FRAUD MONITORING

Modern, comprehensive solution for fraud detection and prevention in banking systems.

www.infigo.hr
INTRODUCTION

Banking institutions are increasingly faced with balancing the provision and maintenance of systems in a complex environment with growing risk - from threats and fraud. Statistics show the number of fraudulent activities and incidents is growing.

As fraudsters exploit new technologies and new vectors of attack, fighting fraud becomes a challenging task. In addition to this as Banks deploy new products across new channels the challenge is extended, which increases risks. INFIGO Fraud Monitoring (INFIGO FM) is a solution to this challenge.

INFIGO FM provides a view of a customer’s activity, near real-time detection of fraudulent activity, prevents atypical behaviour - and as a last resort - remediation.

All transactions (loans, withdraws, deposits, trades, etc.) across the growing range of channels (card payments, ATM use, Internet Banking, phone banking, face-to-face banking) leave a corresponding electronic footprint. The data (the electronic footprints) resulting from transactions is expected to increase with time, as customers start to adopt more digital channels for consuming banking services.

While banking system record this data, the complexity of the technology landscape means that in the absence of adequate real-time detection, banks adopt a reactive response to fraudulent incidents. This approach means any resulting actions are often too late and the damage (financial, brand value, reputation) is done.

KEY FEATURES OF INFIGO FM

- **Real time and near real time monitoring** of all activities in banking systems/channels allows prompt detection of any potentially suspicious or fraudulent activities triggered externally or by insiders.

- **Comprehensive view of customer activity** - providing fraud detection across all channels: Internet Banking; mobile banking; and face-to-face transactions.

- **Flexible and adaptable alerting system** - allowing for automated prioritisation and grouping of suspicious activities without technical assistance.

- **Web-based alarm console** - designed with user friendly navigation and integrated with external information systems, INFIGO FM supports prompt incident review, saving time for fraud analysts.

- **Case management** - recording all activities and additional data – INFIGO FM acts as a central repository for case activity, management and analysis.

- **Rule and analyst performance feature** - providing valuable information for future system and workflow enhancements.

- **Modular design and modern architecture** - allows integration with any technology, system architecture or banking system. INFIGO FM scales horizontally and vertically depending on volume of business transactions, and the businesses' needs.

- **Highly available and resilient** - INFIGO FM is built to be robust, allowing for partial system outages without any loss of functionality or data.

- **Continuous development** - supported by the INFIGO’s team of fraud experts, INFIGO FM is designed with capability at its core - evolving to detect and deal with new attack vectors.
INFIGO Fraud Monitoring (INFIGO FM) is a modern, comprehensive solution for fraud detection and prevention in banking systems.

It is capable of managing fraud on any channel (Internet banking, ATM, phone, face-to-face transactions) and provides users with the ability to detect and prevent fraud as it happens. This allows banks to adapt the INFIGO FM system to new types of fraud, reducing the advantage that fraudsters have, especially across digital banking channels such as Internet or mobile banking. INFIGO FM reduces loss from fraud - delivering a ROI (return on investment) almost from the start – and helps banks to maintain profitability and compliance with financial regulations. The objective of the INFIGO FM is to allow organisations to efficiently react to challenges in an increasingly complex risk landscape.
INFIGO Fraud Monitoring is capable of consuming data from external sources such as public corporate registers, national data sources, and global data sources - enhancing fraud detection capabilities. Combining suspicious activities with additional information enables fraud analysis with a single console – providing all the information required for case investigations.

The alert console provides a unique and completely customisable interface for alert management. Every event which triggers an alert is immediately shown within the console and is available for investigation. Depending on the investigation, a built-in workflow enables users to close one or multiple alerts with a custom status. The user can also e-mail one or more alerts to their colleagues, if needed. Alerts can be classified with a single click of a mouse, individually or all at once. The user is also able to add comments and to upload documentation relevant for the case(s).

Key features:
- Easy to use real-time alert notification
- Data drill-down for further analysis and investigation
- Fraud case workflow
- Full alert history and statistics

The system stores all audit data and information about performed activities by each user, without any limitations on amount of data or retention time.
This information enables users to identify areas to focus – allowing them to improve performance.

**PROACTIVE WARNING – LEVERAGE DETECTION TO ENABLE PREVENTION**

Depending on the alerts, the system can proactively mark high-risk transactions, detecting fraud before the transaction is completed, enabling users to prevent fraud before it occurs. By default, INFIGO Fraud Monitoring can call external web services or execute any program when an alert has been detected. Based on Splunk’s powerful machine-learning capabilities, various models can be applied to transactions and used in a scoring system for proactive warnings.

**DATA WAREHOUSING – KEEP THE DATA IN**

All collected data can be kept in the system available for instant analysis for an indefinite period of time. Data aging, backup and off-line archival are completely configurable. Thanks to the power of Splunk’s indexing and searching engine, statistical calculations can be performed on large data sets in matter of seconds.

**REDUNDANCY AND HIGH AVAILABILITY – RUNNING 24/7/365**

Redundant, high availability deployments are possible with practically no additional cost. High availability options such as data replication factor (denotes the number of redundant data copies) or search factor (denotes the number of redundant fraud interfaces) are configurable.

**MODERN WEB-BASED GUI**

INFIGO Fraud Monitoring system is a web application that only requires a modern web browser to run. The system can be integrated with any authentication system, including 2-Factor Authentication (2FA) authentication.

**FULL COMPLIANCE WITH EUROPEAN BANKING AUTHORITY’S FRAUD MONITORING REQUIREMENTS**

INFIGO FM allows detection, prevention and automatic blocking of fraudulent payment transactions. Parametrisation of rules, as well as integration with real-time black-list lookups and monitoring of atypical behaviour patterns (i.e. based on Geo-IP checks or any other parameter collected from the customer) allows for a highly efficient alerting with low incidence of false positives.

**CONTINUOUS DEVELOPMENT**

INFIGO provides education, expert services, strategic guidance and consultancy to meet customer’s needs. These services can be utilised to maximise the INFIGO FM system’s efficiency and tailor it to the specific needs of the customer. INFIGO’s fraud experts are continually developing the product to meet the challenges of the latest attack vectors and methods.

**ANTI-MONEY LAUNDERING**

INFIGO FM extends intelligence to support anti-money laundering (AML) laws and regulations. The product provides easy compliance with currency transaction reporting (CTR) requirements. It also provides capability for integration with different black-list providers and customer-identity management systems. Finally, it expands its core functionality to additionally track suspicious activity and generate the Suspicious Activity Report (SAR). The SAR breaks down the suspicious activities based on a rule set, which is divided into the following groups:

- Cash transactions
- Non-cash transactions
- Related cash and non-cash transactions

**PROVEN TRACK OF RECORD**

INFIGO FM is an innovative fraud monitoring and prevention product, with a proven track record, installed and used by some of the biggest banks in the region. It is an efficient fraud monitoring product with reporting and analysis that offers exceptional performance, and a quick return of investment while at the same time satisfying regulatory requirements.
## PREREQUISITES AND INTEGRATION

### PREREQUISITES AND SCALABILITY

INFIGO FM is a flexible and scalable solution, available for environments ranging from small (with several thousand accounts) to large banks (with millions of accounts and tens of millions of transactions per day). It can run on a stand-alone server or as a High Availability deployment on physical or virtual components.

- **Virtualization:** VMWare or HyperV
- **OS:** No requirements (Linux preinstalled)
- **DB:** No requirements (no database used)
- **Other:** Splunk Enterprise license

### HARDWARE OR VIRTUAL REQUIREMENTS

- **CPU:** 1-2 Intel quad/six core 2.0Ghz+ CPU
- **Memory:** 8GB+
- **Storage:** min. 400GB (depends on data retention policies)
- **Storage configuration:** SAS 15k RPM, RAID 10 or direct storage access

### HIGH AVAILABILITY

INFIGO FM provides built in high availability (HA). Each deployment can be configured to ensure data redundancy and fraud interface redundancy.

- **Data replication factor:** 2 or more (configurable)
- **Interface redundancy:** 2 or more (configurable)

### SUPPORTED DATABASES

INFIGO FM is capable of interfacing with any SQL based/ODBC supported banking system without need for installation of any software components on:

- DB2
- Informix
- MS SQL
- MySQL
- Oracle
- PostgreSQL etc.

### IN-HOUSE SYSTEM INTEGRATION

Integration with standard products (authentication, security, ticketing) is available out-of-the-box or with minimal customisations. Commonly integration (with ability to extend to other systems) is provided for:

- LDAP/AD
- CRM
- SIEM
- Service Desk/Ticketing

### AML BLACKLISTS INTEGRATION

INFIGO FM provides capability to integrate with different AML blacklists:

- FATF
- OECD grey list
- OFAC etc.