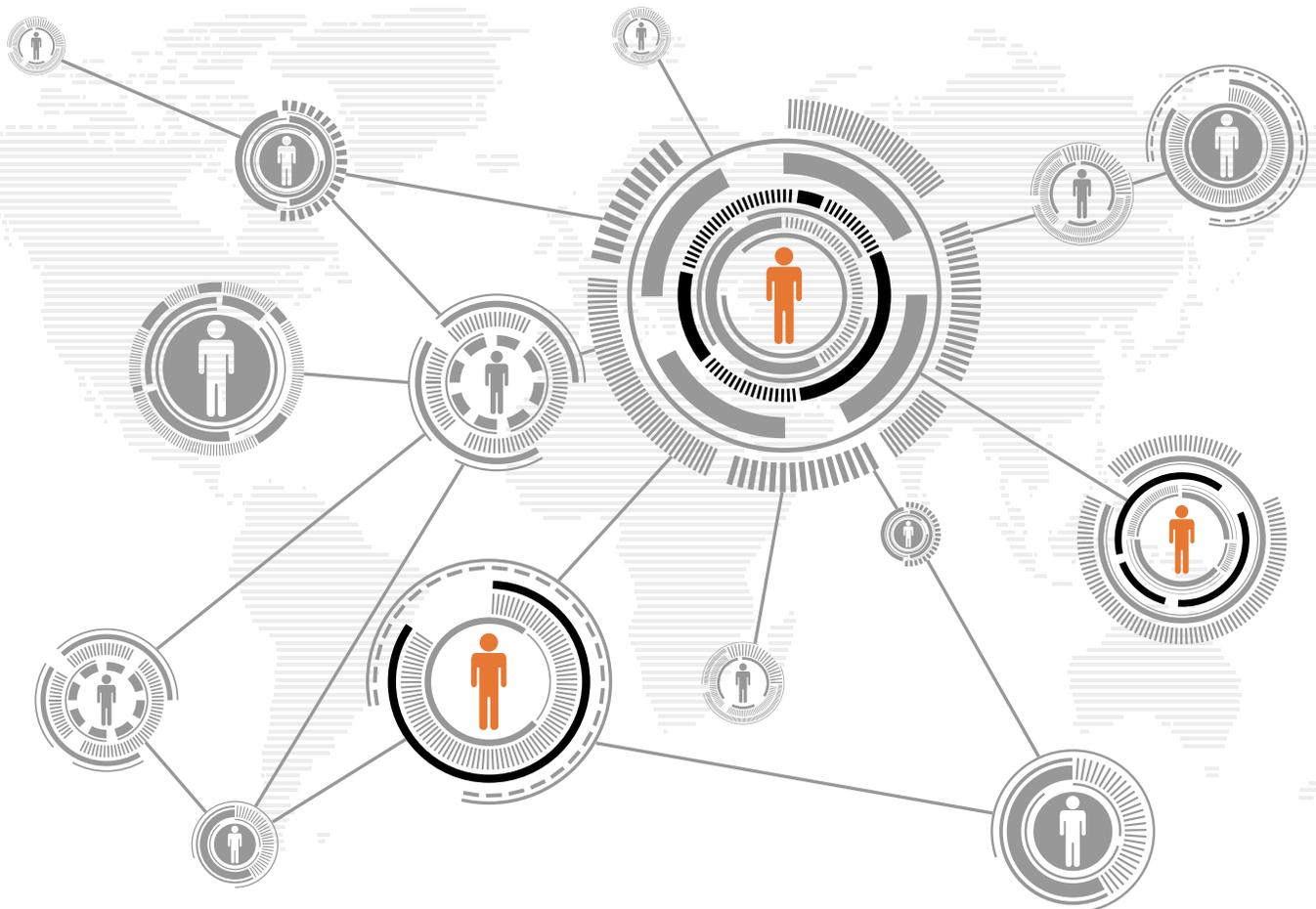# alessa

Financial Crime and Fraud Management Solution

Transaction Monitoring

Financial Crime Detection and Prevention

For organizations looking to enhance their financial crime detection and prevention programs, Alessa is a platform that integrates with core systems for real-time due diligence, transaction monitoring, sanctions screening and regulatory reporting capabilities.

Used for **anti-money laundering (AML) compliance, sanctions screening, enterprise fraud detection, and vendor risk management,** Alessa is configurable to clients' needs and can be deployed as modules or as a complete end-to-end risk management solution. Deployments can be on-premise, hosted or a hybrid of both.
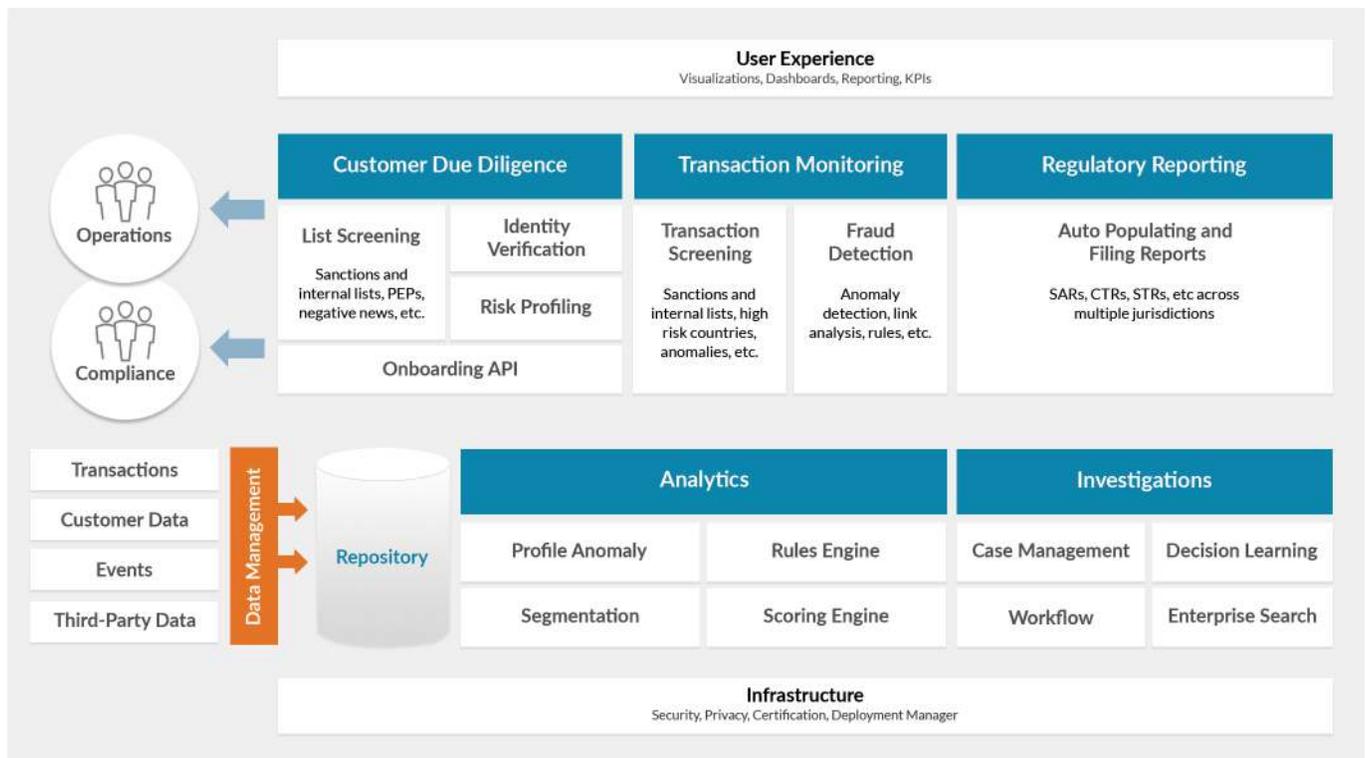

The full capabilities of Alessa for financial crime detection and prevention

Manage High-risk Scenarios in Real-time

Alessa accesses transactional data in real-time and/or periodically and feeds it into the analytics platform to detect high-risk scenarios or events. Once detected, the system will allow transactions to be blocked, investigated, or recorded with no action required.

Alessa uses advanced analytics and rules-based scenarios to score the risks associated with suspicious transactions and help fraud and compliance personnel refine and prioritize investigations.
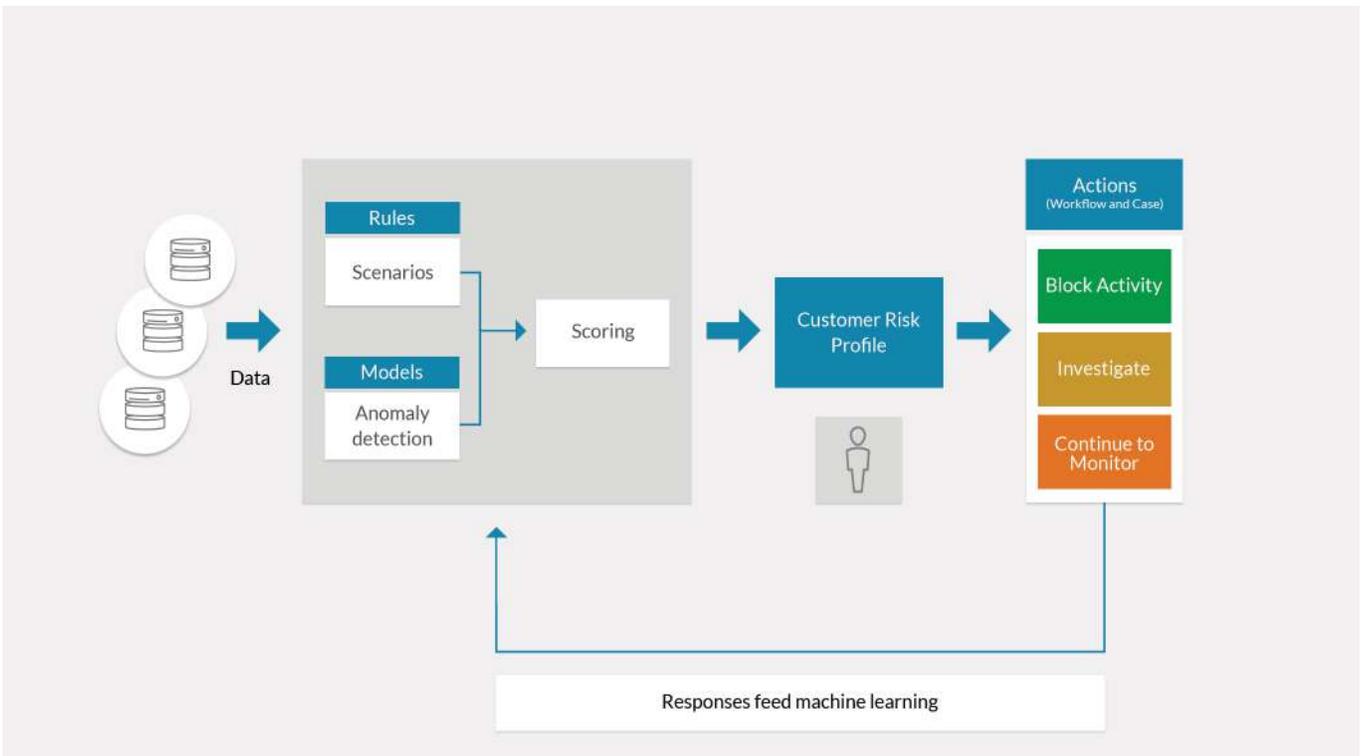
Capabilities

Real-Time, Periodic or Event-Based Monitoring

Monitoring of transactions and entities can be configured to be done in real-time, periodically or by specific events. The tasks execute the specific analytics and based on the results, create relevant alerts for further investigation and remediation.

Decision Learning

Alessa can be configured to learn how alerts have been actioned in the past and to reapply those decisions to future alerts. For example, if wire transfers to specific high-risk countries are always blocked then the system can be "taught" to always make that decision without the need for further human interaction.

Risk Scoring

Risk scoring is used to calculate the risk associated with a business or individual. Profile information and results from both the rules-based and advanced analytics engines are configured and weighted by the organization depending on their risk appetite.

Automated Regulatory Reporting

When a suspicious activity is detected, Alessa creates an alert with all the data needed for the regulatory reports. Once the alerts have been investigated and it is determined that the transaction(s) should be reported to the regulator, Alessa can auto-populate the reports quickly and easily. Almost 100 percent of the threshold reports and as much as 75 percent of the suspicious activity reports can be auto-populated with Alessa.

Designed to Scale

Alessa is scaled to monitor and screen millions of transactions. The technology can be designed to use multiple instances of the screening service and distributed across nodes for load balancing..

Machine Learning and AI

The advanced analytics models include capabilities for anomaly detection, machine learning, and predictive analytics. The models are continuously trained using the business' transaction history and case management actions. Alessa also allows businesses to deploy their own analytic models.

Rules-Based Analytics

While Alessa has out-of-the box rules for specific use cases, these are normally refined based on business requirements. In addition, the rules engine allows organizations to create and deploy their own rules, depending on their specific needs.

Real-time Configuration

Real-time transaction monitoring and screening is deployed using an enterprise service bus (ESB). The business systems route transactional data to the integration platform, and Alessa takes that message and performs the relevant analytics.

Once the analysis is done, Alessa returns a message to the infrastructure for all the relevant systems. In most use cases the message is to allow or block the transaction. Transactions that are blocked may also be further investigated using the case management module and a decision made to confirm or release the block. The decision made in the case then sends a message to the integration platform, and the relevant systems to perform the action.

Managing Suspicious Transactions

Upon identification of a high-risk transaction, businesses can automate investigations using workflow and case management within Alessa. Cases can be created manually or automatically and for either individual or a group of alerts. Workflows are configurable to be as granular or simple as required. Features include assignments to users/teams, permissions, escalations and root cause indicators.

During the remediation process, users transition cases through the workflow. At each transition, different users or groups can be assigned (as established by permissions) and comments and attachments added. Notifications within the case management module specify which users are notified, how they are notified (email, SMS or in-app), and the content of the notification.

Use Cases

Real-time Wire Transfer Screening

Alessa can be used to screen wire transfers in real-time. When the banking system initiates the request for a wire transfer, Alessa screens the sender and receiver against World-Check data and whether the transfer is to a high-risk jurisdiction. If the wire transfer is blocked, a message is returned to the banking system and the status is updated to "At Due Diligence".

An alert is triggered and routed to the appropriate person(s). If after investigation the decision made is to release the payment, the platform sends a new message to the core banking system to update the status to "Processed".

Alessa relays the request to the payment gateway using the messaging infrastructure.

Identity Verification

Alessa can be used to verify the identity of businesses and individuals in the United States during the onboarding phase. Using CLEAR ID Confirm from Thomson Reuters, organizations can enter pre-defined information about the entity and Alessa will return a matching score along with potential matches. Staff can then confirm which match is the client and the system will auto-populate any known missing information.

Periodic Sanctions List Screening

Some customers use Alessa to screen customers weekly against World-Check database from Refinitiv. At a specific time, a task is triggered to get the customer data (either a file or by directly connecting to core systems). Once the matching process is completed and all hits are sent to the case management module for investigation and remediation.

Health Insurance Claims Monitoring

For the use case where Alessa is used to identify potentially fraudulent insurance claims in real-time, first the claim management system sends the claims transactions to Alessa.

Alessa then examines the claims using its anomaly detection engine and scores the transaction based on its attributes. If the transaction is considered high-risk then a message is returned to the claims management system, the status is updated to "At Investigations" and an alert is sent to the appropriate person(s).

If after investigation the decision is made to deny the claim, the platform sends a new message to update the status to "Denied".

Success Story

Challenge

One of the leading commercial banks in the Caribbean needed a new solution to help it fulfill its anti-money laundering (AML) compliance requirements. The high volume of transactions through the bank was challenging, and manual review of transactions was ineffective and inefficient.

Solution

Alessa helped the bank enhance their AML compliance requirements through:

- Automated transaction monitoring
- Sanctions list screening during onboarding
- Periodic sanctions list screening to identify changes in the risk profile of existing customers
- Real-time screening of senders and receivers of wires and drafts
- Automated regulatory reporting that auto-populates and validates reports
- Data quality management, including identifying duplicates and parsing and standardizing records

Results

After implementing Alessa, the bank has already achieved the following benefits:

- Identified more risky individuals, businesses and politically exposed persons (PEPs) where additional due diligence is required
- Enhanced customer data quality across all branches
- Blocked more fraudulent transactions
- Reduced time spent on creating and filing regulatory reports
- Increased accuracy and reduced rejections of regulatory reports
- Increased staff performance by reducing time spent on routine and repetitive tasks
- Achieved greater level of compliance
- Created a greater culture of compliance by sharing responsibilities across the organization

About CaseWare RCM

CaseWare RCM Inc. is the maker of Alessa, a financial crime detection, prevention and management solution. With deployments in more than 20 countries in banking, insurance, FinTech, gaming, manufacturing, retail and more, Alessa is the only platform organizations need to identify high-risk activities and stay ahead of compliance. To learn more about how Alessa can help your organization ensure compliance, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at **www.alessa.com.**

150 Isabella Street, Suite 800,
Ottawa, ON K1S 1V7, Canada

1-844-265-2508

alessa@caseware.com

www.alessa.com