



h p f m s

HP Fraud Management System

Features and Functions List

Version 9.3

HP FRAUD MANAGEMENT SYSTEM (HP FMS) OVERVIEW

The HP Fraud Management System (HP FMS) provides the most sophisticated detection and prevention techniques possible, thereby providing operators the ultimate fraud management solution that can span all network types from Wireline to Wireless, GPRS, IP, and UMTS. HP FMS Version 9 achieves this goal by moving from CDR to Event-centric detection and analysis. This transition preserves all capabilities of previous versions, while expanding the capabilities with all the potential offered by events and services, including those available in a 3G environment. With HP FMS Version 9, the product has taken the next logical leap forward by meeting the changing needs of 2.5 and 3G service providers ... and defeating the next generation fraudster.

HP FMS is a comprehensive fraud management solution, one that provides both *fraud detection capabilities*, and also acts as a *central management platform* for a fraud management organization. HP FMS not only offers revenue protection through its sophisticated fraud detection and prevention techniques, but has been expanded even further to provide comprehensive revenue assurance capabilities. This offers carriers a complete suite of integrated applications for Fraud *and* Revenue Assurance.

KEY BENEFITS

There are a number of unique and critical business benefits of HP FMS, including

- Complete and comprehensive fraud management for all service offerings, including next generation/3G and convergent networks, as well as traditional wireless and wireline services allows increasingly sophisticated fraud detection.
- Increased sophistication and agility detects and responds to rapidly changing and more complex fraud scenarios, to defeat the modern-day fraudster.
- Operators pay back investments in the fraud solution in just a few months, or even in a matter of weeks
- Multi-level representation of an operator's customer base enables multi-level usage accumulation and tracking, and allows operators to focus their resources on the appropriate billing entities representing their customer base.
- More sophisticated scoring increases operational efficiency by reducing the number of cases to be examined.
- Lower cost of ownership allows operators to only buy the functionality they need
- Proven and reliable solution utilizes latest technologies, including rules and data mining (using neural networks, decision trees, and mixed analysis models) for unparalleled results.

Enhanced performance of HP FMS makes smaller hardware investments go even further.

HP also has the largest user group of any fraud management solution with more than 70 operators protecting over 300 million subscribers around the world with HP FMS.



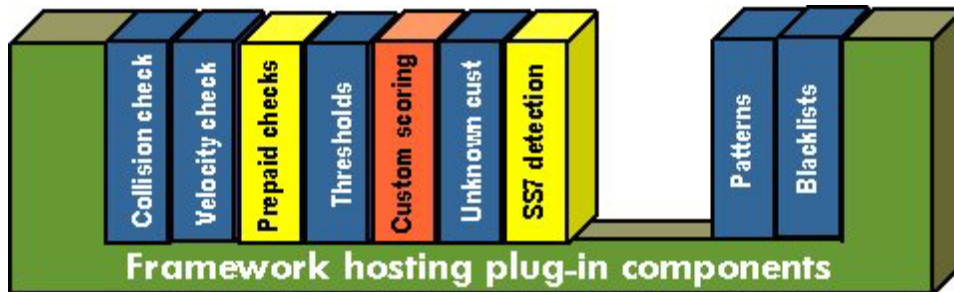
Worldwide protection with HP FMS



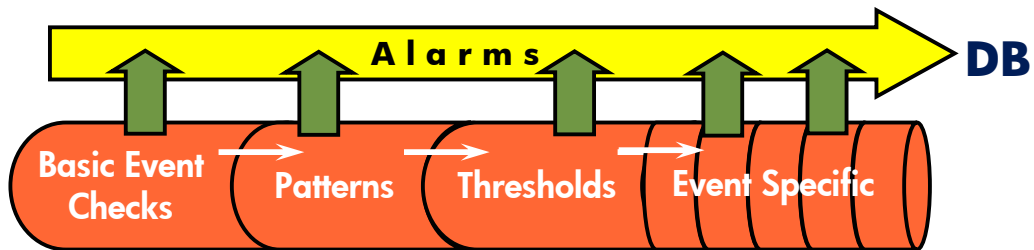
HIGH THROUGHPUT EVENT ARCHITECTURE

Our new "High Throughput Event Architecture" provides several unique dimensions to fraud management, including:

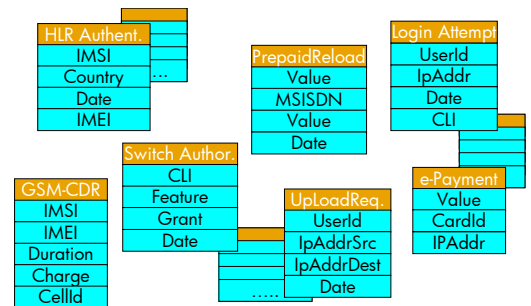
- **Coverage and flexibility.** Comprehensive fraud management has evolved over time and today consists of many functions, including prevention, detection, investigation, resolution, and analysis of results. HP FMS can be at the center of it all. With HP FMS, the next generation architecture provides an operator with the ability to "plug in" modules that customize their fraud solution to their unique needs. In addition to a library of standard and 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 high throughput event architecture, HP FMS has almost unlimited scalability. Modules are replicated and grouped into pipelines: modules within a pipeline can share event and entity data, reducing the need for database access. This design of HP FMS enhances the unsurpassed scaling resulting from HP's leading high-performance servers.



- **Full event model supports next generation networks.** This allows HP FMS to perform comprehensive analysis for all service offerings and all types of transactions, including (but not limited to):
 - Traditional voice call records (CDRs), wireless and fixed line, postpaid and prepaid, prepaid reload
 - MMS, SMS, HLR-authentication, service authorization, upload/download requests
 - ePayment/payment transactions. eCommerce and mCommerce platforms, broadcast servers (music, games, video-on-demand).
 - Login attempt (RADIUS, RAS, DNS and DHCP authentication)
 - In-progress transaction data from SS7, IP sniffers, IP mediation (such as HP IUM), etc.



Operators that already offer data services are already concerned about related fraud losses. For others that 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.

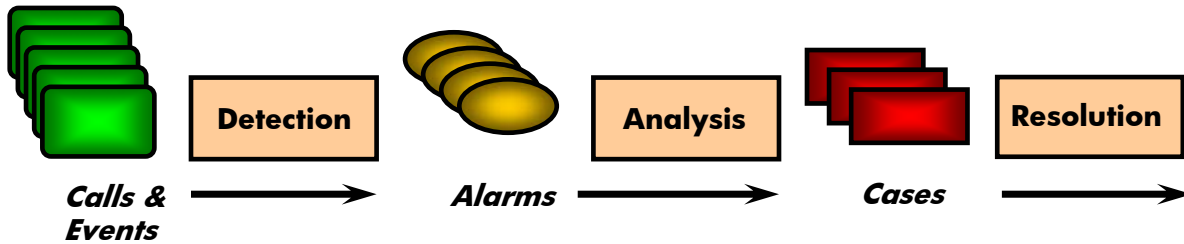


USING HP FMS

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, call sell, content and value-added services theft, SIM-boxing (SIM gateway), and premium rate service inflation
- network fraud, including clip-on, PBX, wireless cloning, IP security events, and 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. And enhancements are continually made as fraud changes in the industry.



The fraud 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 Resolution. This simplified diagram shows the basic flow of information through Detection, Analysis, and Resolution via the User Interface.

- **Detection:** Event and call data records are processed by Detection, which looks for usage 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 billing entity (e.g., subscriber, billing number, company, operator, 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 multi-phased Analysis component consists of numerous scoring models, including a rule-based expert system, and data mining using SPSS’s leading Clementine product for neural network, decision tree, and mixed analysis models.
- **Resolution and the 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 Entity (e.g., customer, company, etc.)**
Determine if an event/call has been received for a customer or billing entity that is unknown to the system. Detects ghost phones and equipment on the network, but not in the billing system.



- **Authorization/Suspension check**

Determine if an event has been received for a billing entity or subscriber who is using a class of service that is either unauthorized or under suspension. Compared with time-stamp of suspension. A carrier may allow calls to special numbers (customer call center, emergency numbers, etc.) without conducting suspension checking.
- **Prepaid-postpaid mismatch**

Determine if an event is labeled as prepaid while the customer is postpaid, or vice-versa. A mismatch could indicate potential insider or dealer fraud (via data manipulation), or could also indicate incorrect provisioning or other inconsistencies between the network and the order entry or billing processes.
- **New customer/billing entity 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 customer (a customer that does not start making calls soon after activation)
 - Change of customer 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
- **Black List checking – Events and Entities**

Detect any event or entity that matches an entry on a black list defined by the carrier. HP FMS allows unlimited types and numbers of blacklists. Operators can define new fields and declare them as being eligible for blacklisting. Typical fields might include A-#, B-#, address, dealer code, Access Point, originating IP address, destination IP address, and equipment number (such as IMEI).

Wildcards may be used when defining black lists and entries may also have an automatic purge time associated with them, after which they are automatically removed from the list.
- **Classic event pattern matching**

Detect any call or event whose characteristics match certain conditions as defined by the carrier, including black list matches. An operator also has the ability to add customer/subscriber-based conditions to the pattern so that patterns can be implemented to look for particular situations with certain types of customers.
- **Accumulation patterns**

Detect when an operator-defined number of conditions (patterns) have occurred for a given billing entity over a rolling period of time (up to two weeks). Examples might include the following:

 - More than 8 premium rate calls of over 60 minutes duration each in a five-day period
 - More than 3 prepaid reloads of more than a certain amount, plus at least one blacklist violation, in a ten-hour period
 - More than 10 accesses of blacklisted sites in a 24-hour period
- **Sequence patterns**

Detect when an operator-defined series or sequence of pattern matches has occurred within a specified period of time. This allows an operator to recognize more complex and sophisticated fraud schemes. Sequence patterns detect the increasingly common situation where a series of otherwise normal or inconspicuous events *is* suspicious when viewed together as a whole.
- **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 customer.



- 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 customer.
- Profile deviation
Detect any instance when a newly calculated individual profile for a given billing entity differs from its previous profile by more than a specified amount.
- Billing entity pattern matching
Detect any entity/subscriber whose characteristics match certain conditions as defined by the carrier.
- Smart Thresholds (against expected Usage)
Determine if a billing entity or subscriber exceeds expected usage in operator-defined categories. The categories and usage types are defined and tailored by the operator, allowing the operator to focus on the types of usage where fraud exposure is most important. Up to 32 combinations of the following can be tracked.

Operators can track any number of service types, including:

- Wireless, analog or digital, including GSM
- Fixed Line, private and public, PBX
- Calling Card
- Data, VoIP, GPRS, UMTS

Sample usage categories an operator might track include:

- International
- Premium Rate or Audiotext Services
- SMS, Premium SMS, MMS
- Content consumption
- Prepaid reload
- 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)
- 4 types of volumes (of data transferred)

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

- Home use
- Roaming

Usage is tracked for various periods of time, including:

- Per call or event
- 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

HP FMS provides the tools to assist the operator in the tuning of thresholds.



- Collision (Call/Event Overlap)
Determine if two events from (supposedly) the same service were in progress at the same time. This is primarily for wireless and calling card services. HP FMS allows an operator to specify through a GUI, what types of events will normally collide with other types of events (e.g., 3-way calls), eliminating false alarms from legitimate combinations.
- Velocity (Distance violations)
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 wireless and calling card services. HP FMS allows an operator to specify through a GUI, what types of events will collide with other types of events, eliminating false alarms from legitimate combinations.
- 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 billing entities (Group profiles)
 - Expected usage levels
 - Patterns – classic event and billing entity, accumulation, and sequence patterns
 - Black Lists
 - Suspicious Country/Area Codes
 - Maximum Profile difference

HP FMS Version 9.3 also supplies a reporting tool to assist with the tuning of threshold levels, based on the existing thresholds and the resulting alarms (analyzes the accuracy of the alarms).

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 customer's recharges (frequency of recharges, amounts of each recharge, and high-value recharges) and determine consistency (balance) with actual usage. Also potentially checks for credit card stuffing (often a symptom of recharging with stolen credit cards).
- High destinations/call forward count
Detect when a customer exceeds a carrier-specified number of either call-forward destination numbers, or different countries called.
- IMEI/IMSI stuffing
Track customers 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. The symmetrical analysis is done on IMSI, monitoring the number of different IMEI used (cloning). The module can create alarms also on the number of 'switches' (e.g. only two different IMEI, but switched 10 times in a day).
- Cross-dimension ratio
Create an alarm when the ratio between two dimensions (usage tracking values) exceeds a specified level. This can be used to detect when there is an unusually high ratio of a particular type of calls (e.g. PRS or international) against the total or other call types. This is also valuable for SIM-box detection by identifying customers with all outgoing calls versus no incoming calls (or nearly so).



ANALYSIS

HP FMS Version 9.3 applies **comprehensive fraud intelligence** to the Analysis task by using a wealth of complementary techniques and technologies. HP FMS Analysis is made up of two primary components:

- the knowledge-based *expert system* with inferencing capabilities to perform a detailed analysis for fraud using the expertise of the operator. The expert system is built using a leading industry-standard rule engine.
- the *Scoring module* that evaluates the current situation against known past outcomes to provide additional perspectives in making a determination of fraud, as well as a means of determining the confidence and credence of the case, and prioritizing the Case. The scoring module utilizes the SPSS Clementine product, and makes use of data contained in the HP FMS Archives *to create and use multiple data mining models*. The scoring module uses multiple techniques (rather than a single technology), including:
 - neural network analysis
 - decision tree analysis
 - hybrid analysis models combining multiple approaches

While the HP FMS Archives are used to train the scoring module, they can also be used for any other data mining analysis as well (e.g., analysis of the outliers or rule induction).

Additional details of the analysis component are listed here.

- Correlate all alarms for a billing entity
Analysis is performed using all alarm information known for the billing entity or customer 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 system. These alarms might originate from an SS7 network surveillance probe or IP sniffers, 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.
- Individual customer profiling and usage signature
Each billing entity (customer) known by the system will have determined a detailed, individual, profile, which describes the historical calling behavior and use of their various services. Profiling will reflect many aspects of the customer, based on the types of usage tracked by the carrier:
 - When different types of events occur and when calls are made (time of day)
 - How many events/calls are made
 - What countries and area codes are called
 - How long the calls last, and 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 billing entity has actually used their various services. 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 customer to determine if observed 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 customer.
- Determine types of fraud indicated and confidence
Presentation to an analyst the final determination of the system of whether fraud is present, the types of fraud detected, and the confidence level.
- Adjust confidence based on customer information
Based on additional information about the billing entity (e.g., they are a new customer, etc.) the confidence level of fraud can be increased or decreased.
- Event Archive facility
HP FMS supplies an Event/Call Archive facility that is used to store all events for use while investigating a case or later performing an off-line analysis. Users may query the Archive for events based on numerous attributes, including: billing entity (e.g. customer or billing number), dates/times, charges, country and area codes, etc. The size of the Event Archive is operator-specified.
- Event Tracer and Link Analysis
To aid fraud case investigation, HP FMS provides functionality to perform link analysis using events and calls from the Event Archive, allowing users to chain their way in either direction from a desired target number or IP address,
 - Displaying in graphical form all numbers/addresses called by the target
 - Reversing direction, and displaying in graphical form all numbers that called the target
 - Iterate through multiple levels of linkage.HP FMS provides an Exclusion List to allow operators to exclude commonly called numbers from the analysis and graphical display (such as customer care, voicemail, etc.), if desired.
- 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.
- 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
- Case worklist assignments

- 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, the module generates a signature that is unique for each subscriber/service. A fingerprint consists of 10 values of 10 observation variables. A fingerprint archive is created, and can be used to match fingerprints of known fraudsters with other subscribers.

- Dynamic credit limit

Analyzes the usage of all customers and checks for direct and extrapolated violations of the credit limit set for each subscriber. Based on usage data for the day, along with the current and previous months, the trend usage is computed and is compared with a credit limit threshold for both monthly and bi-monthly usage.

- 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 customer groupings, types of usage being tracked, times of day, and other discriminating factors.



USER INTERFACE

- Windows access

Ability to access the user interface with a desktop device (client) for Windows 2000 and XP. HP FMS V9.3 provides an 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.

- 10 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:

- adding entries to the black lists
- adding entries to the white list
- performing link analysis
- performing a Event Archive query
- customizing the HP FMS toolbar
- performing system integration activities, such as dynamically defining new event types and field definitions, changing event/detection module assignments, etc.

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 and 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 full 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.

- 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 the HP FMS plug-in interface to the high throughput event architecture as described above. 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. The pre-implementation Workshop is where these desired customizations are usually identified and scoped.

In addition to the detection and analysis modules mentioned above, two commonly-utilized optional modules to aid investigation of cases include:

- Investigation data collector
Collects data from a set of named sources, consolidates 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.

- **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 (Administration Training) which discusses what can be customized in this manner and how to do it.

Predetermined types of customizations (such as defining fields in the Event and Billing Entity data records, some custom reports, etc.) have built-in mechanisms to facilitate these changes.

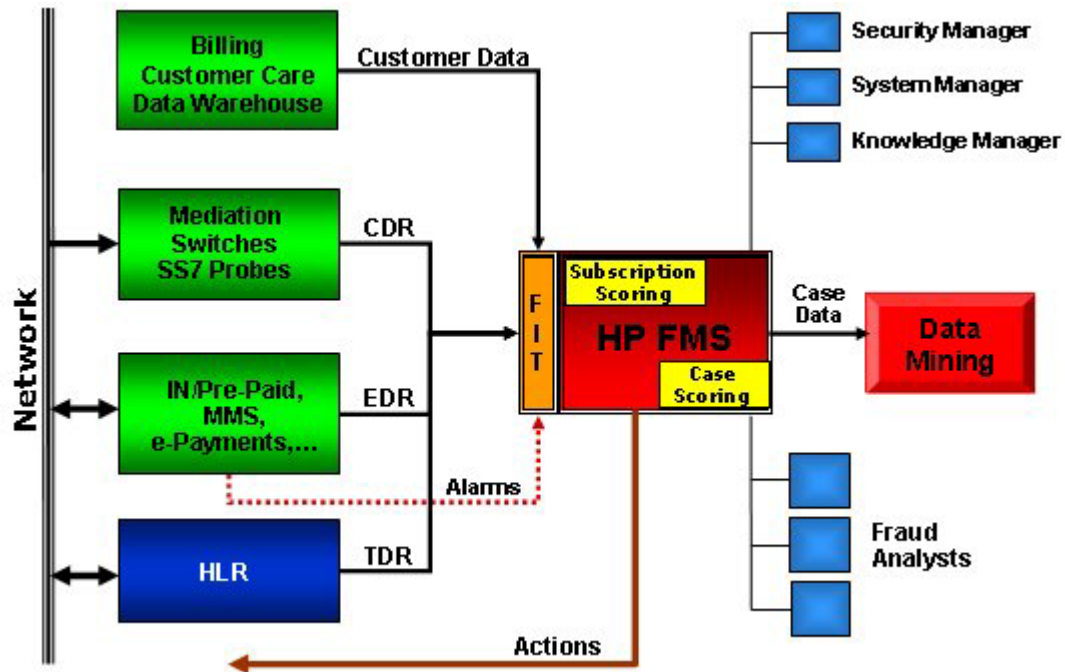
- **Custom Functionality.** In some instances, an operator may desire functionality in the Fraud System which is not present in the product or the library of configurable optional modules, and does not wish to wait for the features to appear in a future version of the product. In these cases, HP may entertain the request to develop custom functionality to be included in the solution as a custom module. These are handled on a case-by-case basis.



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 HP FMS FIT (FMS Integration Toolkit). 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

- Seamless integration with HP Revenue Analyzer

If the operator is also utilizing the HP Revenue Analyzer solution, revenue assurance alarms and cases can be viewed in the HP FMS case management interface. A properly authorized user (with additional Revenue Analyzer privilege) will have access to the Revenue Analyzer Dashboard to conduct drill-down analysis for revenue assurance investigations.

Please see separate Solution Brief for details of the HP Revenue Analyzer solution.

- Performance

HP FMS can accommodate a large stream of events, 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 events being analyzed.



- 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).

- Client/Server solution

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

- Open server platforms

The HP FMS V9.3 solution can be used on three leading Unix server platforms: the HP PA-RISC platform running HP UX, the HP Itanium platform running HP UX, or the HP AlphaServer platform running Tru64 Unix. All 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.

According to the security profile, an analyst can be allowed to see the data in multiple partitions. When the analysts log into the system, they will have visibility to all the data (cases, subscribers, etc.) available in those partitions to which they have been given access privileges. The soft partitioning strategy provides that:

- Databases are logically divided into partitions
- Users are 'logged-in' on multiple partitions according to their user authorizations profile
- Worklists work across partitions
- View provided for both detection and archive components of HP FMS (e.g. link analysis).

- Multi-level billing hierarchy

The multi-level billing hierarchy allows data representation that follows the business model of the operator, and more closely represents the structure of billing systems. This approach also allows tracking on entities that are *meaningful* from the point of view of revenue assurance:

- Any *billing entity* can enter the system:
 - Subscribers, service providers, internal operators, public phones, etc.
- Each level will have a separate threshold configuration and different patterns.
- The operator can define how usage is to be rolled up, and usage will be tracked accordingly at the different levels in the hierarchy.
- Cases can be opened against any *billing entity*.
- Events can be indexed on multiple fields, so that a case can potentially be opened against any field (e.g. IMEI).
- Easier to target analyst resources at the level at which customers/entities are billed instead of the level at which raw data is fed into the system..

- 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, and 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
- Neural Nets – provides important information regarding Neural Network generation
- Alarm/Case Statistics – summary of new alarms and cases for each day
- Alarms by Alarm Type – number of alarms of each type generated in time span
- Pattern Summary – number of events and entities which match at least one Pattern
- Pattern Details – percentage of events or entities that match *each* pattern
- Group Analysis – highlights recommended changes to thresholds based on past accuracy
- Fraudulent Events – lists all “marked” events/calls within a specified time span

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 reports, such as the standardized GSM High Usage Report. HP FMS also supports standard reporting tools as Business Objects to run on its Oracle database, allowing the operator to define new sets of reports.

- Product documentation

Comprehensive online product documentation is available to support the proper understanding, use, and support of the operational system, including the 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.



h p f m s

HP FMS V9.3 Features and Functions List

- 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 and regional support
Local and 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.

Contact your HP Account Manager, or send email to FraudSolutions@hp.com

See also www.hp.com/go/fraud

For additional information on HP products and services, visit us at www.hp.com

December 2005. Windows is a U.S. registered trademark of Microsoft Corporation. All other product names mentioned herein may be trademarks of their respective companies. HP shall not be liable for technical or editorial errors or omissions contained herein. The information is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

