Not only banks and insurance companies but also corporations from the non-finance sector are increasingly shifting their focus from the detection of fraud to its prevention. Fraud is neither limited to a region nor to an industry nor has it anything to do with the size of the organization. National and international studies, e.g. by Association of Certified Fraud Examiners (ACFE), show that the damage caused by fraudulent actions pose a serious threat to the economy.

Due to criminal creativity, new fraud variants evolve every day – regardless of whether online banking, insurances, tendering procedures, or internal fraud are concerned. Fraudsters increasingly use electronic media for their criminal activity, since "invisible" and anonymous money transactions facilitate the concealment of fraud. Yet, the actual fraud-induced costs reach far beyond the financial loss. Banks, insurance companies, and enterprises are challenged with securing their customer's assets, avoiding own financial disadvantages and long-term damage of reputation. Hence, methods for fraud prevention become more important to cope with today’s manifold fraud scenarios in an efficient way.

Real-Time and Ex Post Anti-Fraud

Siron®FD/R uses analyzing techniques especially developed for fraud detection and contains numerous predefined scenarios for powerful anti-fraud measures. These scenarios follow recommendations by ACFE and best-practice examples from FICO consultants. The research system recognizes typical patterns of fraudulent actions and forwards alerts to Case Management. Siron®FD/R also evaluates suspicious processes and transactions in real-time and blocks them. The embedded real-time module grants minimal response times with high decision quality and aims at fraudulent activities with a high damage potential.

Siron®FD/R – Highlights at a Glance

- Reliable, flexible standard solution for effective protection against the most various fraud crimes
- Real-time analysis of data and events that trigger alerts
- Modern analysis methods, such as multi-channel and time-series, pattern detection, or behavioral monitoring to identify complex fraud patterns
- Predefined scenarios to detect fraudulent actions
- Intuitive scenario editor for easy adjustment of the risk-based check strategy including simulation options (what-if analyses) to further optimize the scenarios
- Graphical Link Analysis to visualize relation networks
- Case Management for seamless documentation and analysis of potential fraud cases
- Automated workflow for SARs in a country-specific format
- Compliance with the obligations for record keeping through audit-proof documentation
- Easy integration of front-end or back-end systems for flexible monitoring of interfaces according to customer requirements available for any transaction type
- Use of customer data from Siron®AML without storing data at multiple locations

For further information www.tonbeller.com
**Prevention through Complex Event Processing technology**

Cases of fraud consist of complex event chains requiring the analysis of the interaction between single events within a tight timely sequence. Siron®FD/R uses powerful Complex Event Processing technology to link events that do not have any apparent fraud relevance. Doing so, the system continually processes, stores, and links real-time and historical data. If suspicious patterns and sequences are detected a warning or an alert will be issued that can be evaluated promptly to take immediate action. This prevents financial damage in advance by stopping payments or processes, since the system itself initiates the preventive measures.

**Address New Fraud Variants Fast and Efficiently**

Siron®FD/R also takes the growing momentum of new fraud types into account. To minimize fraud risks specified in the risk analysis, the check strategy must be continually revised and adjusted. Siron®FD/R empowers anti-fraud employees to address these changes in a flexible manner. New fraud types can be integrated into the fraud detection screening fast and easily using a scenario editor designed for this purpose. Scenarios for specific fraud cases (e.g. internal fraud, external fraud) can be created and edited separately from each other. The Fraud Officer may also decide whether scenarios require monitoring in real-time, ex post, or in the simulation environment.

**Compliance with Data Security and Protection**

To monitor employee behavior with the necessary integrity, the research system must provide an adequate response to the requirements of data security and the protection of privacy. Through its sophisticated authorization system, Siron®FD/R guarantees that private data is only disclosed to authorized users in case of an alert. This ensures compliance with data protection regulations.

**Graphical Link Analysis to Visualize Relation Networks**

The graphic analysis of Siron®FD/R generates an overview of the suspicious persons including their relation network ties with third parties, other persons and employees. By visualizing payment flows and economic entities, it localizes concealed relations in no time and increases the fraud detection rate.

**Analysis of Alerts and Suspicious Activity Reports (SARs)**

Siron®FD/R analyzes and processes unusual behavior and transactions that match with the defined scenarios. All necessary details of the detected irregularities and alerts are available online to the Fraud Officer with just one click. This workflow and the audit-proof documentation ensure that users can always track the processing steps and the detection procedure.

Siron®FD/R helps Fraud Officers meet their obligation to report potential internal cases of fraud. They can file and send suspicious activity reports to the authorities from within the system. Siron®FD/R provides the necessary SAR templates.