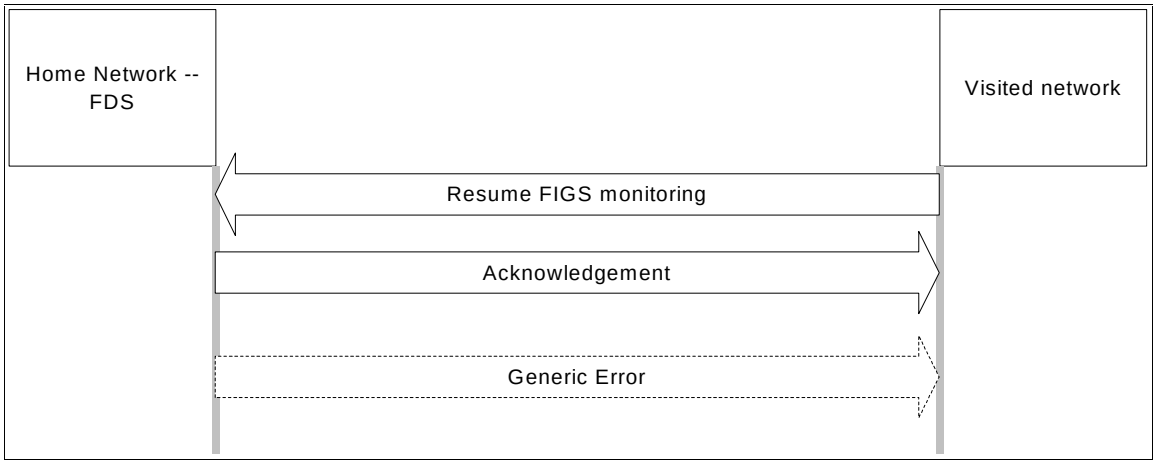

Figure 11: Message flow to Resume FIGS

In this scenario, as shown in Figure 11, the Visited Network informs the Home Network—FDS of its decision to resume monitoring of the previously suspended roaming subscriber.

6.3.7.1 Information Flow

	Home Network FDS	Visited Network	Notes
3G User Identification List	m	m=	List of unique identification of the wireless subscriber e.g. (International Mobile Subscriber Identity(IMSI) or Universal Personal Telecommunications Number)
Electronic Serial Number	m	m=	The Electronic Serial Number of the subscriber terminal as defined in the wireless signalling standards.
Resume service code	m		Reason code : - System restored - Other
Confirmation		m	Confirmation code : r0: other r1: Success r2: Unknown subscriber

Table 8: Advise Resume FIGS exchanged information

The Advise Resume FIGS exchanged information is detailed in Table 8.

Annex A: Fraud Management Criteria (Informative)

Telecommunication Management Networks need to provide the management means to detect and analyse security violations and include security aspects that evolve from the mobility of customers. Examples of detecting fraudulent use may be the result of:

- Analysis of collected subscriber information on a customer suspected of security violations such as simple MIN/ESN cloning
- Analysis of collected network information on the network to detect a suspected security violation
- Customer usage pattern analysis indicating a significant variation from normal usage patterns
- Internal traffic and activity pattern analysis that results in the detection of a customer or user (external or internal) security violation.

Fraudulent use may or may not be a consequence of the following detected failures:

- Network failure to decrypt customer-encrypted messages
- Customer failure to produce correct responses to authentication challenges
- Mismatches in the customer-reported value of the “call-count” parameter
- Failure reports indicating difficulty in updating users Shared Secret Data (SSD)

Annex B: Information Transferred by the Visited Network

Information	Description
Dialled digits	The D**ialled digits** are required as these are an important indicator in deciding if a call is fraudulent or not - certain call destinations are more likely to be called fraudulently than others.
A subscriber	**A subscriber** can be used to identify the subscriber
B,C subscriber	**B, C subscriber** are relevant as some call destinations are more subject to fraud than others
CGI	Cell Global Identifier (**CGI**) is relevant as some cells in a PLMN are more subject to fraud than others.
IMSI	The **IMSI** is used to reference the subscriber.
IMEI	The **IMEI** can be used to check if a stolen handset has been used.
Call Start Time/Date	The **Call Start Time/Date** is required so that the call duration can be calculated (if the call end time and not call duration is given at call conclusion) and because the call start time can also an important indicator of fraudulency.
Call Duration	The **Call Duration** gives the duration of the call at the sending of the partial call information - call duration can be an important indicator of fraudulency. If call end is sent instead, the duration can be calculated using the call start and end times.
Call Reference	The **Call Reference** is used to reference a particular call.
MO/MT indicator	The **MO/MT indicator** is required because call charging is different for MO and MT calls.
Visited MSC address	The **Visited MSC address** gives the PLMN on which the call was made.
Type of SS event	The **Type of SS event** record is sent if the “call” start is actually the invocation of a supplementary service, e.g. ECT. The Type of SS event is required as this can help to indicate if the mobile is being fraudulently used or not.
Type of Basic Service	The **Type of Basic Service** indicates whether a teleservice or bearer service is being used and which sort of teleservice or bearer service is being used and is sent if the event is a call and not a supplementary service. The Type of Basic Service is required as this can help to indicate if the mobile station is being fraudulently used or not.