

Siron®FD

Monitoring and screening of transactions, accounts, clients, employees log data and behaviour/profiles

With Siron®FD TONBELLER offers a turnkey, cost-effective and safe solution for all finance service providers, for fighting fraud.

Siron®FD is a system-independent user solution for preventive early diagnosis, analyses and monitoring of striking financial movements. Using Siron®FD you meet your liabilities within a short period of time; with moderate costs and fast.

Long-standing knowledge of the banking environment, the conceptual participation of credit institutions and auditors as well as currently more than 500 international clients at private banks, big banks and savings banks up to the present day make sure that the specific requirements of the credit institutions with respect to functionality, security, quality and efficiency are taken into account to a high degree. The use of our approved systems substantially contributes to the compliance of the legal requirements relating to supervision.

■ Key findings about Fraud

The true cost of fraud goes beyond the financial loss to the impact on reputation, diversion of management focus, morale and loss of trust within the team.

Nearly 85% of the worst frauds were by insider on the payroll and over 50% of the perpetrators were from the management (E&Y Survey 2004).

Fraud was not concentrated in any one geographic region, industry or size of the organization. As organizations open their business and of course their systems to electronic commerce, they become more susceptible to the risk of external fraud.

Fraud causes costs more than \$400 bn. a year and broadening up the array of fraudulent activities daily. Fraudsters increasingly leverage their crimes with technology and these "invisible" of electronic monetary transactions, makes fraudulent activity easier to hide. Anti-fraud measurements shall prevent both financial losses and reputation damages.

■ Which Obligations and Requests arise for Credit Institutions?

In order to face the target to decrease the causes of fraud, the institutes look at different facts and compliance needs:

- Analysis of customer and employee data
- Analysis of transactions
- Analysis of employees access to customer accounts
- Analysis of profile data
- Analysis of relationships between customers and employees and within customers and employees

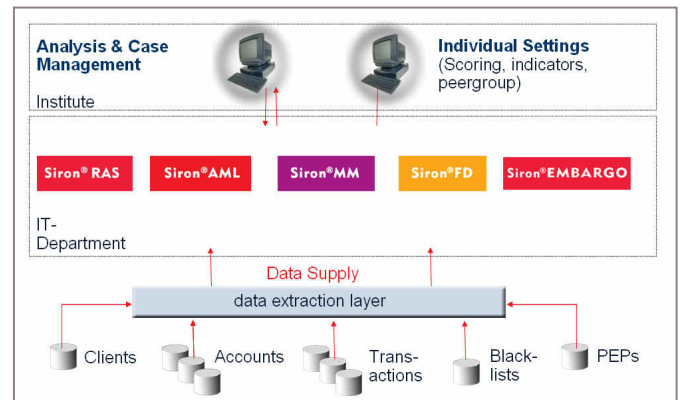
With regard to a steadily increasing complexity of modern banking products and growing electronic payment transactions these requirements can only be met with suitable IT-based analysis methods. List-based, periodical checking approaches will not be sufficient any longer on the background of the new requirements.

Extensive IT-supported security systems rather have to be implemented, which enable the compliance representative to examine all transactions and customers and employees profiles for the various fraud methods and to observe and document striking features over longer periods of time. Security, data protection and a revision-safe documentation of analysis results have to be granted mandatorily in the interest of the bank.

■ Technological Approaches

Accounts, customer and employee data, transactions, log files and recipients of account movements were in the centre of the inspection and the basis for the further steps.

Rule-based systems offer the compliance representative the possibility to describe behavior patterns known from the past by means of rules (typologies). Rule violations identified by the system (e.g., cash deposits of large, round amounts on newly opened accounts) are listed to the compliance representative for further judgment and tracking down. The disadvantage of these purely rule-based systems can be found



in the permanent manual effort to reconstruct the steadily changing methods in the system as well as in the mostly high number of "false" striking features.

Self-learning systems, however, make use of modern technologies (e.g., data mining), to create dynamic profiles for each customer/employee or group, based on the behavior up to now. In self-learning systems, therefore, an extensive knowledge (KYC, KYE) about each customer/employee is being built up. Behavior amendments, abnormalities and typical or similar behavior patterns will be automatically recognized by the system and shown to the compliance representative as risks. The disadvantage of these exclusively "self-learning" systems is based essentially in their high complexity as well as in the long introduction times (long learning curve of the systems).

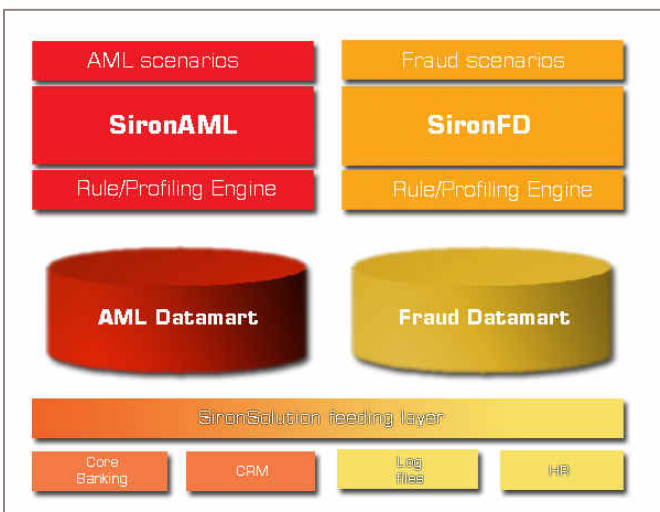
■ **Best Practice by Combination of Both Worlds**

Siron®FD makes use of both rule-based and self-learning technologies. Using the intelligent combination of both technologies, the institutions' requests for

- optimum protection from known money-laundering practices (adjusted rules / typologies)
- dynamic, risk-based adaptation of KYC, KYE profiles
- recognizing unexpected / unusual behaviors (e.g., cluster analysis, time progression analysis)
- automatic determination of existing risks (e.g., formation of risk customer groups)
- delivery of predefined fraud scenarios
- flexible definition of fraud indicators
- easy way to unhide economic units like employee vs. customer an vice versa (with link analysis)

will be realized in an optimal way.

There is a huge similarity between Siron®FD and Siron®AML. Both do have the same in over 500 installations proven easy usability. In addition to the Siron®AML functionality, Siron®FD monitors the recipients of account movements and the log files of employee activities.



■ **The Solution in Practice**

With Siron®FD and Siron®AML, the complete process is mapped, from data provisioning, setting up data marts by means of scoring, monitoring the suspicious cases up to reporting / logging. In this case, by means of its integrated and standardized support, Siron®FD and Siron®AML guarantees a high degree of efficiency increase and quality improvement, a complete documentation and logging: at minimum costs with lowest effects on the core business.

Siron®FD and Siron®AML can be implemented without problems in any existing infrastructure and is available on all platforms (e.g. Windows, Linux, Unix, z/OS, OS/400). Data provisioning can be carried out both directly from the

operative systems and from a data warehouse already existing.

External data (e.g., embargo lists of the EU, OFAC, PEP-databases, HR systems or log files) are completely integrated into the process.

The implementation of Siron®FD and Siron®AML into the existing infrastructure enables shortest introduction times and costs.

The flexible scoring procedure, based on up to 200 individual rules / typologies, 100 customer groups as well as adaptive customer profiles makes it possible for the compliance representative to quickly and efficiently build up the striking check portfolio (data mart). The further analysis and evaluation of the risks shown is supported by means of a comprehensive case management.

In principle, all system settings and rule adaptations can be carried out by the compliance representative himself after a short training period.

In the context of the workflow, all checking actions are automatically logged by the system so that the compliance representative can account for the checking process in detail any time.

In the Siron®FD and Siron®AML reporting module, detailed performance figures are made available about the results of the fraud and money-laundering analysis. All report-relevant information is edited by the system and displayed and archived in arbitrary formats.

When provisioning the data (data collection and provisioning) TONBELLER supports the customer in the context of integration consulting. Furthermore, TONBELLER provides the required technical and professional support for Siron®FD and Siron®AML, which takes into account the high and permanently changing requirements of the supervisory authorities.

TONBELLER AG
Werner-von-Siemens-Str. 2
D-64625 Bensheim

Fon: +49 (0) 6251 / 70 00-0
Fax: +49 (0) 6251 / 70 00-140
www.tonbeller.com