

# HP Fraud Management System

## Features and Functions List

### Version 8.1

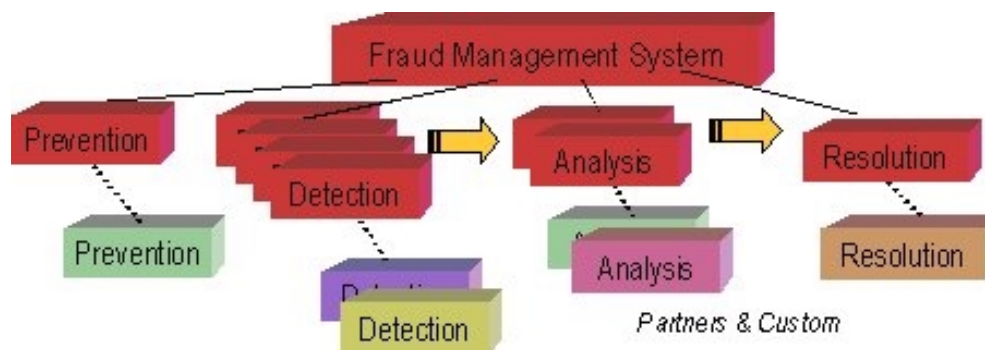
## HP FRAUD MANAGEMENT SYSTEM (HP FMS) OVERVIEW

---

The HP Fraud Management System (HP FMS) is comprehensive fraud management solution, one that provides both *fraud detection capabilities*, and also acts as a *central management platform* for a revenue assurance or fraud management organization. HP FMS is a *framework* that allows easy integration with components that supplement functions included in the base product, including a library of optional modules. This “plug-in” architecture provides several unique dimensions to fraud management, including:

- **Coverage and flexibility.** Comprehensive fraud management has evolved over time and today consists of many functions, including prevention, detection, investigation, resolution, and analysis of results. HP FMS can be at the center of it all. With HP FMS, the next generation architecture provides an operator with the ability to “plug in” modules that supplement the base HP FMS product thereby customizing their fraud solution to their unique needs. In addition to a library of optional modules, additional custom functions may be provided by HP, partners, or the operator’s own I.T. organization. Various technologies are employed where they provide most value, rather than using a single technology across the entire system.
- **Ability to Scale.** Also as a result of the distributed Plug-In Architecture, HP FMS has almost unlimited scalability. By allowing modules to be configured and distributed, the design of HP FMS enhances the improved scaling resulting from HP’s leading high-performance servers.
- **Next Generation Networks.** The industry is moving to 2.5G and 3G networks, which use packet-switched data networks to provide services. (Non-voice services are becoming popular in some parts of the world, and extensive growth is expected worldwide within the next couple of years). As operators deploy these services they obtain increasing revenue. These new types of transactions and events need to be examined for fraud. HP FMS V8.1 enables its leading fraud management capabilities to be applied to data from these new networks, including VoIP, GPRS, UMTS, etc. Operators who already offer data services are concerned about related fraud losses. For others who will soon implement these new networks, fraud protection is available in HP FMS even *before* they experience fraud losses. This allows operators to be proactive about next generation fraud, rather than reacting only after experiencing catastrophic losses.

This plug-in architecture is depicted in the diagram below.



A note that ties these together: Next generation networks will generate explosive growth in the number of events/transactions. Additionally, these new services and network types will see fundamental changes in the fraud perpetrated, and only a “plug-in” architecture will provide the flexibility needed to react quickly to new types of fraud.

## HP FMS 8.1 Features and Functions List

HP FMS is for use by both fixed line and wireless, prepaid and postpaid, for a wide range of fraud types, including:

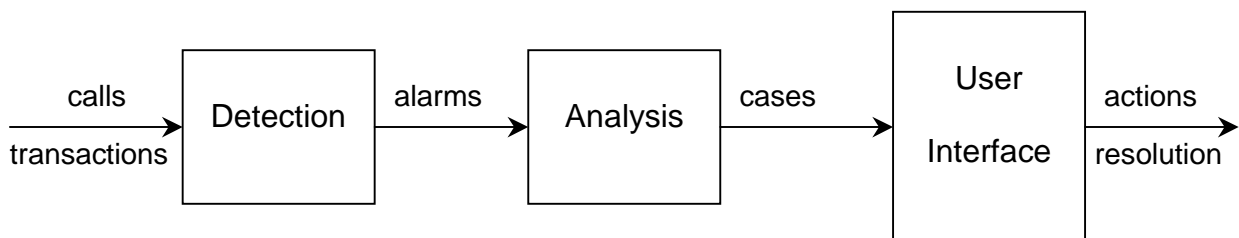
- subscription fraud, including identity theft, content and value-added services theft
- technical fraud, including clip-on, PBX, and wireless cloning
- calling card fraud
- prepaid fraud, including fraudulent recharging of services
- insider fraud, including illicit activation of unbilled services
- dealer fraud, fraudulent activations to gain unearned commissions
- handset or equipment fraud, counterfeit or black-market handsets

and more. HP FMS provides good breadth of coverage, and enhancements are continually made as fraud changes in the industry.

The detection system contained within the HP FMS product consists of three primary functions, along with numerous supporting components. The primary functions are: Detection, Analysis, and the User Interface. A simplified diagram below shows the flow of the basic information through Detection, Analysis, and the User Interface.

- **Detection:** Call or transaction data records are processed by Detection, which looks for calling patterns or behavior that are unusual or suspicious. When the Detection component finds one of these anomalies, it will generate an Alarm.
- **Analysis:** The Analysis component will review each alarm in detail, and correlate with all other alarms for that service number (subscriber, billing number, etc.). Utilizing additional customer information, including a detailed individual profile, HP FMS will make a determination as to the existence (or not) of fraud. If fraud is found, Analysis will create a Case for an analyst to review. The two-phased analysis consists of a rule-based expert system, followed by an optional neural network-based review.
- **User Interface:** HP FMS provides a graphical user interface (GUI) for each type of person who will utilize the fraud system. This includes the Fraud Analyst (or Case Manager), as well as the persons who are responsible for setting up the operator-specific knowledge, parameters, and otherwise ensuring the system is implementing the policies of the operator. Case Management and resolution tools are provided to ensure rapid and efficient response to fraud.

The key features of each of these three primary functions are summarized below, along with some general system characteristics and details.



## DETECTION

The following are some of the many fraud detection mechanisms provided by HP FMS:

- **Unknown customer**  
Determine if a call record has been received for a service number or subscriber who is unknown to the system. Detects ghost phones that are on the network, but not in billing system.
- **Authorization/Suspension check**  
Determine if a call record has been received for a service number or subscriber who is using a class of service for which he/she is suspended. Compared with time-stamp of suspension. A carrier may allow calls to special numbers (customer call center, emergency numbers, etc.) without conducting suspension checking.

## HP FMS 8.1 Features and Functions List

- New subscriber checks

Determine if a new customer violates a set of constraints that can be highly indicative of subscription fraud. Some of these checks include:

- Contact number analysis (calling home or work contact numbers)
- Inactive new subscriber
- Change of subscriber data soon after activation (example: billing address changed within the first month of service)
- Immediate roaming (wireless) after activation with absence of home carrier calls
- Roaming calls not to home country or home carrier

- Prepaid-postpaid service mismatch

Detect any customer where there is a prepaid/postpaid inconsistency between what the customer is supposed to be, and what is observed in the customer's calls.

- Call pattern matching

Detect any call whose characteristics match certain conditions as defined by the carrier. New with the Version 8 release is the ability to add customer/subscriber-based conditions to the pattern so that patterns can be implemented for certain types of customers.

- Black List checking

Detect any call that matches an entry on a black list defined by the carrier. HP FMS provides seven standard types of black lists (From-#, To-#, Service Number (such as a billing number or subscriber identity), Access Point, Originating IP address, Destination IP address, or Equipment Number (such as a wireless ESN or IMEI). Carriers can also have up to 12 additional (custom) types of black lists.

Black list entries may also have an automatic purge time associated with them, after which they are automatically removed from the list.

- Suspicious international country

Detect any call made to a country on a "suspicious countries" list as defined by the carrier, when that country is not known to be within the normal calling profile of the service number or subscriber.

- Suspicious area/city code

Detect any call made to an area code on a "suspicious area codes" list as defined by the carrier, when that area code is not known to be within the normal calling profile of the service number or subscriber.

- Profile deviation

Detect any instance when a newly calculated individual profile for a given service differs from its previous profile by more than a specified amount.

- Service pattern matching

Detect any service number or subscriber whose characteristics match certain conditions as defined by the carrier.

- Smart Thresholds (against expected Usage)

Determine if a customer exceeds expected usage in operator-defined categories. The categories and usage types are defined and tailored by the operator. Up to 32 combinations of the following can be tracked.

Operators can track a number of service types, including:

- Wireless, analog or digital, including GSM
- Fixed Line, private and public, PBX

## HP FMS 8.1 Features and Functions List

- Calling Card
- Data, VoIP, GPRS, UMTS

Sample usage categories an operator might track include:

- Long Distance
- International
- Premium Rate or Audiotext Services
- Total

Calls (of the above types, as defined by the operator) can be tracked in the following directions:

- Outgoing
- Incoming
- Either direction

Usage can be tracked for any category in the following usage types:

- Duration (minutes of use)
- Attempts (number of calls)
- Charges (cost in local currency)

Usage can be tracked for any category in the following service types:

- Home
- Roam

Usage is tracked for various periods of time, including:

- Per call
- Times within a day (4 defined zones denoting time of day, tailored by the operator)
- Daily (peak days, off-peak days, tailored by the operator using a calendar)
- Weekly
- Monthly

- Collision (Call Overlap)

Determine if two calls from (supposedly) the same phone or service were in progress at the same time. This is primarily for calling card and wireless services.

- Velocity (Geographical)

Determine if two calls from (supposedly) the same phone or service were made from two locations, far-enough apart and too close together in time, to be feasible. This is primarily for calling card and wireless services.

- Number level detection

Perform Detection optionally at the phone number level (in addition to the service level) – in GSM, a single IMSI may have multiple phone numbers associated with it.

- Customize detection parameters

Provide the ability for the carrier to easily change various parameters and other required values needed for the detection of anomalous calling behavior:

- Groups of Service Numbers (Group profiles)
- Expected usage levels
- CDR and Service Patterns
- Black Lists
- Suspicious Country/Area Codes
- Maximum Profile difference

HP FMS Version 8.1 also supplies a reporting tool to assist with the tuning of threshold levels, based on results of existing thresholds and the resulting alarms (accuracy of the alarms).

## HP FMS 8.1 Features and Functions List

In addition to the standard detection components, there are some features that are applicable to some, but not all, operators. These additional functions are available as optional configurable modules that supplement the core HP FMS platform during system integration and installation. These features include:

- Prepaid anomalies  
Track a prepaid subscriber's recharges (frequency of recharges, amounts of each recharge, and high-value recharges) and determine consistency with actual usage. Also potentially checks for credit card stuffing (often a symptom of recharging with stolen credit cards).
- High destinations count  
Detect when a subscriber exceeds a carrier-specified number of either call-forward destination numbers, or different countries called.
- Equipment collisions  
Detect any equipment (IMEI – International Mobile Equipment Identity) that is in use at the same time, which could indicate cloned equipment.
- SIM stuffing  
Track subscribers that use multiple Subscriber Identification Modules (SIMs or smart cards) on the same equipment (IMEI), and alarm when the number of different SIMs exceeds an operator-defined number.

## ANALYSIS

- Knowledge-based analysis system  
Utilization of a true rule-based expert system with inferencing capabilities to perform a detailed analysis for fraud.
- Neural Network analysis system  
Use a neural network and the Case Archive to perform a second analysis, scoring the current case of suspected fraud against historical case data, representing both true fraud and false cases. The neural network score will provide another means of determining the confidence and credence of the case, and also prioritizing the new case on the Case List.
- Correlate all alarms for a service  
Analysis is performed using all alarm information known for the service number at the time (versus performing analysis only on each individual alarm).
- Analyze external alarms  
Ability to include in the analysis, additional alarm information provided to the fraud management system by an external entity. These alarms might originate from an SS7 network surveillance probe, authentication/Home Location Register system, credit system, etc.
- Severity of each alarm  
The ability to determine evidence of fraud based on the *severity* of any of the alarms (e.g., expected usage exceeded by a specified amount).
- Number of alarms of a specific type  
Ability to determine evidence of fraud based on the *number of occurrences* of a particular type of alarm, without necessarily caring about the severity of any of the alarms themselves.

## HP FMS 8.1 Features and Functions List

- Individual service profiling and usage signature

Each individual service or subscriber known by the system will have determined a detailed, individual, profile, which describes the historical calling behavior. Profiling will reflect many aspects of the service number, based on the types of usage tracked by the carrier:

- When calls are made (time of day)
- How many calls are made
- What countries and area codes are called
- How long the calls last
- How much money is spent
- How much usage is accumulated daily, and weekly.

Profiling is based on how the carrier configures usage tracking and threshold checking, and is designed to provide an operator with an accurate description of how each customer has actually used their service. This aids in the accuracy of detection in the resulting Cases of suspected fraud.

- Compare observed usage to profiled usage

Ability to use a longer-term detailed profile of each service or subscriber to determine if observed calling behavior is outside what is expected for that individual. This is to ensure maximum accuracy in the findings.

- Combine evidence of multiple types of Fraud

Ability to take multiple pieces of evidence for different types of fraud and combine to determine the overall confidence of fraud for a given service.

- Determine types of fraud indicated and confidence

Presentation to an analyst the final determination of the system of whether fraud is present, the type of fraud detected, and the confidence level.

- Adjust confidence based on service information

Based on additional information about the service number (e.g., they are a new customer, etc.) the confidence level of fraud can be increased or decreased.

- Call Archive facility

HP FMS supplies a Call Archive facility that is used to store all CDRs for use while investigating a case or later performing an off-line analysis. Users may query the Archive for calls based on numerous attributes, including: service number, dates/times, charges, country and area codes, etc. The size of the Call Archive is operator-specified.

- Call Tracer and Link Analysis

To aid fraud case investigation, HP FMS 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.

- Case Archive facility

HP FMS provides an archive of resolved cases, both true fraud as well as cases determined not to be fraud. Cases in the archive are available to be displayed in the User Interface, and are also the primary input data for the neural network case analysis. The Case Archive may also be utilized by the carrier as a data source for additional, more advanced, analysis.

## HP FMS 8.1 Features and Functions List

- Provide explanation of reasoning  
HP FMS provides a description of the reasoning steps and an overall explanation of how the system arrived at the conclusions it did regarding fraud and confidence. All evidence is presented.
- Recommend counteractions  
Recommendations for counteractions to be taken for the type of fraud detected are presented to the analyst, based on the policies and business practices of the carrier (customized by the carrier).
- Distribute cases via Worklists  
The cases of detected fraud can be distributed to different analysts or groups for review, based on various factors (types of fraud, region, security, specific customers, etc.).
- Automated action taking  
HP FMS allows for certain types of counteractions (such as suspension or rerouting calls to a customer care hot line) to be automatically executed by the system, based on the policies and business practices of the carrier.
- Customize analysis parameters  
The ability for the carrier to easily change the parameters and knowledge associated with the detailed fraud analysis:
  - Alarm Severity levels
  - # of occurrences of Alarms
  - Types of Fraud indicated
  - Ranking of Fraud Types
  - Actions to counter fraud
  - Automated Action activation
- Customize analysis rules  
The ability for the carrier to easily change the rules used in Analysis via a rule editor.

In addition to the standard analysis tools, there are some optional configurable modules that supplement the core HP FMS platform during system integration and installation. These tools include:

- Subscriber fingerprint  
Identify a subscriber based on his or her usage (versus the demographic information). According to the numbers called (destinations) and other factors defined by the operator, the module generates a signature that should be unique for each subscriber/service. A fingerprint consists of 10 values of 8 observation variables. A fingerprint archive is created, and can be used to match fingerprints of known fraudsters with other subscribers.
- Investigation data collection  
Collects data from a set of named sources, correlates the information into a file with date/time stamps, and sends the data to HP FMS for use in Case review via the Investigation Data interface.
- Billing history investigator  
Collects bill items (billing records, status, unbilled calls) over a time period, computes indicators (such as averages, trend, spread, etc.), and generates alarms based on the indicators and custom analysis. Results stored via the Investigation Data interface.
- Profile-based tuning tool  
Collects and analyzes data in the HP FMS profiles, and creates histograms to analyze the distribution of an operator's customers' profiles, based on subscriber groupings, types of usage being tracked, times of day, and other discriminating factors.

## HP FMS 8.1 Features and Functions List

- Account analysis

Monitors the collective usage of an account (multiple subscriptions/services). Generates alarms/cases when specific usage thresholds are violated at the account level or when the collective number of alarms exceed a specified count. The analysis is done on an account-by-account basis.

## USER INTERFACE

- Windows access

Ability to access the user interface with a desktop device (client) for Windows 2000 and XP. HP FMS V8.1 provides a new Explorer-type graphical user interface (GUI) that provides easy navigation, pane-based editing and hierarchical views of the various types of information required by the various types of users of the system.

- 9 Levels of secured system access

HP FMS provides a distinct, secured, user interface for each of the four primary types of users:

- Case Manager (Fraud Analyst)
- Knowledge Manager
- System Manager
- Security Manager

Additional privileges that can be assigned to users include:

- editing black lists
- editing the white list
- performing link analysis
- customizing the HP FMS toolbar
- performing a Call Archive query

There is general system security by requiring (or permitting the use of) passwords for each individual user of the fraud system. The carrier can specify the complexity of the passwords, and can also assign expiration timeframes for passwords.

- Printing of windows

HP FMS provides printing capability from the various windows of the user interface, making it easy for case details, system settings, message logs, etc., to be printed.

- Black list maintenance

Entries can be added to the HP FMS black lists from the Case Details window, as well as from the Link Analysis windows (as well as the Knowledge Management interface). These are two of the most common places where an authorized analyst determines the need for new entries to be added to the black lists.

- On-line help

There is on-line help available at each window, question, etc., if needed.

- Reports

The user can create summary or detail reports regarding the different aspects of the operation of the fraud system, or on specific entities within the fraud system (e.g., cases of suspected fraud).

- Customizable field labels

Data field labels may be customized to display using the terms in use at the carrier.

## HP FMS 8.1 Features and Functions List

- User interface individualized

Various aspects of an individual's "account" on the fraud system may be tailored to his/her liking, including color-coding of cases for the fraud analyst, selection of customer data fields on the Case List, window sizes, and various other attributes of the user's environment.

## CUSTOMIZATION

HP Fraud Management System may be customized in a variety of ways, including setting of installation-time settings, utilizing the HP FMS Application Program Interface (API), or by the implementation of custom functionality.

- **Optional Configurable Modules.** A library of *configurable modules* can be integrated using HP FMS standard interfaces. Some of these optional modules have been described above under DETECTION and ANALYSIS sections, depending on the type of module. Additional custom processes, action interfaces, etc., would be developed as a system integration activity, usually as part of the overall preparation prior to installation, or done at a later time. The additional pricing of the customizations is dependent on the details of the specific requirements. A Fraud Assessment consulting activity is where these desired customizations are usually identified and scoped.
- **Installation-time Settings.** HP FMS has a set of parameters which may be used to specify field names, lengths, ordering of columns on some of the displayed tables, enabling or disabling of detection techniques, usage types, or displayed fields. These are specified at installation time, and are a normal installation activity, not incurring additional cost. Training is provided (Technical Training) which discusses what can be customized in this manner and how to do it.

Predetermined types of customizations (such as the use of installation-defined fields in the Call, Account, and Subscriber/Service data records, some custom reports, etc.) have built-in mechanisms to facilitate these changes.

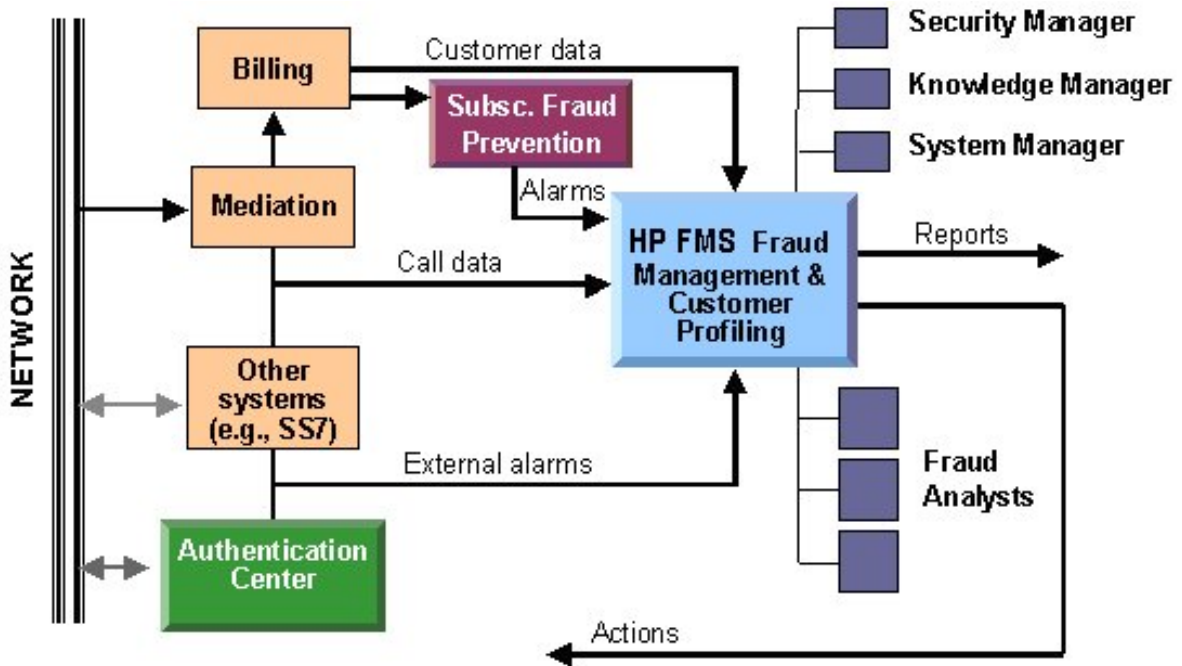
- **Custom Functionality.** In some instances, an operator may desire functionality in the Fraud System which is not present in the product or the library of plug-in options, and does not wish to wait for the features to appear in a future version of the product. In these cases, HP may entertain the request to develop custom functionality to be included in the solution as a custom plug-in. These are handled on a case-by-case basis. In most cases, the requirements of the operator will be satisfied by the base product, or with customizations developed by a Systems Integration effort utilizing the optional Plug-in Modules or the HP FMS API.

## HP FMS TECHNICAL DETAILS

---

- Ease of integration

Overall ease of integration of the HP FMS system with other existing systems (such as billing system, mediation device, SS7 probes, Home Location Register/Authentication Center, etc.), by the use of the HP FMS Application Program Interface (API). In addition, a point-of-sale subscription fraud prevention module greatly enhances the value of a total fraud management solution.



**HP FMS Integration with other systems**

- Performance

HP FMS can accommodate a large stream of call data records, and can provide its analysis in a timely manner, meeting the needs of the operator.

- Ability to scale

The system can support (by architecture and design) a significant growth in an operator's customer base as well as the rate of call records being analyzed. HP FMS provides added scaling by supporting clustering of server machines via clusters.

- Data reduction

The system provides a step-wise process which automatically screens large amounts of data, quickly focuses only on that which is suspicious activity, and ultimately provides to the analyst only the information relevant to fraud, and only in the cases where fraud is highly suspected (to limit false positives).

- Real-time detection

HP FMS provides the ability to detect anomalous calling behavior immediately upon receiving each call from a call collection system or signaling network (e.g., SS7) one at a time (versus in receiving a group of calls in batch).

- Batch mode detection

HP FMS provides the ability to perform detection on call records received in a batch process, evaluating them sequentially, at intervals defined by the carrier.

- Client/Server solution

The architecture of the solution provides a desktop client networked with a server performing the heavy processing.

## HP FMS 8.1 Features and Functions List

- Open server platform

The HP FMS solution can be used on either of two leading Unix server platforms: the HP PA-RISC platform running HP UX, or the HP AlphaServer platform running Tru64 Unix. Both of these server types support superior integration with external systems as well as excellent ability to scale.

- Partitioning/service bureau

The solution allows the customer base to be divided into different partitions which are managed separately (e.g., by product, region, or market) or to include multiple carriers, in such a way that there is proper segregation of confidential data, etc.

- Account information

Multiple Service Numbers (or subscriptions) may be associated with an Account Number. This is particularly useful for corporate accounts that are often comprised of numerous subscriptions, billing numbers, and services.

- Auditing

The system keeps track of user activity, particularly noting the disposition of cases of suspected fraud, changes made by a user to the knowledge base, or other important system parameters.

- Error logging

System-related errors that are detected and may have adverse effects on overall system performance or usefulness are provided via a specified device/mechanism to the carrier.

- Self monitoring

The system keeps track of database "flooding" which is caused by two things:

- too many alarms created in too short a time due to incorrectly set parameters
- too many error conditions in too short a time,

and is equipped with an automatic shut-off mechanism to prevent database corruption.

- Database Management

The solution provides tools, utilities, or reports, which assists the carrier in managing the contents (size, layout, amount, accuracy, relevancy) of the database.

- Localization

The client interface, related help text and documentation can be easily translated into the local language, including those using multi-byte character sets.

- Reports

HP FMS provides a standard set of Reports that are available to the different users of the Fraud system. These reports include:

- Detailed Case Report – for an active Case of suspected fraud for a specific service/subscriber
- Archived Cases Report – for customers with confirmed and resolved cases of fraud
- Case Value Report – summary of the value of fraudulent cases
- Case Resolution Averages – summary of resolution times for cases, by fraud type
- Case Resolution Details – resolution status for each case within a specified time frame
- Analyst Activity – details on activities performed by each fraud analyst
- Cases by Fraud Type – number of cases for each type of suspected fraud
- Alarm/Case Statistics – summary of new alarms and cases for each day

## HP FMS 8.1 Features and Functions List

- Alarms by Alarm Type – number of alarms of each type generated in time span
- Calls Matching Patterns – number of call records which match at least one Call Pattern
- Patterns Matching Calls – percentage of calls which match *each* pattern
- Service Pattern Matching – number of service numbers that match at least one pattern
- Services Matching Patterns – percentage of service numbers matching each pattern
- Group Analysis – highlights recommended changes to thresholds based on past accuracy
- Fraudulent Calls – lists all “marked” call records with a specified time span
- Service Load Report – lists status of processing the Service Loader

These reports are delivered in Web-ready HTML files. In addition, other reports can be added to HP FMS, either custom-developed or using optional plug-in reports, such as the standardized GSM High Usage Report.

- Product documentation

Comprehensive online product documentation is available to support the proper understanding, use, and support of the operational system, including the integration activities needed for installation and system setup.

- Installed base

HP FMS has a substantial installed base of communications service providers that use the system as part of their day-to-day business, who can attest to the product’s usefulness and reliability. The product provides a track record of success on an international basis.

- Complete solution

Ability of the carrier to secure the entire solution (including delivery/support thereof) from a single source, including the fraud system product, hardware, base software, integration with existing systems, etc.

- Local or regional support

Local or regional support for the solution is available, which can answer many of the questions of the carrier, as well as resolve most of the problems that may arise during the use of the system.

- Engineering support

Support for the base fraud system product is available from the Engineering group, and defects to the base product software can be remedied and made available to the carrier (in the form of patches, maintenance updates, etc.).

- Consulting services

Comprehensive consulting services availability to assist the carrier in determining the applicability of the fraud system, planning for installation, providing recommendations for the system’s use (including augmenting existing procedures, policies, etc.) from the business, technical, and organizational perspectives.

- Training

Extensive training services are available to support the proper understanding, use, and support of the operational system, including the technical activities needed for installation and system setup. Training is usually presented at the operator’s site in conjunction with installation.

- User Forum

Carriers using HP FMS meet annually for a User Forum, where they share their fraud experiences and ideas, hear of HP FMS product direction, and provide input to HP FMS Product Engineering.