LAVASTORM analytics

Transforming Fraud Management with Agile Data Analytics

Fraud Management Organizations Are Transforming

Fraud management organizations within communication service providers (CSPs) are undergoing a transformation to become more agile. It's being driven by business demands for greater agility to combat determined fraudsters and a sea change in the broader analytics field that has made agile technologies and methodologies available that can enhance our traditional analytic and business intelligence (BI) approaches.

Determined Fraudsters Are Driving Demand for Agility

The need for greater agility starts with the fraudsters themselves. Fraudsters are professionals, running a business to make a profit. They typically have the following characteristics:

- **Extremely determined** – Fraud perpetrators treat their fraud operation as a business. With a high stake in the success of the business, they have a large incentive to maximize their profits and overcome business challenges because their success directly impacts their financial wellbeing.
- **Highly adaptable** – Fraud perpetrators make their financial gains by exploiting imperfections in the business processes of large CSPs, which are typically slow to change. By comparison, the perpetrators themselves have often shown the ability to quickly and continuously evolve their persona and approach to avoid detection and to adjust when the communication company takes steps to reinforce weak areas in their fraud protection schemes.
- **Increasingly invisible** – New services that are IP-based, have given fraudsters new ways to mask their identity and to operate more freely to exploit the weaknesses of the CSP's processes.

With these characteristics, fraudsters are difficult to discourage. In fact, fighting fraud has been likened to squeezing a balloon filled with air. When you squeeze one part of the balloon, rather than escaping, the air simply moves to a different part of the balloon. Similarly, when you close one area of vulnerability, the fraudsters shift to another part of your organization to expose another weakness. Agility is their advantage. So, in the end, fraud management organizations need to recognize that dynamic and be able to identify those additional areas of vulnerability and shift their attention to those areas quickly if they are to have success at minimizing their exposure to fraud risks. Fraud management organizations, therefore, are increasingly demanding more agility in their systems and processes so that they can address these dynamic fraud risks.

Requirements for Fraud Management Systems Are Changing

A traditional fraud management system (FMS), as shown in Figure 1, consists of a data processing module that takes in call detail records (CDRs), a rules engine that evaluates the CDR and other data against a set of rules and thresholds that represent known fraud patterns, an alarm generator that sends out an alarm if one of the rule thresholds is violated, and an alarm and case management user interface that helps fraud analysts receive and process alarms and cases.

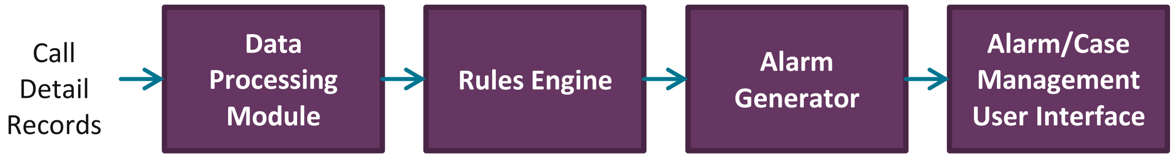

Figure 1 – Components of a typical Fraud Management System

A recent review of request for proposals (RFPs) from major CSPs shows that each component can be lacking when it comes to the requirement for greater agility. Table 1 shows some of the detailed requirements that were identified in those RFPs that reflect agility gaps in current and past systems and the system components that they affect. Additional gaps were identified in areas that closely relate to agility, in particular the need for:

- **Real-time Response** – to allow the fraud management organization to detect threats more quickly
- **Greater Accuracy** – to provide the fraud management organization with fewer false positives while not missing potential fraud cases so that they can respond more quickly to alarms and potential suspects
- **Additional Data** – to provide the fraud management organization richer and more complete data so that they have better visibility into the alarms and potential suspects and can investigate alarms and process cases more efficiently

Fraud management organizations that are requiring more agility in their fraud response are, therefore, asking for an FMS that has greater agility in every major area. The core functions of the FMS are still necessary therefore, even when the priority is to provide greater agility to the fraud managers, but to address the agility need, flexibility must be built into every core component of the system.

The Agile Data Analytics Revolution Reaches Fraud Management

Just as agility is becoming a critical requirement of fraud management organizations, agility has also become a critical requirement for data analytics. In fact, over the past 3-5 years, the analytics world has been undergoing a dramatic shift from traditional approaches and architectures to those that emphasize agility and allow businesses to sense and react more quickly. So while investment in traditional reporting systems still continues, the fastest growing segment of the analytics market is the agile data analytics segment, which includes “data discovery” platforms that give the business users more analytic power and more control over their disparate data. These platforms emphasize agility over other characteristics, such as volume, and they are racing to the forefront of the analytics world, moving from niche solutions to a mainstream architecture because of overwhelming customer demand for more agile solutions.

Requirements from Recent RFPs for a Fraud Management System	FMS Requirement Category	Primary FMS Component Affected
"Close future gaps so the FMS can manage all of the fraud threats being experienced by the business"	Agility	Rules Engine
"An innovative and flexible solution to the company's current and future requirements"	Agility	Rules Engine
"Change the FMS to protect against current and emerging threats"	Agility	Rules Engine
"Flexible user definitions of rules and alarm thresholds – including 'on the fly' rule definition"	Agility	Rules Engine
"An increasingly strategic approach to fraud management "	Agility	Alarm/Case Management UI
"Real-time and automatic actions to reduce exposure to airtime fraud"	Real-time Response	Alarm Generator
"An informed, 'real time' aggregated view on traffic to help uncover fraudulent patterns"	Real-time Response	Alarm/Case Management UI
"Collect and process event data records (EDRs) in real time"	Real-time Response	Data Processing Module
"Minimize the delay that must exist from call completion to call rating to transmission to the FMS or billing system"	Real-time Response	Data Processing Module
"Fewer false positives and better prioritization ability so that restrictive fraud controls don't impact customer experience"	Greater Accuracy	Alarm/Case Management UI
"dig deeper by investigating call patterns when fraud is suspected"	Greater Accuracy	Alarm/Case Management UI
"Include all data, including real-time customer and payment data"	Additional Data	Data Processing Module
"Use many different data sources, including a variety of formats and a variety of technologies (e.g. ,3G, 4G, LTE, IP, etc), and define and use new data sources"	Additional Data	Data Processing Module

Table 1 – Select requirements from FMS RFPs and requests for information issued in 2012

The reason for this rapid acceptance of these products is a strong desire for more and better analytics that allow the business to move faster. So, while Analytics and Business Intelligence (BI) has been a top priority of CIOs for the past ten years and it remains the top priority of CIOs[1]

[1] Gartner press release, "Gartner Executive Program Survey of More Than 2,000 CIOs Shows Digital Technologies Are Top Priorities in 2013", January 16, 2013.

today, there is recognition that traditional analytic approaches have not reached their potential. In fact, Gartner Research has reported that 70-80% of Corporate BI projects fail[2]. This shortfall is due to a number of factors, with the main one being that the traditional approach didn't free the data for the business to use and it simply didn't allow analysts and the analytic application developers to move fast enough to support the changes the business.

Those agile data analytics technologies have given business analysts and IT/BI groups greater control over their data and a fast way to construct analytic applications. They are now being applied to a host of business areas where agility is a critical requirement, such as sales and marketing, finance, strategic planning, customer service, and fraud management departments.

The Advantage of Using an Agile Analytic Platform to Manage Fraud

When an agile analytics platform, such as a data discovery platform, is applied to fraud management there are a number of advantages. When used as the foundation for an FMS, the agile analytics platform provides advantages for all system components. These advantages are shown in table 2.

Advantage of Agile Analytics Platform	**FMS Component Affected**	**Benefit When Applied to Fraud Management**
Rapid data integration – including the ability to combine disparate data sources	Data Processing Module	❯ Improve fraud detection accuracy or resolve cases faster by enhancing CDR data with additional data to give fraud analysts a more comprehensive picture of fraud suspects. ❯ More quickly identify new fraud patterns
User-configurable analytic logic	Rules Engine and Alarm Generator	❯ More rapid modification of alarm and rule configurations to adjust for changing thresholds and new or changed fraud patterns ❯ Greater resolution of alarm and rule definitions which can lead to more accurate identification of potential fraud
Exploration and discovery	Alarm/Case Management UI	❯ On demand data access and ad hoc analytics that enable fraud analysts to drill into the data that led to the alarm and access different data sources to evaluate fraud suspects. ❯ Greater flexibility to evaluate potential new fraud patterns and incorporate new controls into the rules engine

Table 2 – Advantages of using an agile analytics platform as a foundation for an FMS

[2] Patrick Meehan, president and research director in Gartner's CIO Research Group interview with Computer Weekly (http://www.computerweekly.com/news/1280094776/Poor-communication-to-blame-for-business-intelligence-failure-says-Gartner)

Introducing Lavastorm Fraud Manager for Communications Services Fraud

Lavastorm Fraud Manager is a comprehensive FMS that uses the Lavastorm Analytics Platform, a fully configurable, agile analytics platform, as its foundation. Unlike other FMS systems that may have an analytic engine inside with hard-coded analytic rules, Lavastorm Fraud Manager exposes the platform's full analytic capabilities to the fraud management organization, and, therefore, provides organizations with an open, agile FMS that offers superior agility. Lavastorm Fraud Manager includes these unique capabilities:

- **Fraud Management Essentials** – A collection of pre-defined alarm rules, aggregates, workflows, hotlists, reports, user structures, case management structures, CDR fields, customer details, and profiles, that captures industry best practices for fraud management. Fraud Management Essentials ensures that organizations can deploy a value-generating, customized FMS in just a few weeks.

- **Read from anywhere** – Read data from any source, including CDR data, customer relationship management systems, billing systems, social media sources, employee databases, dealer databases, and more.

- **Ad hoc investigation with query, drill down capabilities** – Access new information such as account profiles, usage histories, social media profiles, and suspect reports through the system's in-context data analysis and enrichment tools. These information sources allow users to go beyond the standard views of each case, which provides relevant customer, use, alarm, and historic data, to conduct ad hoc investigation on additional data sources.

- **User-controlled definitions – suspects, alarms, more** – Tune existing alarms, rules and suspect definitions for optimal detection and extend the fraud management system by creating new alarms, rules and suspect definitions to detect new fraud patterns as they develop over time.

- **User-defined data enrichment** – Enrich CDR data with any source, including customer, product, rating, and other relevant data to give analysts information to determine the nature, impact, and appropriate response to fraud. Organizations have the ability to define their own enrichment modules, including adding user-defined fields and rating on almost any data field, to customize the system as new data becomes available or relevant.

Improved Business Results from an Agile Fraud Management System

Some of the benefits and advantages of using an agile analytic platform for fraud management are show in the case studies below.

Mobistar Reduces Fraud Risks and Improves their Bottom Line

Mobistar, one of the major telecommunications service providers in Belgium and Luxembourg, faced more fraud threats and a greater variety of fraud threats as their customer base grew. In the face of these increased threats, Mobistar sought a new FMS to address two needs: 1. To allow the company to understand emerging potential threats more quickly, and 2. To increase their efficiency in managing fraud cases and lessen the potential negative economic impacts of fraud on the company's bottom line. They chose Lavastorm Fraud Manager because the flexibility of the system would allow Mobistar to adapt to changing threats, case management priorities, and financial goals. They identified the following benefits to the new approach:

- **Superior Accuracy** –Mobistar was most concerned with running fuzzy-matching analytics for all new subscribers, subscriber profiling, and sequential analysis. For these three controls alone, Mobistar has achieved a hit rate of over 90 percent. Across the board, Mobistar has tripled its fraud threat hit rate to more than 60 percent.
- **Faster Fraud Identification** – "With certain queries, we're able to run specialized analyses in real time to detect and prevent the latest fraud threats. We can run matches of suspected fraudsters against older fraud cases to narrow down the list of suspects," said Stéphane Dose, Fraud Expert Mobistar. "These queries have shortened our investigation time for certain fraud types significantly, and the hit rate is higher than ever."
- **Greater Control to Adapt the FMS** – "With Lavastorm Analytics we can automate features, freeing up additional resources for more proactive fraud response and scenario analysis. Because it's so flexible, we can innovate new fraud prevention methods on our own," said Fabrice Deneft, Fraud Operational Manager, Mobistar.

Kable Deutschland Optimizes Fraud Management Processes

Kabel Deutschland (KD) faced greater exposure to fraudulent customer activity as it grew to become Germany's largest cable operator. The company struggled to manage the volume of data and analysis required to mitigate this risk using Excel and SQL queries. Additionally, fraudsters were always trying new tactics, putting pressure on KD to both automate and accelerate processes and continuously test new quality checks and query billing systems in real-time. While improving revenue assurance (RA) and fraud management (FM) processes was critical, KD did not want a fraud management system that would prevent them from moving into additional areas or tweaking the kinds of services they offered and how they offered them. They identified the following benefits to the new approach:

- **Faster Identification of New Fraud Types** – "We can analyze new theories or questions on the fly and easily translate them into a persistent process in [Lavastorm Fraud Manager]," said Christoph Klein, Sr. VP, Credit Management & Revenue Assurance, Kabel Deutschland.
- **Less Bill Shock and Better Customer Experience** – KD continuously monitors key processes and uses results from the system to proactively serve customers. Says Klein: "For one example, we saw that a customer's call volume increased significantly. We called the customer and it turned out that a new foreign student had moved in and was calling home a lot. We were then able to control spend for the customer."
- **Real-time Response** – "There used to be at least a 24 hour delay to detect fraud. Now it is near real-time," said Klein.

Additional Information on Lavastorm Fraud Manager

For additional information on Lavastorm Fraud Manager, visit http://www.lavastorm.com/products/applications/fraud-ready-system/. To experience the benefits of the Lavastorm Fraud Manager, request a demonstration by contacting Lavastorm Analytics at http://www.lavastorm.com/company/contact-us.