Jumio Transaction Monitoring provides public REST APIs that enable developers to programmatically send data to Jumio, create and retrieve objects in the Jumio Investigation Manager and subscribe to notifications through webhooks. The APIs all use OAuth 2.0 to secure access, and they send requests securely via SSL through a proxy URL to the internal services.

### Sending Data to Jumio

To begin using Jumio Transaction Monitoring, you send your data to the Jumio platform using the Data Ingestion API. This API lets you integrate your data with Jumio so you can process entities like transactions, parties and accounts. You can then detect suspicious activity, screen customers against watchlists and verify their identities and investigate related data. When you call the API, you supply the IDs that the API uses to update existing data objects and to create new ones.

### Creating and Retrieving Objects in the Jumio Investigation Manager

When the detection engine spots scenarios that need further review, such as suspicious activity, parties requiring identity verification or parties with watchlist matches, it creates cases. Analysts then use the Jumio Investigation Manager to investigate and manage those cases. Developers can use the Investigator API to programmatically retrieve cases, upload documents and create cases from an external system such as Salesforce if needed.

### Subscribing to Notifications

Jumio generates notifications for key events, such as when a transaction or party exceeds a certain threshold. You can subscribe to these notifications using the Webhooks API so that you can integrate them with a separate workflow in an external system. For example, if you want to be notified immediately if one of your customers violates an implemented policy, you could subscribe to the alert.created notification and write logic in your system to temporarily lock that user’s account.