Lavastorm Transaction Warehouse (LTW) 3.4 includes new and significantly improved capabilities for both the fraud analyst and the fraud manager. These capabilities dramatically improve the ability for providers to keep pace with the fraudsters, by enabling them to continuously and rapidly adapt their systems and their methods, while at the same time optimizing fraud analyst productivity.

**For the Fraud Analyst**

LTW 3.4 provides new alarm and case management functionality that automates and simplifies the creation, prioritization and resolution of individual alarms, cases and master cases. It enhances how the fraud analysts can see, correlate, organize and source different alarm and suspect data, helping to ensure that the most important alarms and cases are worked first. It provides improved tools to address cases, increasing the number of cases worked by each analyst, and improving overall financial productivity.

- **Alarm Routing and Case Creation:** All alarms, including both newly generated and historical alarms, can be specified to automatically route to a new or existing case, or to generate a new alarm for the Alarm Manager.

- **Alarm and Case Management:** Analysts can operate almost exclusively within their Case Manager view for the range of tasks they perform to research and resolve fraud threats, including researching underlying CDRs and any associated alarms or cases. This consolidated workspace directly improves analyst focus and productivity.

- **Case Summary:** Analysts can view summary information for all cases within a folder, and drill down from this Summary through to each case, the associated alarm(s), and directly back to the raw CDR data itself.

- **Alarm Window Optimization:** Sliding alarm windows, and the option to include or exclude previously-alarmed data, increase the precision of issue detection, reducing research time and false positives.

- **Advanced Sorting, Filtering and Searching:** Organization of alarms and cases, including the use of dynamic templated queries, aid the investigative process and helps analysts identify the highest priority cases, or ones that should be associated together.

- **History Exclusion:** Anomalous but explained usage spikes can be optionally excluded from a user’s profile to avoid skewing the ‘normal’ usage pattern for that user.

- **Workspace Personalization:** Analysts can personalize and optimize their Case Manager view (display settings, re-sizeable grids, sort options, etc.) for their specific role and work style.deployment that capitalizes on existing infrastructure.

**For the Fraud Manager**

LTW 3.4 places an entirely new level of adaptability into the hands of the fraud manager, without time delays or costs frequently associated with the use of corporate or third-party technical resources.
By directly enabling the fraud manager with the intelligent tools to quickly detect new threats and immediately implement the rules to intercept them, they can continuously adapt their fraud management operations to keep pace with fraud.

Alarm Testing and Optimization: As new Alarm Profiles are defined by the fraud manager, they can be tested against real data to ensure the right level of detection, run against historical data to identify suspect events that may have gone undetected by previous profiles, and then immediately put into full production.

- Flexible Dimensions: The fraud manager can organize CDRs by whichever dimensions make the most sense for specific fraud threats and controls. These may include customer segments, pre-defined and changing cohorts, products, Account ID, Trunk Group, Switches, or OCN, among others.
- Configurable Aggregates: Aggregate definitions can be easily adapted by the fraud manager to respond to changing threats and detection techniques. Through this process, analysts are provided smaller, better organized populations that dramatically improve the detection and pattern analysis.
- Score-based Highlighting: Automated highlighting of alarms and cases, configured by the fraud manager, speeds the identification of top priority issues, based on either personal work patterns or corporate ‘best practices’.
- Reports, Metrics and KPIs: Automated generation and delivery of key reports and analyses, configured for each user’s specific role, provide the information each analyst and manager need every day.

For the Internal Security Officer
- New security features within LTW 3.4 also improve the ability to detect, investigate and manage internal fraud risk, by limiting access to certain types of alarms and cases to select groups of users, and enabling separate fraud profiles.

For IT Management
- LTW 3.4 operates with Oracle 11g (release 11.1.0.6 or later); LTW 3.4 does not support Oracle 10g or prior versions of Oracle.

“Keeping up with the challenge of detecting new fraud threats as our business grows is essential to protect our subscribers and our financial results. With LTW 3.4, we are able to achieve this goal through three important elements; a proven, world-class fraud management platform, a highly efficient operating environment for our analysts to detect and prevent fraud, and the ability for our fraud managers to quickly and continuously optimize the fraud management environment for maximum results.”

Head of Fraud, RA and BI
Multi-national Quad-play Provider

LTW and Adaptive FMS
LTW 3.4 is the heart of MDA’s AdaptiveFMS Platform, which provides a robust set of fraud solutions to address identity, payment, operational, and usage fraud – all leveraging a single technology platform.

The key elements of AdaptiveFMS, as enabled by LTW 3.4, are outlined here.
Data Enrichment: CDR data is enriched with customer, product, rating, and other relevant data, to create the greatest operational value from data flowing into the system. Fuzzy matching of different customer representations helps create a single entity view. These capabilities enhance both detection and case management, giving the fraud analysts better information and tools to make decisions on the nature, impact, and appropriate response to fraud.

Aggregation Engine: CDRs can be organized by whichever dimension(s) makes the most sense for the specific fraud threat and fraud controls. These may include customer segments, pre-defined and changing cohorts, products, Account ID, Trunk Group, Switches, OCN, and others. Analysts can easily adapt the aggregates to respond to changing threats and detection techniques. Through this method, analysts create smaller, better organized data populations that dramatically improve the detection and pattern analysis.

Hotlisting: Providers can hotlist on any data element or threshold, such as the IMEI, “B” number, etc. - not just on telephone numbers or related markers – in order to strengthen detection and accelerate critical alarm and case management activities.

Simple and Composite Rules: Fraud managers can establish both simple (single clause) and composite (multiple clause) rules on any type of data (customer, usage thresholds, “B” number, etc.). Composite rules enable providers to isolate on multiple variables that when seen together, reveal stealthier forms of fraud.

Pattern Analysis: Simple white lists are replaced by embedded pattern analysis that can look at patterns such as historical customer profiles or profiles across cohorts, which provide operationally valid methods to understand possible fraud or to use pattern-based methods to eliminate alarming on normal usage.

Scoring and Ranking: Effectively score, filter and route cases so that analysts work on the most important cases. Utilize intelligent scoring and ranking methods with a flexible case management environment to filter and route alarms with the greatest financial risk, affiliate alarms to form complete and coherent cases, and enable fraud teams to maintain high levels of productivity while maximizing fraud hit rate.

Case Management: A visually rich and intuitive web-based environment presents relevant customer, use, alarm, and historic data so the analyst can understand and action the case with a clear and complete view. Simplifying the visual relationships among alarms and cases enables analysts to forensically understand the case, inter-relate cases to understand if there are larger, more organized threats, and drive the case to closure through the respective workflow stages.

Reporting and Optimization: High value reports, KPIs and analyses on the performance, trending and financial value of fraud detection and case management, provide management with a constant and accurate view of the threat, and the effectiveness of fraud operations.

With LTW 3.4, fraud managers obtain increasingly powerful analytics, and the flexibility to quickly detect new threats and immediately implement the rules to intercept them. LTW 3.4’s streamlined case management provides fraud analysts with operational efficiencies and higher fraud resolution hit rates. In total, the system gives providers the capabilities they need to perform the automated, efficient and effective fraud management needed to keep pace with the fraudsters.