Jumio Transaction Monitoring uses cutting-edge technology to help you comply with anti-money laundering regulations. Let’s take a closer look at how Jumio Transaction Monitoring detects suspicious activity and ensures peak performance.

**Flexible Data Ingestion**

Data from various source systems can be fed into Jumio Transaction Monitoring via our library of RESTful APIs. Our standard data model simplifies data mapping, but we also have the flexibility to accept any custom data fields you want to send. These custom fields can then be used as part of the detection rules and for display as part of the case during the investigation process. Additionally, one of our core competencies is using external data sources to supplement both the detection of suspicious activity and the analyst’s investigation process. We can accept any type of JSON payload.

**Powerful Rules Library**

Jumio Transaction Monitoring utilizes a library of rules to detect suspicious activity. The out-of-the-box rules are based on common AML typologies, industry best practices and our internal compliance expertise. You can modify these rules, adjust parameters and thresholds as needed, and build your own custom rules to meet your specific requirements. During detection, these rules are run on the transactions, customers, accounts, users and other data sources that are fed into the Jumio system, and any hits result in the creation of a case, which can cover categories such as money laundering, KYC, sanctions screening, fraud and surveillance.

Each generated case also includes labels that indicate what issues were identified by the rules during detection. Our in-house data science team provides assistance with writing your rules based on specific requirements and leveraging our machine learning capability to improve the detection performance over time (tuning).
Data Aggregation for Advanced Detection

Transaction Monitoring can operate in both batch and real-time capacities. Most transaction monitoring rules look at patterns and trends over time; they are rarely used to stop a transaction in real time due to suspicion of money laundering.

Jumio Transaction Monitoring aggregates your data to identify patterns and trends and enable more advanced suspicious activity detection. It can also identify duplicates based on data points that you specify and handle them according to your use cases. For example, if you specify that an SSN field should be de-duped, we can treat multiple counterparty records with the same SSN as the same entity.

Rule Tuning Guided by Machine Learning

Performance dashboards let you evaluate each rule’s performance based on how the resulting cases were resolved and then adjust and tune them to maximize their performance. Our data science team leverages our platform’s machine learning capability to proactively identify ways to improve the rules’ detection performance. For example, it may identify that changing a threshold or adding another data point may reduce false positives without sacrificing any cases that led to a regulatory filing. Compliance teams have full control over whether these suggested changes are implemented.