feedzai | Solution Guide

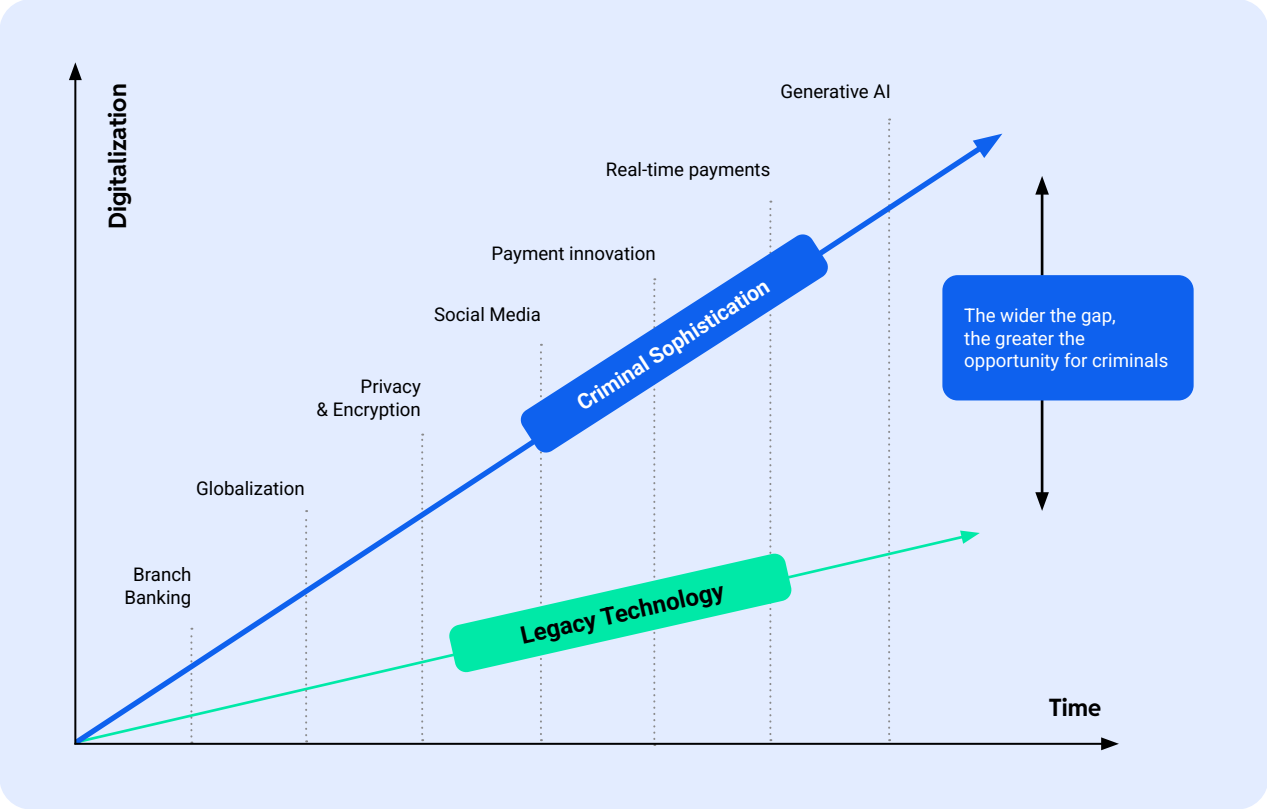
AML Transaction Monitoring

Contents

Contents

1. Introduction

Traditional anti-money laundering (AML) systems often struggle to cope with the complexity of today's financial crime challenges. These legacy systems typically heavily rely on rule-based approaches and static data that cannot keep up with the sophisticated techniques employed by criminals. Feedzai's anti-money laundering solution provides a modern approach to the problem by taking a holistic approach to the systems and relying on a combination of rules and machine learning to detect criminal activity and alert prioritization.



The rapid evolution of technology has expanded the avenues for illicit activity, making it easier for bad actors to launder money and evade detection. In addition, the high volume of financial transactions and the increasing interconnectedness of global markets can overwhelm traditional systems, leading to high false positive rates, increase of workload and inefficient investigations.

To effectively combat financial crime in this dynamic environment, AML systems must incorporate advanced analytics, machine learning, and real-time data processing to identify and adapt to emerging threats.

1.1. Effectively face the ever-changing market landscape

Traditional methods of compliance management, which rely heavily on manual processes, are not as effective in addressing emerging challenges. This creates risks, including costly fines, reputational damage, and business disruption.

Advanced technology, particularly AI and machine learning, has become a great ally in the fight against financial crime in recent years, and Feedzai's anti-money laundering (AML) transaction monitoring solution is an example of how financial institutions can leverage cutting-edge tools to create a robust compliance framework.

By automating the detection of suspicious activity, the capacity of prioritizing different alert levels and providing features such as rules management and model governance, Feedzai not only streamlines the compliance process, but also increases accuracy and adaptability. As a result, institutions can more effectively mitigate risk, stay compliant with ever-changing regulations, and focus on growth and innovation rather than the complexities of compliance.

> **Advanced technology, particularly AI and machine learning, has become a great ally in the fight against financial crime in recent years...**

1.2. Reduce False Positives

Minimizing false positives in AML programs is critical to maintaining both operational efficiency and customer confidence. False positives, which are legitimate transactions that are mistakenly flagged as suspicious, can overwhelm compliance teams and drain internal resources from investigating actual threats. This inefficiency not only drives up operational costs, but also risks missing true illicit activity, undermining the very purpose of AML programs. To address this issue, advanced AML solutions focus on reducing false positives, thereby increasing the accuracy and effectiveness of compliance efforts. By leveraging sophisticated algorithms and machine learning, these programs can better distinguish between legitimate transactions and those that truly warrant further investigation. This targeted approach not only reduces operational costs by streamlining compliance processes, but also protects the integrity of financial systems while maintaining strong customer relationships. As a result, financial institutions can improve their ability to detect and prevent illicit activity without compromising productivity.

> **Minimizing false positives in AML programs is critical to maintainingboth operational efficiency and customer confidence.**

1.3. Improve Alert Prioritization

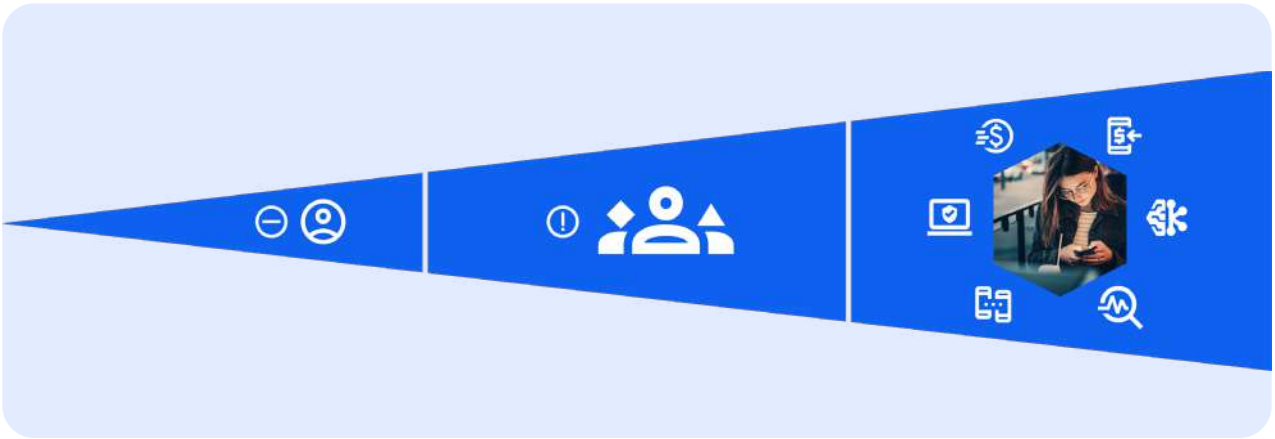
Effective management of alert prioritization and threshold adjustments is critical to the maintenance of robust AML practices. Traditional thresholds often struggle to keep pace with evolving criminal tactics and new regulations, resulting in outdated thresholds that can delay detection of emerging risks. At the same time, inconsistent prioritization affects the efficiency of triaging and analyzing alerts, and ultimately hampers analyst productivity. Feedzai addresses these issues by using machine learning to dynamically prioritize alerts, allowing analysts to focus on high-risk alerts first.

In addition, optimizing compliance analysis and reporting processes is key to operational efficiency. Feedzai enhances this by significantly accelerating case processing and regulatory reporting, handling up to 50 times more transactions and entities and enabling 20 times faster SAR filings. With tools such as SAR Manager, Feedzai simplifies the reporting process by automating the collection and validation of reporting data. SAR Manager generates regulatory reports in standard formats accepted by different jurisdictions which can then be submitted directly to the relevant regulatory bodies. By automatically populating key information based on case data, SAR Manager significantly reduces manual effort, reducing the number of clicks required to complete compliance tasks from an average of 22 to as few as 5. This streamlined approach reduces complexity and time, improving overall workflow efficiency and compliance effectiveness.

2. AML Transaction Monitoring Capabilities

2.1. Customer Activity Alerting

Feedzai offers a powerful combination of rules and behavioral profiles to enhance AML transaction monitoring. This dual approach targets both known patterns and suspicious behavior, evolving as criminals change their tactics. The solution workflow ingests the aggregated data on a configurable scheduled frequency to detect suspicious behavior in the customer and / or account history.



Rules Only Systems

- Only scored on transaction risk
- No in-depth context
- Inaccurate risk assessment

Cohort Profiling

- Group users with similar characteristics
- Profiling is based on the cohort
- Higher false positives

Rules Only Systems

- Profiling done on an individual level
- Hyper-granular entity views
- Frictionless Customer Experience

Feedzai's "Segment of One" or behavioral profiling creates individual profiles rather than relying on cohort-based assessments. This allows for accurate comparisons between an individual customer's current and past behavior. Using cohort groups to identify anomalies often results in a high number of unproductive alerts because it does not take into account the individual nature of each customer. A better risk-based approach is tailored to each individual to be effective.

When a new transaction occurs, Feedzai's profiling system compares it to the established spending habits of the individual or entity and flags any anomalies. By understanding customers at a granular level, financial institutions can set more accurate thresholds for different scenarios. This individualized approach ensures more relevant and productive alerts.

In addition, Feedzai's technology simplifies the process of adjusting and fine-tuning thresholds based on an organization's risk appetite. This flexibility allows for continuous improvement and optimization.

> **Feedzai's "Segment of One" or behavioral profiling creates individual profiles rather than relying on cohort-based assessments.**

2.2. Dynamic Thresholds

Not all customers pose the same risk. That's why organizations need to maintain an optimized risk playbook by assigning thresholds that accurately reflect varying risk profiles.

Feedzai's dynamic thresholds leverage multiple combinations of customer or account attributes across four key thresholds to fine-tune risk detection. As new patterns emerge, organizations can quickly create and implement new rules or models in days and integrate them into the workflow. By incorporating variables into both new and existing rules, organizations can take a more nuanced approach to risk management and make smarter decisions before alerts are triggered. For example, existing rules and thresholds can be adjusted - without the need to create entirely new ones - by taking into account variables such as the customer's risk score, nationality (especially in cases of dual citizenship), and the range of products they use.

2.3. Whitebox Explanations

When an alert is generated, the platform provides a clear explanation, giving the organization's analysts a head start on investigations and ensuring they understand the rationale. Feedzai's risk platform dynamically generates whitebox explanations - a layer that integrates rules with machine learning models. This provides users with contextual information about why an alert was triggered, why it received a certain score, or why a transaction was flagged as fraudulent. As a result, analysts can quickly understand the reasons behind an alert and focus on the relevant data without digging through unnecessary information.

2.4. Audit Rules

Audit rules are fundamental to maintaining the integrity and effectiveness of an AML transaction monitoring system. They define the parameters and conditions under which transactions are monitored and flagged for review.

4-Eyes Check

The 4-eyes check is a control mechanism that requires at least two people to approve rule changes before they go live. This process minimizes the risk of error and ensures consistency in the application of rules. By implementing a 4-eyes check, financial institutions can improve the accuracy and reliability of their AML programs and reduce the chance of accidental or malicious changes.

2.5. Audit Models for Alert Prioritization

Effective alert prioritization is essential to manage the high volume of alerts generated by AML transaction monitoring systems. These audit models are used to prioritize alerts based on assessed risk, enabling compliance teams to focus on the most critical cases.

» Model Risk Governance

Model validation ensures that models are functioning properly and producing reliable results. Governance helps address any issues that may arise, thereby maintaining the credibility and effectiveness of the AML program.

» User Autonomy

User autonomy in the context of audit models allows users to inspect, understand, and replicate models. This capability ensures that users can independently verify the functionality and accuracy of models. By storing all information used to build models in one place, financial institutions can increase transparency and facilitate audits and inspections.

Explainability for Audits

Explainability is a critical aspect of auditability in Feedzai's AML Transaction Monitoring. It involves providing clear and comprehensive explanations for the results generated by the models. This transparency is essential for both regulatory and internal audits as it demonstrates that the models are relevant, unbiased and compliant. The access to detailed explanations helps to demonstrate the integrity and fairness of the AML program, therefore fostering trust among stakeholders.

2.6. ML Alert Prioritization

The difficulty in prioritizing cases involving actual money laundering schemes has affected the consistency and quality of case investigations, as well as the productivity of analysts.

Feedzai prioritizes the alerts so analysts can focus on cases with the highest risk. Machine learning dynamically learns which cases will result in a SAR filing. This prevents repetitive alerts from reaching the analyst's disposition process and ensures that only relevant alerts that require attention and focus are investigated. A recurring alert that involves the same entity, the same rule scenario, and a related subset of transactions within a defined look-back period.

2.7. Integrated SAR Reporting

When a compliance analyst uncovers evidence of unusual activity during an investigation, they can seamlessly submit a Suspicious Activity Report (SAR) through Feedzai SAR Manager which is fully integrated with Feedzai Case Manager, allowing analysts to benefit from automated form submission and validation. Feedzai further empowers financial institutions by prioritizing alerts, allowing teams to focus on high-risk money laundering cases. Using AI, Feedzai dynamically learns and predicts which cases are likely to result in a SAR filing. For cases deemed low-risk, customizable workflows can automatically hibernate or send them for a lighter review, optimizing resource allocation.

> **Feedzai further empowers financial institutions by prioritizing alerts, allowing teams to focus on high-risk money laundering cases.**

Streamlining financial compliance analysis and reporting processes is critical to maintaining regulatory standards while improving operational efficiency. Feedzai increases efficiency from case management to SAR filing, handling 50 times more transactions and entities and enabling SAR filing up to 20 times faster. The SAR Manager tool simplifies the reporting process with automated activity capture, auto-validation and seamless filing across multiple jurisdictions, and integrates seamlessly with goAML.

In comparison, where it typically takes an average of 22 clicks to complete an online transaction, Feedzai reduces the number of clicks required to adjust thresholds or complete tasks to as few as 5. This significant reduction in complexity and time enables a more efficient and streamlined compliance workflow.

2.8. Link Analysis

Enabled by default in the Transfers channel, Feedzai Link Analysis, Genome, shows information in the event detail page and also opens the graph of the event in a new tab for more details, interaction and filters. Genome displays not only the relationships between customer and accounts but also and more importantly the money flow between them.

2.9. Insights

Feedzai Insights includes the following pre-integrated dashboards.

Business Overview

Provides an overview of the disposition process, the total number of alerts raised and their current status, how many alerts and cases by rule scenarios, among others.

The list of metrics is as follows:

- **Total Transactions:** Total amount and number of processed transactions.
- **Total Assessed:** Total number of assessed customers.
- **Total Alerts:** Total amount and number of alerted events.
- **Closed Alerts:** Total amount and number of closed alerts.
- **Total Cases:** Total amount and number of created cases.
- **Total SARs:** Total amount and number of SARs. Each SAR originates from a case closed with SAR.
- **Avg Amount by Alert:** The average amount and number of transactions that contributed to raise each alert.
- **Avg Alert Age:** The average time an alert is open before reaching the Closed status.

- **Avg Case Age:** The average time a case is open before reaching the Closed or Closed with SAR status.
- **Alerted:** The number of alerted events versus the number of alerted customers.
- **Alerts by Status:** The number of alerts by status versus the number of alerted customers by status.
- **Alerts closed with/without case:** The number of alerts versus the number of alerted customers, broken down by whether they lead to a case or not.
- **Alerts by Rule Scenario (Top 5):** The top 5 rule scenarios, showing the number of alerts and number of alerted customers for each scenario.
- **Cases by Status:** The number of cases by status.
- **Cases by Rule Scenario (Top 5):** The top 5 rule scenarios, showing the number of cases for each scenario.
- **Cases by Source:** The number of cases by source.

SAR Overview

Keep track of the exact number of ongoing, under approval and/or filed SARs. It is also possible to observe the number of cases that have been closed with SAR, and confirm the resolution time from filling out a SAR to obtaining the acknowledgement by the respective FIU.

The metrics are as follows:

- **Total SARs:** Total amount and number of SARs. Each SAR originates from a case closed with SAR.
- **Pending Approval:** Total amount and number of SARs in “Pending Approval” status.
- **Acknowledged:** Total amount and number of SARs in “Acknowledged” status.
- **Cases Closed w/ SAR:** Total number of cases that were closed with a SAR. The number of escalated cases does not increase if a case is closed with more than one SAR.
- **Avg Resolution Time:** The average resolution time from the creation of a SAR until its final status (“Acknowledged”).
- **SAR by Status:** The number of SARs by status.
- **Average Age by Status:** SAR average age breakdown by status.
- **Statuses Over Time:** The current number of SARs by status over a defined interval of time (e.g. every 12 hours). Select the legend icon to see the statuses and respective colors.
- **SARs by Case Source:** Displays which AML Transaction Monitoring’s Case Sources originated SARs and the number of SARs by Case Source.
- **Breakdown by Rule Scenario (Top 5):** The top 5 rule scenarios, showing the number of SAR for each scenario.
- **SARs by Maker:** The number of SARs attributed to each maker (i.e. the person who creates and fills out a SAR).
- **SARs by Checker:** The number of SARs attributed to each checker (i.e. the person who approves a SAR in Pending Approval status).

Analyst Performance

Two dashboards that regularly manage and measure the analysts' performance on an individual level, allowing MLROs to make decisions that enhance operational efficiency.

The metrics on Alert (L1 Analysts) decisions are:

- **Avg Resolution Time:** The average time an alert is open until reaching Closed status.
- **Avg Resolution Over Time:** The average time it takes to close alerts over a defined period.
- **Alerts by Status:** The current number of alerts in each status.
- **Avg Resolution Time by Analyst:** The average time in days each analyst takes to close an alert.
- **Avg Resolution Time per Day:** The average time it takes to close alerts on a daily basis.
- **Avg Resolution Time by Analyst per Day:** The average time each analyst takes to close alerts on a daily basis.
- **Alerts Closed with case vs. without case by Analyst:** The ratio (in percentage) of alerts closed "with case" versus alerts closed "without case" by each analyst.

The metrics on Case (L2 analysts) decisions are:

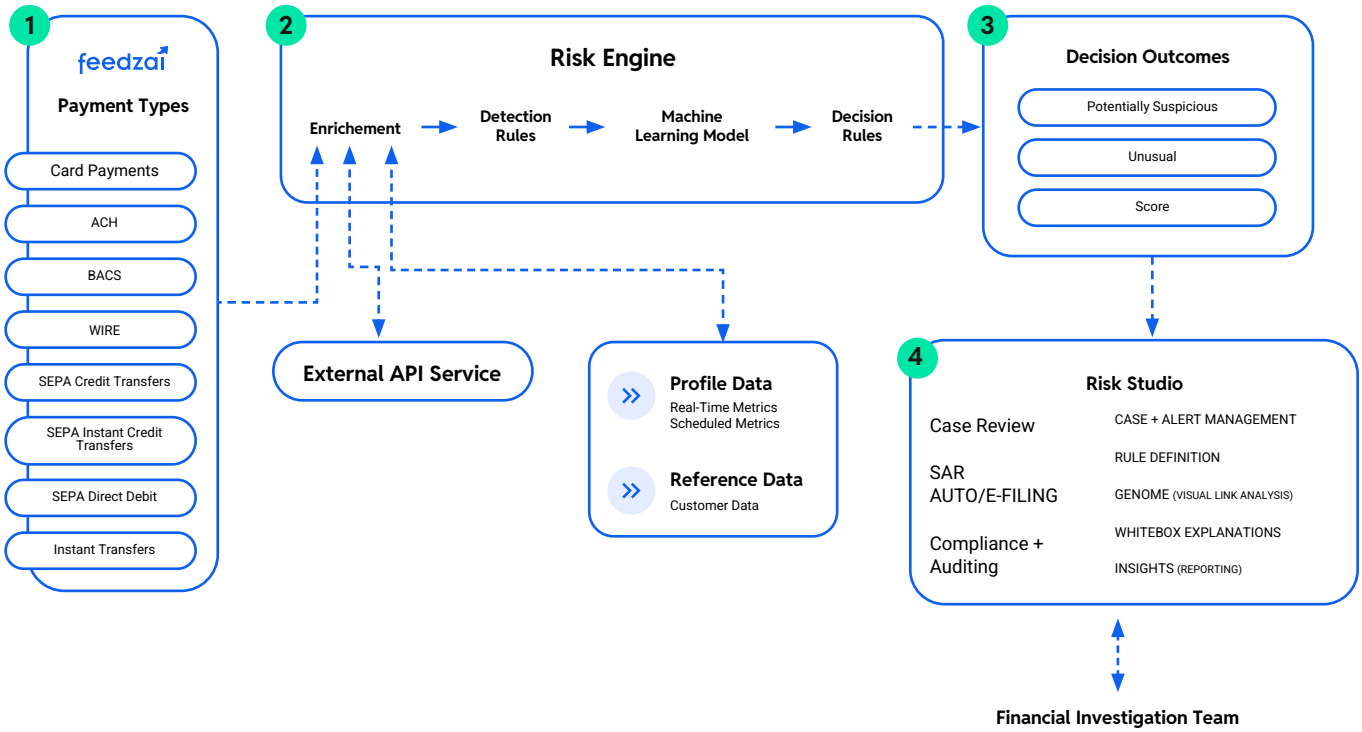
- **Avg Resolution Time:** The average time a case is open until reaching Closed status.
- **Avg Resolution Over Time:** The average time it takes to close cases over a defined period.
- **Cases by Status:** The current number of cases in each status.
- **Avg Resolution Time by Analyst:** The average time in days each analyst takes to close a case.
- **Avg Resolution Time per Day:** The average time it takes to close cases on a daily basis.
- **Avg Resolution Time by Analyst per Day:** The average time each analyst takes to close cases on a daily basis.
- **Cases Closed with SAR vs. without SAR by Analyst:** The ratio (in percentage) of cases closed “with SAR” versus cases closed “without SAR” by each analyst.

3. Automated Workflow

Feedzai's AML Transaction Monitoring delivers operational efficiencies by reducing false positives and increasing productivity by prioritizing high risk alerts. Feedzai uses transaction activity (e.g. card payments, money transfers, etc.), customer reference data, location data and more to detect long-tail patterns of anomalous behavior through profiling and alert on potential suspicious activity at the customer and account level. It uses customers' historical data to set a baseline for expected behaviors that will generate higher rates of productive alerts.

Detailed rule explanations provided at every alert helps compliance analysts understand the behaviors evaluated and why an alert was generated. It also helps auditors review the context for decisions and gives compliance officers relevant information to meet regulatory requirements.

3.1. Payment Types



Feedzai's Anti-Money Laundering (AML) solution includes support for the following payment types to monitor and detect suspicious activities across different financial transactions and schemas:

Card Payments
(Card Present and Card Not Present)
(ISO-8583 v3 compliant)

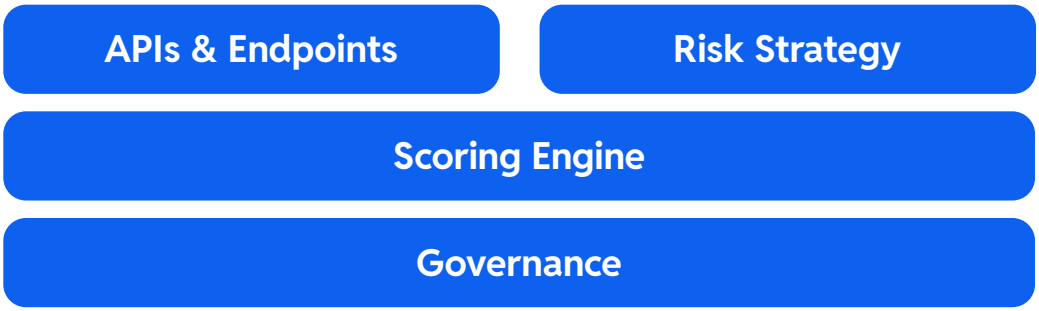
- Mastercard
- VISA
- AMEX
- Discover
- UnionPay

Transfers
(ISO-20022 Based)

- Automated Clearing House (ACH)
- Bankers Automated Clearing System (BACS)
- Wire Transfer (SWIFT; FEDWIRE)
- Single Euro Payments Area (SEPA):
  - Credit Transfer
  - Instant Credit Transfer
  - Direct Debit
- Faster Payments Service (FPS):
  - Single Immediate Payments
  - Forward-dated Payments
  - Standing Orders
- Boleto Bancario
- Pagamento instantâneo brasileiro (PIX)
- Zelle
- Real Time Payments The Clearing House
- Interac Email Money Transfers (EMT)
- New Payments Platform (NPP)
- Bill Payment (BPAY)

3.2. Risk Engine

At the heart of Feedzai is the patented Pulse Risk Engine—a powerful fusion of real-time event processing and a flexible data science toolkit. It supports the full machine learning lifecycle while making instant, high-volume decisions at low latency. Key capabilities include:



APIs & Endpoints

Feedzai's AML Transaction Monitoring solution uses transactional and reference data APIs to collect the necessary data for its workflows.

Payments APIs

These APIs are used to confirm the movement of funds, helping the Risk Engine detect suspicious activities. They use JSON RESTful API technology.

Cards (ISO-8583 v3 compliant)

Clearing (mandatory, non-scorable)
Clearing event which informs Feedzai when a card transaction is settled.

Transfers (ISO-20022 inspired)

Settlement (mandatory, non-scorable)
Settlement event which informs Feedzai when a transfer transaction is settled.

Reference Data API

The goal of the API is to ingest entity-level data into Feedzai to create the portfolio baseline for the periodic risk assessment of the solution. The integration technology is based on a JSON RESTful API and follows the CRUD approach (Create, Replace, Update, Delete).
An initial setup is required for first-time load before go-live and maintenance of reference data is achieved by consuming the endpoints mentioned below.

Account (optional)

Receive events to create, update, replace or delete account-level information associated with an account's IBAN.

Customer (optional)

Receive events to create, update, replace or delete customer-level information associated with a customer ID.

An entity subject to risk assessment in AML Transaction Monitoring is constructed by Customer, Account or a combination of both.

> **The goal of the API is to ingest entity-level data into Feedzai to create the portfolio baseline for the periodic risk assessment of the solution.**

Scoring Engine

Feedzai's Risk Engine, Pulse, is a high performance complex events streaming scoring engine.

Real-time or batch payments ingestion

It can process transactional data instantly via API or through scheduled batches.

Customer and account-level alerting

It identifies unusual behavior and alerts at the customer or account level, using both transaction and entity data.

Alert Optimization

The system reduces unnecessary alerts, ensuring analysts only see the most relevant ones for investigation.

Omni-channel

It monitors activity across all payment channels to detect suspicious behavior, allowing analysts to access data from various workflows.

Scheduled alerting

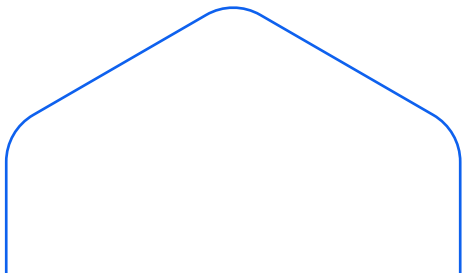
Alerts and risk assessments are generated on a set schedule (usually every 24 hours).

Scheduled baseline metrics

Regularly calculates metrics based on selected time windows and specific data groupings.

Entity-level aggregated metrics

Aggregates data at the entity level, such as daily transaction averages.



Risk Strategy

Feedzai's AML Transaction Monitoring includes the below pre-integrated capabilities and risk strategy.

Related Transactions

Automatically identifies and displays the specific transactions linked to each alert, making investigations easier.

Whitebox explanations

Human-readable explanations for why an incoming event has been assigned a particular Risk Score.

Dynamic thresholds

Allows flexible adjustment of detection settings by combining different entity attributes to create custom risk levels. These custom thresholds apply to existing rules based on attributes like "customer segment" and "account type."

Rules Tuning with Jupyter Notebooks

The process of rules is now semi-automated by using Jupyter notebooks. The following stepsare fully automated in a pre-packaged notebook:

- Replicate the solution workflow
- Run rule evaluations
- Generate a KPI report

AML Transaction Monitoring Rules Playbook

Standard rules designed to detect suspicious activity scenarios and meet compliance requirements from regulators. The package includes detection for the following money laundering typologies:

- **Transactions Involving High-risk counterparty**
  Incoming and outgoing transactions involving high-risk counterparties, which have a greater risk of exposure to illegal activity.

- **Transactions Involving High-risk and Very High-risk customers**
  Incoming and outgoing transactions involving customers included in high-risk and very high-risk customer watchlists. Such lists contain PEPs, customers previously linked to money laundering schemes, customers linked to high-risk countries/business sectors, or customers under surveillance by law enforcement.

- **IP monitoring**
  Unusual usage of IP addresses by a customer, such as a high number of distinct IP addresses or IP locations as well as significant amounts transacted from IP addresses in high-risk geographies. This could be interpreted as a sign of account takeover or shared usage of an account for money laundering purposes

- **Significant Change from Previous Average Activity**
  Sudden changes in transaction activity and targets accounts with a volatile historical behavior.

- **High-risk and Very High-risk Geography Activity**
  Transactions made to, from or through a high-risk or very high-risk geography, by leveraging watchlists. High-risk and very high-risk geographies have poor regulations and a greater prevalence of financial crime.

- **Rapid movement of funds**
  Rapid movements of funds in and out of customer accounts, namely when similar aggregated amounts enter and leave one account in a short period of time, which often suggests complex financial transactions intended to conceal the origin of the illegal proceeds.

- **Structured activity**
  Occurrence of repetitive patterns or a high percentage of transactions in the same amount or similar amount may be unusual activity for the account or customer.

- **Transactions in Round amounts**
  Round-amount transactions at account level, as defined by the number of trailing zeros in the amount field (e.g. USD 1,000.00). Since most transactions are purpose-specific and in varying amounts, a significant percentage of transactions in round amounts could be a sign of money laundering and structuring of funds.

- **Activity in Dormant Account**
  Unexpected activity in idle accounts, namely, a significant withdrawal of funds.

- **Large Significant Transactions**
  Customers that have performed one or more transactions (such as cash withdrawals and/or deposits) that amount to a large aggregated sum

- **Reportable transactions**
  Transacted amounts that exceed a predefined threshold, as required from financial institutions to report.

- **Avoidance of Reporting Thresholds**
  Structuring activities designed to avoid reporting thresholds.

- **Anomalies in ATM, Bank Card - Foreign Transactions**
  Abnormal usage of cards and ATMs in foreign countries because cards can be easily used at ATMs to transfer assets to other individuals or locations due to the anonymity granted to ATM users.

- **Suspicious Keyword**
  Transactions that contain blacklisted keywords in free text fields of the transaction data. Certain words may be considered suspicious (i.e. blacklisted) in the context of financial activity.

- **Multiple originators to single beneficiary**
  Transactions that have different points of origin (originators) but a single beneficiary. Transactions that have different points of origin and a single beneficiary might flag an account created for the purpose of receiving illicit funds (e.g. the beneficiary account working as a mule account).

- **Single originator to multiple beneficiaries**
  Transactions with the same point of origin and sent to multiple different accounts (multiple beneficiaries) suggest dispersion to hide the origin of funds and create complex layers.

- **Excessive Aggregated Cash Withdrawals and Advances**
  Cash withdrawals from an account that are higher than or equal to a set percentage of the account's cash advance balance and higher than or equal to a certain amount threshold.

- **High-risk Merchant Monitoring**
  Payments and refunds between customers and high-risk merchants, as defined by the type of business they conduct. High-risk merchants offer products or services vulnerable to illegal activity, and are less likely to conduct any verification or identification on a client. This facilitates frequent and/or high-value transactions.

- **Excessive aggregated cash withdrawals**
  Incoming/outgoing movements of funds trying to break the audit trail.

- **Multiple Geography payments**
  Unusual activity that may indicate geographic dispersion of funds.

Machine Learning models

These models are trained to score customer assessments using high-quality historical client data. Creating and training these models requires customized effort for each project.

Governance

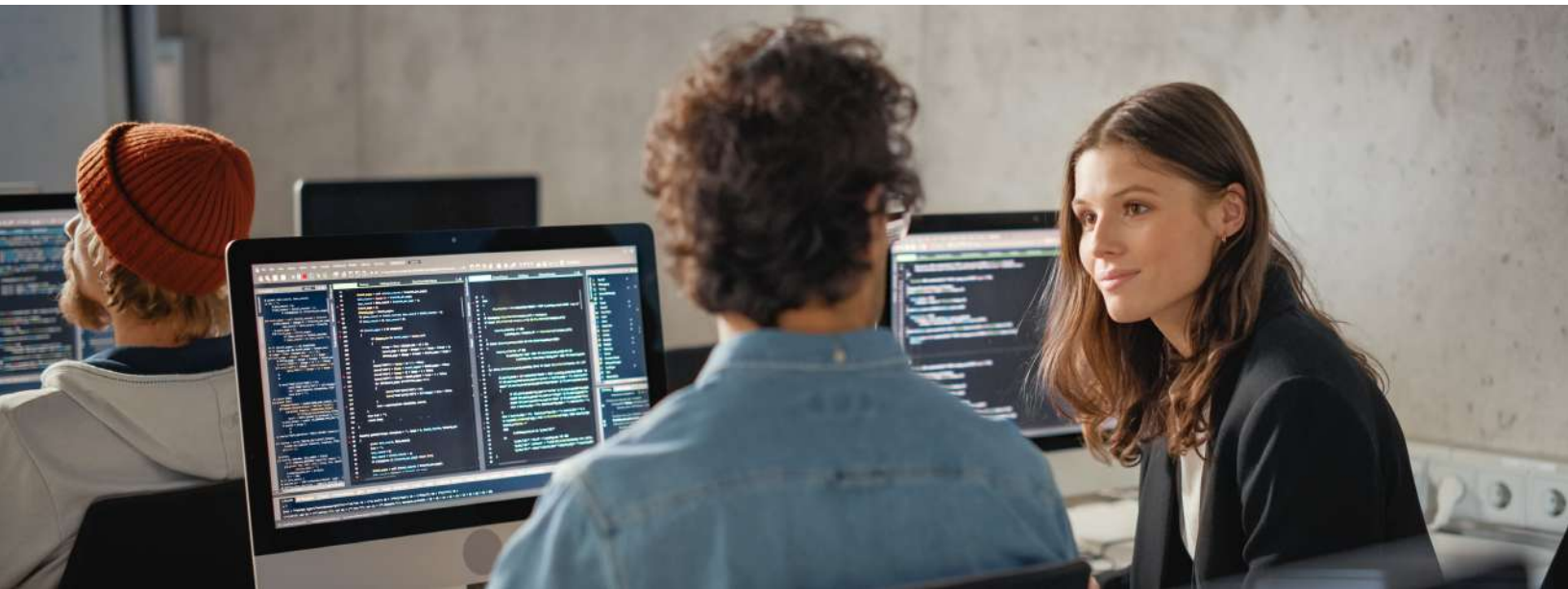
Feedzai's AML TM meets flexibility with governance capabilities to support the evolution of the risk strategies and audit needs.

Cards (ISO-8583 v3 compliant)

Auditability
Automatically generates audit trail logs for all operations executed within the Risk Engine.

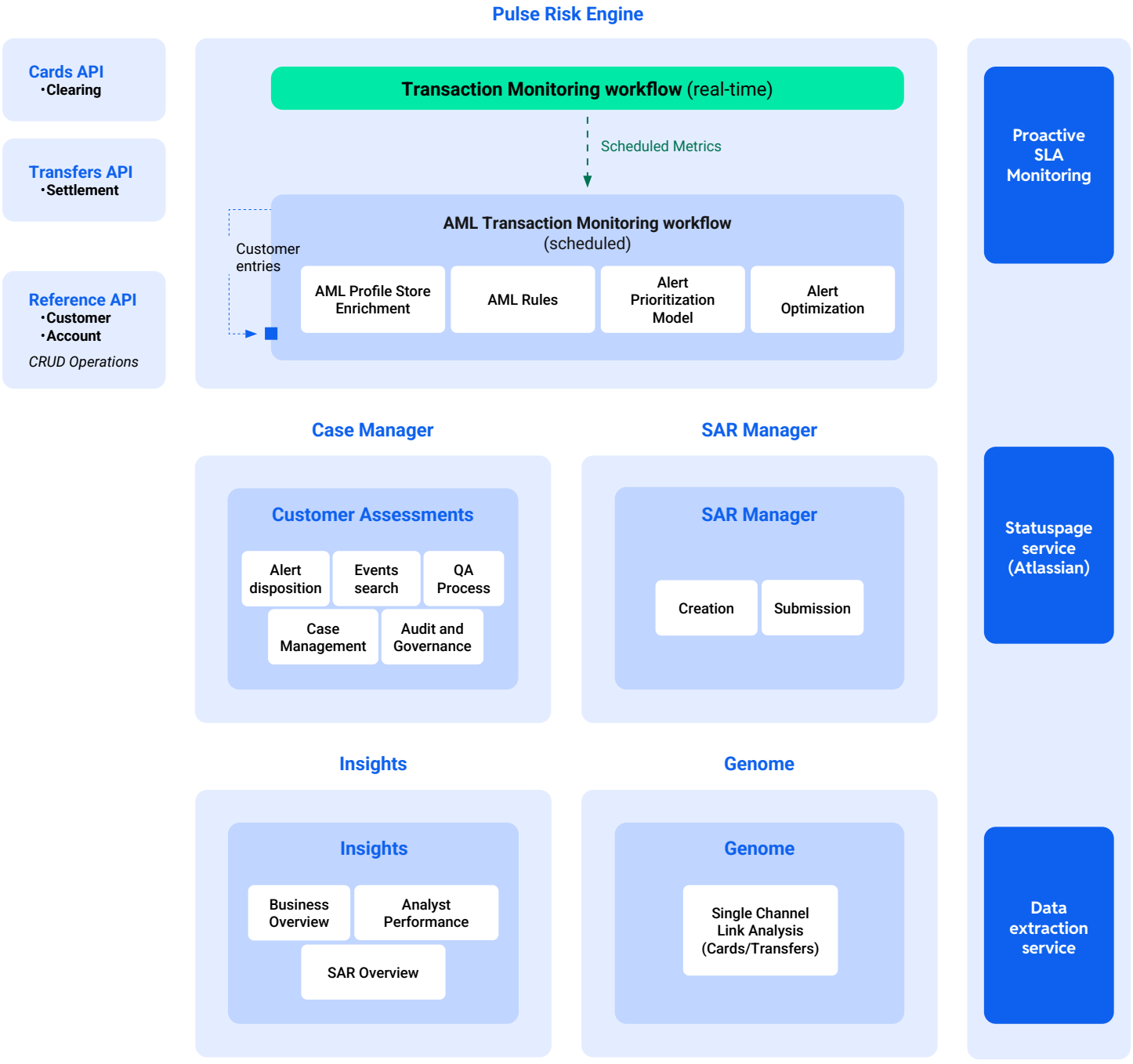
Transfers (ISO-20022 inspired)

4-eyes check
Any change made on the rules risk strategy needs to be validated by another authorized user before the changes are published to the runtime environment (lists management excluded).



3.3. Risk Studio

At the heart of Feedzai is the patented Pulse Risk Engine—a powerful fusion of real-time event processing and a flexible data science toolkit. It supports the full machine learning lifecycle while making instant, high-volume decisions at low latency. Key capabilities include:



Case Manager

Case Manager helps users become more efficient and effective at fighting financial crime through the following capabilities and pre-configurations.

- **Customer/Account-level alerts**
  Displays alerts with relevant customer and account details, rule explanations, and transaction history. It also includes the ability to filter transactions that triggered the alerts using the Related Transactions feature.

- **Case/Alert Investigation**
  Set of tools and functionalities to enable risk analysts to effectively review and act on alerts and/or cases. Moreover, once alerts are promoted to a case, and the investigation results in confirmed suspicious behavior, the case can then be promoted to a Suspicious Activity Report (SAR).

- **Entity page**
  Customer's historical information such as the customer portfolio, transactional trends and behavior fostering a better understanding of what is usual customer behavior, and easily detect any suspicious deviations.

- **Omnichannel**
  Risk analysts have access to a unified view of customer activity across channels, helping them assess risk holistically. Supports different event schemas, multiple outcomes, and multiple risk workflows to expose historical data and potential risky situations across multiple channels. Role-based access control can be set up allowing different data segregation policies at individual, team and channel level. Included channels:

  - **Customer Assessment:** a channel where entity-centric risk assessments are located to facilitate alert disposition and review.
  - **Cards:** the cards channel where card present and card not present transactions are persisted, as a baseline for the customer risk assessments.
  - **Transfers:** the transfers channel where transfer transactions are persisted, as a baseline for the customer risk assessments.

FRAML-enabled, Feedzai's Riskops Platform seamlessly combines fraud and anti-money laundering (AML) in a single system. It integrates fraud detection with AML transaction monitoring, providing a complete view of customer risk and improving overall risk assessment, all controlled by strict user access controls.

Key benefits include reduced investigation time through auto-fill capabilities, unified fraud data streams for earlier and more accurate detection, and improved decision making through machine learning and rules that consider behavior throughout the fraud lifecycle.

In addition, visual link analysis and cross-organizational data visualization enable better investigations, helping to detect and prevent fraud before it causes significant damage.

> **Feedzai's RiskOps Platform seamlessly combines fraud and anti-money laundering (AML) in a single system.**

Alerts

- **Alert list screen:** Lists will have the most important alert fields to be displayed for an initial assessment (e.g. timestamp, customer, outcome suggestion).

- **Alert investigation screen:** A one-page interface that presents the most relevant data and actions needed to investigate and resolve alerts. It contains the following data structures:

    - **Alert-level information,** namely the status, reason codes applied, assigned queue, assigned analyst and linked cases (when applicable).
    - **Entity-level information,** (eg, customer, account).
    - **Risk assessment details** such as whitebox explanations and outcomes including associated suspicious transactions.
    - **Transaction history,** using predefined entity fields and timeframe the user can quickly put the alert into context by linking past events to the corresponding entity. The following for transaction are available:
      - Originator, Beneficiary, Transaction type and subtype and Counterparty Country.
    - **Related transactions,** this enables analysts to filter out by Risk Scenario which were the transactions that contributed to trigger an alert.
    - **SAR history,** containing previous filled SARs for the current alerted entity.
    - **Activity log,** contains the audit trail of all actions taken by the user or the system from the moment an event is sent to Feedzai Case Manager.

- Furthermore, a subset of the following actions is available:

    - **Alert decisioning -** ability to tag an alert as suspicious / not suspicious and broadcast the same decision to other unreviewed alerts based on specific criteria.
    - **Assign alert to user -** own user or other
    - **Add note to alert -** ability to add plain text notes and attach to the alert being investigated.
    - Move alert to queue.
    - **Update lists -** ability to add, change or remove entities present in the alert to the configured lists in the system.
    - **Update reasons on alert -** add or amend reason categories into the alert upon investigation.
    - **Link alert to case -** ability to link the alert to an existing case or new one.

Customer page

This page is the centralization of all info about a given customer, insights for its transactional patterns, customer demographics and more.

Users will have available to the following info:

- **Header -** displays general information about the customer such as risk rating, name, and total balance
- **Customer Insights -** the customer's historical transactional information regarding a specific timeframe.
- **Customer Details -** general information about the customer, such as location, contact, and business-related details.
- **Customer Portfolio -** the different cards and accounts associated with the customer.
- **Transaction History -** the transactions involving the customer.
- **SAR history -** previous filled SARs for the customer.
- **Notes -** the existing notes regarding a customer.
- **Attached Files -** allows users to Upload, Download, Update or Delete files.
- **Activity Log -** actions performed in the customer page, namely regarding attached files, notes, and updates to lists.

Cases

Case list screen
shows cases that users have created or that were automatically generated, however automatic cases aren't part of the default setup. These cases are assigned to queues that the user is part of.

Case investigation screen
Investigation screen dedicated to display in a one-page design the most relevant data and actions for case investigation and resolution. Users will have available to the following data structures:

- **Case-level information,** namely the status, assigned queue, assigned analyst and description.
- **Transaction-level information,** with the details of the case linked events.
- **Attached files information,** containing the details of the files attached to the case.
- **Activity log,** contains the audit trail of all actions taken by the user or the system from the moment a case is generated.

Furthermore, there is a subset of following actions available in the screen:

- **Case decisioning -** ability to tag a case as to be reviewed / In analysis / Waiting for info / Closed (plus ability to attach closure note).
- **Assign case to user -** own user or other.
- **Add note to case -** ability to add plain text notes and attach to the alert being investigated.
- **Move the case to the queue.**
- **Update reasons on alert -** add or amend reason categories into the alert upon investigation.
- **Download case details -** ability to download the case details to PDF.
- Promote to SAR.

Cascading Case decision
When an L2 Analyst makes a decision on a case, that decision automatically applies to all related events. For example, if the analyst decides to "Close as Suspicious," all linked events will also be marked as "Closed" and "Suspicious" without needing any extra steps.

Search & Self-serviceability

Feedzai's Risk Engine, Pulse, is a high performance complex events streaming scoring engine.

Alert search screen

It can process transactional data instantly via API or through scheduled batches.

Transactions Search

It identifies unusual behavior and alerts at the customer or account level, using both transaction and entity data.

Case search screen

The system reduces unnecessary alerts, ensuring analysts only see the most relevant ones for investigation.

Manage Details page

Analysts spend most of their time reviewing alerts, cases, or customers. However, the out-of-the-box interface configuration of these pages doesn't always match the processes used by each financial institution which leads to analysts spending more time to make a decision.

To help managers optimize their team's workflow, Case Manager allows them to edit the configuration of the Details pages. For example, managers may want to adjust a field's naming to ensure that all analysts work with company-compliant terminology, or change the order in which the fields are displayed.

Alert search screen

It can process transactional data instantly via API or through scheduled batches.

Transactions Search

It identifies unusual behavior and alerts at the customer or account level, using both transaction and entity data.

Governance

- **Customer re-monitoring**
  After a SAR is filed the investigated subjects (customers of the FI) enters a 90-day re-monitoring period, this means that every alerted activity will be compiled in a case and then when the monitoring is over, the case is sent for the disposition period where an analyst must be decide if a Continuous Activity Report needs to filled.

- **Assign and lock**
  When assigning an alert, there is an option to assign all alerts on the same customer so that the analyst can investigate all the pending alerts related to a customer, and consequently have a more complete knowledge of a customer's activity and behavior.

- **Queue optimization and routing**
  Queues can be configured to reflect different priorities to organize events/alerts, cases, and assignment to team members based on the payload attributes.

- **Process automation:**
  The following automations are available to configure the alert governance model:

  - **Queues:** Logical element where alerts and cases can be sent to queues depending on review state or alert/case severity. Queues can be alert-centric or case-centric. Users or groups of users can be assigned to specific queues. Queues can also be configured to be tenant aware - queues specific for each tenant, if multi-tenant capability is being used.
  - **Automatic case creation:** Generate a case when an alert arrives upon defined conditions, as well as the ability to associate that case and other related events that arrive within a configurable time range. The cases can also be manually created by the user (e.g., when closing an alert as suspicious).
  - **SLA Rules:** Configure time-box windows for alerts and cases, for when there is a breach, an action can be taken. (e.g. unreviewed case or alert can be migrated automatically into a high priority queue).
  - **Automation Rules**: Configure specific conditions for alerts and cases that will trigger an action. (e.g. Input: Event Arrives; Condition: Score > 800. Action: Auto-Deny the event.).

- **Roles & permissions:**
  Configurable role-based access control of a user-role for the Case Manager, that allows permissions to be assigned accordingly.

  Standard roles & permissions are:

  - **L1 Analysts:** Access to the L1 queue and its actions
  - **L2 Analysts:**
    - Access to the L1/L2 queues and their actions.
    - Complex investigations and decisions on Alerts
    - Work with cases and Genome
    - Maker in SAR Manager (i.e. create, request approval, and submit SARs to the FIU, and finally confirm FIU's acknowledgement).
  - **QA Analysts:** Review assessments after they've passed through theL1/L2 Analyst workflow.
  - **Managers:**
    - Take action on events and cases.
    - Access to dashboards and reports.
    - Perform analyst management operations, such as managing queues and SLAs.
    - Maintain rules, lists, thresholds in Pulse and Case Manager.
    - If four eye-checks are enabled, submit rules for review.
  - **MLROs**
    - Access to L1 and L2 Analyst actions.
    - Access to dashboards and reports
    - Checker in SAR Manager, i.e. review and confirm SAR is ready to be submitted to the FIU (i.e. SAR approval).
  - **Integrator**
    - Create and manage JWK keys.
    - Read-only access to Pulse user list (accessible via Pulse base URL - /pulseviews/management/#admin/security).
    - Read-only access to Pulse workflows
  - **Auditability:** Audit trail for every action done at alert or case level such as alert creation, assign to user, moving alerts between queues, added notes and/or documents and review outcome.

Want to learn more?

Reach out to your Feedzai representative

Request a demo

feedzai

sales@feedzai.com info@feedzai.com feedzai.com