

kdprevent™ is an analytical software solution that supports financial institutions in detecting money laundering activities and other financial crimes. The system is based on state-of-the-art data-intelligence techniques in combination with domain knowledge of legal experts. It covers the new legal requirements in Europe, the United States, and in the major offshore markets. Thanks to its open architecture, it is possible to integrate kdprevent™ into almost any IT-environment. In addition to the classical management and control of a bank in the fight against financial crime, kdprevent™ also provides preventive functions to detect potentially fraudulent behavior even when it occurs following patterns never seen before.

Financial Crime

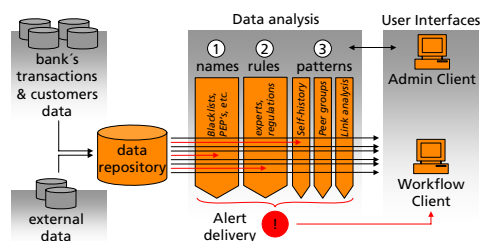
The prevention of money laundering, financial crime and terror funding, have become a major challenge for banks and asset managers throughout the world. The task is not only to detect and to investigate suspicious transactions, but, whenever possible, to block them before they occur.

The solution

kdprevent™ is an automated software solution designed to detect *unusual*, *unexpected* and *suspicious* activities of a bank's customers. Upon detection, it automatically delivers alerts to the responsible individuals in a bank, typically relationship managers and the Legal & Compliance officers.

kdprevent™ offers the possibility to configure, test and tune various detection techniques and to fully automate their application. The history of all identified cases is systematically recorded. The product documents all interactions with the system, thus maintaining a complete audit trail.

kdprevent™ is based on three major elements: a *Data Repository*, an *Analytical Engine* and *User Interfaces*. Due to the modularity of the software, various combinations and integration approaches are possible.



Data Repository

Data from different sources are integrated into a unique data repository, and pre-processed for the analytical procedures. As a minimal set of internal data usually customer information, account information and transactional data is loaded. Additional data, such as product usage, channel or contact behavior of the customers, increase the analytical power.

In addition to the bank's internal data, the system can make use of any external data source, such as lists of politically exposed persons (PEP), black lists and lists of exposed countries. All external data sources to be integrated can be defined according to the user's needs. Interfaces to commercial providers of black lists (such as World Check, Thomson or Factiva) are already in place.

Analytical Engine

The analytical engine is designed to detect unusual, potentially suspicious, activities of a bank's customers. It uses three major detection techniques that can be individually configured and automatically applied:

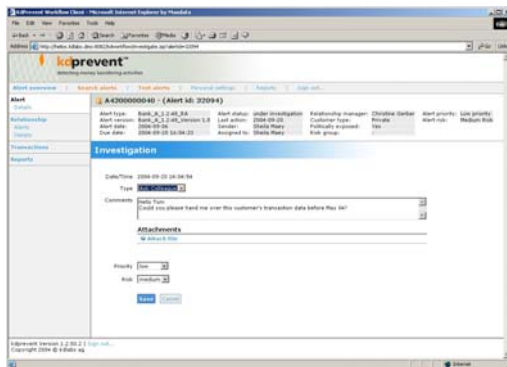
- *Name, source and target matching*: multi-language comparison of the customer database and of transactions (names of senders and beneficiaries) against internal and external black lists based on the most sophisticated names matching procedures.
- *Application of rules*: based on integrated Legal & Compliance expertise as well as internal know-how, alert rules are flexibly defined and applied according to banking regulations and to the bank's internal requirements.
- *Pattern recognition*: state-of-the-art data analysis and data mining techniques deliver an alarm even based on previously unknown, but suspicious behavioral patterns, such as significant deviations from a customer's historical behavior.

User interfaces

kdprevent™ generally serves two user groups: the relationship managers and the Legal & Compliance officers. According to the bank's needs, the members to be included in the workflow as well as their interaction rights can be flexibly defined.

Relationship Managers: They are alerted by the system in case of suspicious customers and transactions. A description of alert reasons is included in the alert. Relationship managers can investigate, administer and comment on the identified cases and pass them to the users in the Compliance group.

Legal & Compliance officers: the officers can monitor and check all open and closed cases and generate status reports at any time. To manage the process, internal and external detection rules as well as legal requirements can be flexibly implemented, tested, monitored and tuned. In addition, users and profiles can be defined and managed. This leads to an efficient internal workflow control as well as to an effective management of a bank's effort in the fight against money laundering and financial crime.



Additional components

RTTS (Real-time transaction screening): A completely integrated application checks incoming and outgoing transactions in real-time. Suspicious transactions are set on hold, alerts are generated into the kdprevent™ workflow, and interrupted transactions can be released or prevented. All steps of the process are documented within the proven audit trail of kdprevent™.

Data encryption package: In addition to the security features in the basic package of kdprevent™, sensitive person-related information can be stored in an encrypted manner within the kdprevent™ database by using strong and industry-proven encryption methods (DES/3DES). All related processes decrypt such information on the fly, so that sensitive information is never revealed to any unauthorized person.

Key benefits of kdprevent™

- **Completeness:** state-of-the-art technology investigates all aspects of money laundering and financial crime according to current legal regulations.
- **Security:** provides maximal protection against damage of reputation, legal consequences and financial loss.
- **Modularity:** a wide range of modules and components can be individually combined to cover single requirements up to the most complete Compliance demands.

- **Quality:** Swiss quality standards are combined with extensive Legal & Compliance expertise.
- **Reliability:** professional maintenance, active support and continuous development of the product are provided.
- **Flexibility:** can be integrated into practically any IT-environment and tuned according to the needs of the end-users.
- **References:** used by leading financial institutions such as AIG Private Bank Ltd. and Dresdner Bank (Switzerland and Luxembourg).
- **Price:** Exceptional functionality at a competitive price.

Contacts



European Business Consultants (EBC) was formed in 1998 to help organisations, primarily in the financial services sector, to develop their capabilities in the rapid analysis of information. EBC focuses on providing solutions, which yield real value to the client, via modular solutions and rapid development of the business model. Regarding the prevention of money laundering and financial crime, EBC proposes kdprevent™, a powerful solution developed by kd labs AG (Zurich, Switzerland).

Brian Howells
brian.howells@ebcuk.com
 28 Oaken Lane, Claygate, Surrey, KT10 0RG
 Phone: + 44 (0) 1 372 811 676

Paul Burkitt
paul.burkitt@ebcuk.com
 37 Cobden Street, Wollaston, Stourbridge, West Midlands, DY8 3RU
 Phone: + 44 (0) 1 384 345 988