COMPAQ

Software Product Description

PRODUCT NAME: Compaq Fraud Management System, Version 7.0 **SPD: 61.40.05**

DESCRIPTION

Compaq Fraud Management System is a fraud management platform that provides detection, analysis, and decision support functions for communications service providers, both fixed line and wireless. Fraud Management System provides support for IP and next generation data networks, as well as traditional voice networks. Compaq Fraud Management System detects and analyzes fraud and recommends fraud counteractions.

Fraud Management System detects fraud by reading and analyzing various defined streams of call and/or event information, including the same stream of call detail records that is used for billing purposes. Fraud Management System detects anomalies within the data and automatically generates alarms. Fraud Management System then analyzes these alarms and identifies likely fraudulent behavior. This information is then presented to a fraud analyst in case form using a window-based graphical user interface. As part of its detection function, Fraud Management System builds individual profiles for each customer, which provides a longer-term view of how each customer uses their different services. This is used to enhance the accuracy of detection.

Fraud Management System can be customized by defining parameters based on unique business and operator policies. Fraud Management System uses these parameters to determine if anomalies represent evidence of fraud, prioritize fraud cases, and define recommendations for counteractions. These parameters also determine the behavior of the Fraud Management System's case management and decision support features in instances of suspected fraud. Actions can be changed at any time, activated automatically, or suppressed if manual review is preferred.

FEATURES

Data Reduction

Fraud Management System analyzes and in a stepwise manner, eliminates extraneous data from the fraud management process. Data that is not relevant for fraud management purposes is filtered in multiple stages leaving fraud-related data for detailed analysis and presentation to the users. In the first stage, the set of all calls and events is analyzed by a detection mechanism, a subset of which generates alarms when suspicious behavior or anomalies are found. In the second stage, the Fraud Management System assesses the alarms to produce a still smaller subset of data that is arranged into cases.

Detection

Detection is achieved through a variety of techniques. Each technique can be tuned with user-accessible parameters to reflect the business policies of the operator. The detection techniques employed include:

- New subscriber checks – behavior of new customers are check against known characteristics that indicate a likelihood of subscription fraud.

- Thresholds --- observed behavior is checked for breach of any of a series of thresholds for duration of calls, number of calls, cost of calls, or volume of data in a transaction. Thresholds are applied for operator-defined customer groups, for any types of calls or events desired by the operator.
- Call Collision/Overlap --- incidence of two or more concurrent calls from a single customer is detected.
- Geography --- detects unlikely travel times indicated by a series of two or more calls originated within a given period of time from geographically separate points by a single customer.
- Call Patterns --- operator-defined values for any field or fields in the call detail record that indicate fraud. Any call or event record matching the specified pattern is detected. The operator can create, maintain or change patterns.
- Service Patterns --- operator-defined values for any field or fields in the customer data that indicate fraud. Any service record matching the specified pattern is detected. The carrier can create, maintain, or change patterns.
- Unknown Customer and Suspension Checking --- detect calls or transactions made by an unknown customer, as well as any calls in violation of known suspension or authorization levels currently in place for a customer.
- Profile Comparison --- potentially fraudulent behavior is compared to the customer's normal usage profile to avoid false positive identification. Profile comparison is conducted on an individual service level, and optionally at the number level (for multiple-number services).
- Destination Tracking --- the system keeps a history of calling patterns for each customer. Calls made to operator-specified country and area/city codes not within the customer's normal calling pattern are evaluated as indicators of potential fraud.
- Black List Checking -- the system compares all calls with up to five operator-defined black lists, including destination number, equipment number, etc. Any call that matches entries on the black lists is detected as an indicator of potential fraud.

External Alarms

Interface to allow Fraud Management System to analyze alarms generated outside of Fraud Management System. Examples include SS7 surveillance systems, pre-call registration, subscriber credit scoring, etc. Interfaces to external systems are determined based on unique operator requirements.

Profiling

Fraud Management System builds and maintains usage profiles for every customer of the operator. Profiles are based upon a period of observed behavior that is determined based upon operator requirements. The profile includes information about call frequency, call times, domestic or international calling, call duration, calls to specific country/area codes, charges incurred, data volumes, and wireless home/roaming behavior, as required and defined by the operator.

Because subscribers in wireless GSM networks can have multiple numbers (for voice, FAX, data, etc.), Fraud Management System will optionally track usage at the individual number level within a given service.

Partitioning

Fraud Management System allows the installation to divide up the customer base into subsets, each of which can be managed as a group. An operator may choose to define partitions based on types of service or network, region or market. Additionally, customers for multiple (perhaps competing) operators can be maintained in the same Fraud Management System installation (Service Bureau) with complete data separation and confidentiality.

Worklists

Fraud Management System creates a set of cases of suspected fraudulent activity that are reviewed by Fraud Analysts. An analyst will have a personal worklist, and may also share a worklist within a group of analysts. Fraud Analysts review cases that appear on their worklist. As cases of suspected fraud are created by the system, they are placed onto a worklist for the appropriate person or group, as specified by the operator. An operator may choose to route a case to a particular worklist for reasons of case specialization, security, etc.

Rule Based System

Fraud Management System relies on a rule-based system (often called an expert system) to perform a detailed analysis of a customer once unusual or suspicious activity is detected. A graphical editor is provided for the operator to view the rules defined in the Fraud Management System, make changes to these rules, or define additional rules which customizes the analysis, findings, suggested actions, and worklist assignments based on the policies and procedures of the operator.

Neural Network System

Fraud Management System also utilizes an optional Neural Network component to analyze suspected cases of fraud against historical case data to render a second determination of whether the current situation is likely to be fraud or not. This allows Fraud Management System to look at longer-term trends and obscure patterns that determine the presence of fraud. The neural network is "trained" using the Case Archive (below).

Case Archive

Fraud Management System provides an archive to store information about cases, whether they actually represented fraud or not. This archive is useful for query during investigation of subsequent suspicious activity. This Case Archive is also used by an optional neural network component to discover previously unknown predictors of whether a given type of situation is likely to be fraud or not fraud.

Decision Support

Fraud Management System compiles all data related to an instance of suspected fraud into a case. Based on parameters reflecting operator business policy, Fraud Management System prioritizes cases and recommends appropriate counter-action. These actions can be automatically or manually invoked. Fraud Management System provides supporting details for its recommendation that the Case Manager can review on demand.

Link Analysis and Call Tracer

To aid fraud case investigation, Fraud Management System provides functionality to perform link analysis using calls from the Call Archive, allowing users to chain their way in either direction from a desired target number,

- Displaying in graphical form all numbers called by the target
- Reversing direction, and displaying in graphical form all numbers that called the target
- Iterate through multiple levels of linkage.

This is a valuable tool for the early detection of fraud "rings" – collections of fraudsters that call common numbers or each other. If a subscriber is a known fraudster, then any one who calls or is called by the fraudster is more likely to have a higher level of suspicion.

Customer Information System Interface

Fraud Management System has an interface that allows it to read information directly from the customer administration or billing system. The customer information that is made available within Fraud Management System for use during detection and case analysis can be customized.

Operator-specific Parameters

Fraud Management System conducts its detection, analysis, and recommendation tasks in accordance with system settings and parameters. Fraud Management System allows the operator to change settings governing detection techniques, detailed analysis, policies, and recommendations.

Security

Only defined users may have access to Fraud Management System. Access for all users is password protected. Fraud Management System provides seven types of secured functional access:

- Case Manager --- basic analyst access.
- Call Archive – query capability in the call archive
- Link Analysis – access to the Link Analysis and Call Tracer features
- Knowledge Manager --- access to parameters that define fraud management policy.
- System Manager --- access to parameters for system configuration and application tuning.

- Custom Toolbar – access to a customized part of the graphical user interface which interfaces to external applications as defined by the operator
- Security Manager --- access to user and security administration.

INSTALLATION REQUIREMENTS

Fraud Management System should be installed by qualified Fraud Management System integration professionals only. The prerequisite systems integration activities and installation processes include steps for:

- defining fraud management policies so they can be reflected in system settings and parameters
- integration with a source of call or event data, including deployment of software to perform call detail record format conversion
- integration with a source of customer or line information, such as a customer care or billing system
- identifying, planning, and implementing for any required integration and customization
- user training and organizational acceptance

HARDWARE REQUIREMENTS

Platforms Supported

Fraud Management System is installed on a central server that is accessible by desktop clients via TCP/IP.

Server: Fraud Management System is deployed on 64-bit Compaq AlphaServer platforms. Supported platforms include AlphaServer ES and GS series supporting Compaq Tru64 Unix. Processor and memory requirements are determined by several factors, including the size of customer base and call or event volumes to be processed.

Desktop Client: The desktop device must be a Windows 2000, Windows 98 or Windows NT (Version 4 or later). The desktop clients access the server's databases using ODBC and CORBA technology.

Disk Space Requirements

Disk requirements are determined on an operator by operator basis, based on volumes and archive storage requirements.

SOFTWARE REQUIREMENTS

Server operating system: Compaq Tru64 UNIX Version 5.1 or later
Client operating system: Microsoft Windows2000, Windows 98, or Windows NT V4.0; with Internet Explorer 5.0
Database software: Oracle 8.1.7
ODBC software: OpenLink Software, Inc. ODBC Enterprise Edition V3.2 (license only)
Neural Network: MATLAB and Neural Network Toolbox, Release 12**

** Fraud Management System can be run without MATLAB by bypassing the neural network analysis component.

SOFTWARE LICENSING

This software is furnished only under a license. This product does not provide support for the Compaq Tru64 UNIX License Management Facility. A Product Authorization Key (PAK) is not required for installation or use of this version of the product. The following terms supersede Compaq's standard Concurrent Use License terms:

This software is offered under 2 categories of Concurrent Use Licenses, either **per-customer** or **per-event**. Each has 2 sub-categories related to the size of the workload being analyzed by the system. All licenses are limited to a site (mailing address). Once a license has been purchased for a given site, the software may be copied onto any system in that site for purposes of licensed use. A customer must have purchased sufficient licenses to cover the total workload being analyzed at a site, whether the workload existed at initial installation time or was added later.

Per-customer licenses are for sites analyzing workloads specified in terms of customer units. Licensed workloads may be any combination of unit types. The following weights apply to calculate the total workload requiring license coverage at each site.

1 customer unit = any of the following:
- 1 postpaid wireless subscriber, or
- 1 postpaid fixed-line billing number, or
- 2 prepaid wireless subscribers, or
- 2 prepaid fixed-line customers

For sites with workloads up to the first 4 million customer units, order the following part numbers:

Part Number	Customer Units
QL-6T2AM-3C	50,000
QL-6T2AM-3D	100,000
QL-6T2AM-3E	500,000

For sites with workloads greater than 4 million customer units, order the following part numbers (the customer MUST have pre-requisite licenses for the first 4 million customer units):

Part Number	Customer Units
QL-6T2AM-3F	50,000
QL-6T2AM-3G	100,000
QL-6T2AM-3H	500,000

Per-event licenses are for sites analyzing workloads specified in terms of event units. Event units are expressed in terms of events/day and are averaged over a 1-week time frame. Licensed workloads may be any combination of unit types. The following weights apply to calculate the total workload requiring license coverage at each site.

1 event unit = any of the following:
- 1 postpaid wireless call/event, or
- 1 postpaid fixed-line call/event, or
- 2 prepaid wireless calls/events, or
- 2 prepaid fixed-line calls/events

For sites with workloads up to the first 40 million event units, order the following part numbers:

Part Number	Event Units
QL-6T3AM-3C	500,000
QL-6T3AM-3D	1,000,000
QL-6T3AM-3E	5,000,000

For sites with workloads greater than 40 million event units, order the following part numbers (the customer MUST have pre-requisite licenses for the first 40 million event units):

Part Number	Event Units
QL-6T3AM-3F	500,000
QL-6T3AM-3G	1,000,000
QL-6T3AM-3H	5,000,000

GROWTH CONSIDERATIONS

The minimum hardware and software requirements for any future version of this product may be different from the requirements for the current version.

DISTRIBUTION MEDIA

CD ROM (write once compact disc).

Part Number	Description
QA-5HHAA-H8	Fraud Management System CD Media Kit

SOFTWARE WARRANTY

This software is provided by Compaq with a 90 day conformance warranty in accordance with the Compaq warranty terms applicable to the license purchase.

SOFTWARE PRODUCT SERVICES

A variety of service options are available from Compaq. For more information, contact your local Compaq office.

NOTICE