PayPal Risk APIs

Payment Assessment API
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Benefits</td>
<td>4</td>
</tr>
<tr>
<td>Integration Details and Outcome</td>
<td>7</td>
</tr>
<tr>
<td>Sample Use Case</td>
<td>11</td>
</tr>
<tr>
<td>Limitations</td>
<td>12</td>
</tr>
<tr>
<td>Frequently Asked Questions</td>
<td>13</td>
</tr>
</tbody>
</table>
Overview

PayPal Payment Assessment API helps enable merchants to assess the risk of a credit card before approving it. The easy to integrate API leverages the PayPal 2-Sided Network of over 25 million merchants and 330 million active accounts transacting over 12 billion times each year to provide merchants with enhanced information to identify high risk transactions.

Payment Assessment API evaluates the risk level of each payment in real-time using hundreds of signals specific to that payment. Then, using a combination of historic events as well as device and IP information, the API derives a risk score for that payment ranging from 0–1000, where higher the number, higher the risk. The score, along with corresponding reason code(s) and explanation, helps merchants assess the risk level for that payment.

The API is targeted towards merchants and marketplaces that are looking to integrate a reliable payment fraud management provider’s scores into their existing internal tools, instead of buying a new fraud management solution.

Payment Assessment API’s use of information is compliant with global standards such as GDPR and PSD2.
Benefits

Payment Assessment API seamlessly integrates with merchant’s existing fraud prevention services or solutions and helps provide immediate input to support risk decisioning based on patterns gathered from device and IP data as well as historical activity within PayPal.

Here are the key benefits of the Payment Assessment API:

**Reduced Declines and Chargebacks** – The success of a risk model ultimately depends on its ability to detect fraudulent transactions while maintaining a low decline rate. The PayPal risk model helps merchants detect potentially fraudulent transactions before they are processed, helping to minimize the number of chargebacks and declines.

The chart below shows stellar performance results where the Payment Assessment API has lower decline and chargeback rates in comparison to those of a competitor:

<table>
<thead>
<tr>
<th></th>
<th>Decline rate</th>
<th>Chargeback rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incumbent</td>
<td>0.2%</td>
<td>0.4%</td>
</tr>
<tr>
<td>Risk APIs</td>
<td>0.05% - 0.15%</td>
<td>0.2% - 0.3%</td>
</tr>
</tbody>
</table>

Results specific to select merchants. Results may vary.
**Increased Merchant Confidence** – The API helps minimize false positives, lower customer friction, avoid authorization, reversal, or refund fees, and reduce chargebacks by empowering merchants with enhanced intelligence regarding the risk involved with a specific transaction before they process it. As a result, the merchant can minimize risk and authorize the transaction with confidence.

**Eliminates Need for Advanced Data Training** – The underlying machine learning model is trained on the PayPal and Braintree network of merchants. Data from the payment being assessed and the risk profile of similar payments processed from other merchants in the network are used to generate the score and reason for each payment. This results in the API returning accurate scores for newly onboarded merchants and marketplaces without additional training, whereas competitors who require six months of data beforehand for model training.

**Enhanced Fraud Predictability** – Data from the PayPal 2-Sided Network as well as machine learning models and rules power the API and help predict whether a transaction might be fraudulent and likely to result in a dispute. The resulting risk score helps guide merchants in deciding on a course of action for potential fraudulent transactions.

**Notes**
- Even if the API returns a positive risk evaluation, a customer’s issuing bank may still decline the transaction.
- As the service does not provide chargeback protection, the merchant is responsible for chargebacks.
Seamless Integration – The easy-to-use REST API integrates seamlessly with both websites and mobile applications with a few lines of code. It is accompanied with comprehensive documentation that helps merchants evaluate the risk associated with each payment before authorizing it.
Integration Details and Outcome

Payment Assessment API helps the merchants evaluate any potential risk associated with a payment before approving it.

The merchant calls the API before authorizing a credit or debit transaction with their issuing bank. The API evaluates the transaction using various data points and provides the merchant with a risk score for that transaction. The risk score as well as the reason code(s) and explanation help the merchant assess the risk and decide if they should approve or reject the transaction.

Here’s a summary of the process involved in the API deriving the risk score:

1. Assess Comprehensive PayPal Data – The PayPal network processes tens of billions of events per year and collects customer and transaction information as well as device information and connection data, which is leveraged via the
PayPal Risk Data Acquisition (RDA) service through use of Java Scripts and SDKs embedded in all merchant web and mobile applications.

Payment Assessment API uses the different types of data collected, as shown below, to conduct risk assessment on a transaction.

<table>
<thead>
<tr>
<th>Customer Data</th>
<th>Event Related Data</th>
<th>Connection Data</th>
<th>Device Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Transaction Amount</td>
<td>IP</td>
<td>Operating System</td>
</tr>
<tr>
<td>Address</td>
<td>Shipping Address</td>
<td>Cookie</td>
<td>Device Model</td>
</tr>
<tr>
<td>Account Age</td>
<td>Merchandise Vertical</td>
<td>FSO</td>
<td>Screen Resolution</td>
</tr>
<tr>
<td>Financial Instruments</td>
<td></td>
<td>TCP/IP Packet</td>
<td>And more...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>

PayPal Risk excels in using all available data.

2. **Evaluate Data Using Rules and ML Models** - The API processes, analyzes, and runs the collected data against a large set of rules and machine learning models. The rules and ML models assess the risk of a transaction by evaluating data points such as frequency of use, distance travelled/time calculations since last event, device OS and settings, IP risk as well as the type of transactions, MCC code, history of the customer including any previous risky events, chargebacks, and more.

**Note** - There is no model governance or other types of details delivered with the API.
3. **Generate Risk Score** - After the detailed evaluation, the API produces a risk score of the transaction for the merchant. The score, ranging from 0–1000, is accompanied with one or more reason codes and corresponding explanations, and is intended to help the merchant in deciding if they should authorize the transaction with their issuing bank.

Below are the details for the risk score:

<table>
<thead>
<tr>
<th>Band</th>
<th>Score Range</th>
<th>Suggested Reason Code</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED</td>
<td>999</td>
<td>HIGH_UNAUTHORIZED_RISK</td>
<td>Transaction is declined. Client cannot approve.</td>
</tr>
<tr>
<td></td>
<td>UNUSUAL_ENTITY</td>
<td>UNUSUAL_ENTITY_DEVICE_RISK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UNUSUAL_ACCOUNT_ENTITIES</td>
<td>HIGH_VELOCITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HIGH_RISK_CONNECTION</td>
<td>NEGATIVE_HISTORY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HIGH_RISK_LINKING</td>
<td>HIGH_RISK_GENERIC</td>
<td></td>
</tr>
<tr>
<td>YELLOW</td>
<td>600-999</td>
<td>UNUSUAL_ENTITY_DEVICE_RISK</td>
<td>Client should consider declining the transaction unless their profit margin allow for high likelihood of loss</td>
</tr>
<tr>
<td>GREEN</td>
<td>000-599</td>
<td>LOW_MERCHANDISE_RISK</td>
<td>Client should consider approving the transaction</td>
</tr>
</tbody>
</table>

API Score Index
4. **Enhance PayPal’s Fraud Detection Model** - In an effort to optimize the fraud detection model, PayPal continuously updates its historical data and collects new transaction data. PayPal requests that merchants notify them of the outcome of a transaction so that they can compare their prediction about a transaction to the actual outcome of that transaction and update the risk model based on those learnings.

This is mutually beneficial to the merchants and PayPal as:

- Merchants depend on the performance of the PayPal risk models to help reduce chargebacks and declines.
- PayPal can continuously enhance and optimize its risk models based on feedback data from the merchant.

Once the merchant authorizes a payment with its card processors, they can call the Lifecycle Event API to notify PayPal of the final outcome of the transaction. The API enables the merchant to share data for the following events:

- **Payments complete** – Informs PayPal of the final outcome of the transaction. For every transaction, be it successful, voided, refunded, etc., PayPal expects a notification in order to compare the final outcome to what it originally predicted for that transaction. The payment complete notification, regardless of the result, also helps PayPal avoid incorrect assumptions, such as in the case of a transaction that was refunded (no chargeback issued) and PayPal incorrectly marking it as successful.

- **Chargeback** – Notifies PayPal whether the merchant received a chargeback or not, with the corresponding reason.
Sample Use Case

The typical use case for Payment Assessment API is “card not present” transaction fraud. As every transaction is either an online purchase or a product/service query, the device/IP information that is collected is instrumental in helping to determine the overall risk of a transaction.

In internal testing, the API has shown to help provide valuable lift in identifying fraudulent transactions, which could be a result of stolen credentials, stolen credit cards, card testing, and many other fraudulent acts. It also provides an overall trend for the user based on historical events.
Limitations

Payment Assessment API is a comprehensive approach to help merchants evaluate each transaction that is being processed via a risk score. The score is derived, in part, by leveraging and evaluating a large repository of users and merchants within the global PayPal network.

Although this footprint is extensive, many consumers do not use a PayPal product. This results in Payment Assessment API being beneficial to merchants processing transactions through PayPal or Braintree.

Here are the limitations based on the current capabilities of Payment Assessment API:

- Although the API generates a risk score with a corresponding reason code and explanation, no additional attributes are provided.
- The library of payment activity is limited to the global PayPal network.
- The service cannot be enabled for historic data and/or non-API (Bulk) loads.
- The merchants must share user identity and device/IP information with PayPal to use the API.
Frequently Asked Questions

What is PayPal Payment Assessment API?
PayPal Payment Assessment API helps merchants evaluate the potential risk associated with a transaction before accepting it. The API assesses each payment’s risk in real-time using hundreds of signals for the payment and leverages data from the PayPal 2-Sided Network of merchants and customers to help predict the likelihood of a payment being fraudulent.

What are the data sources?
The API leverages information from the PayPal network of over 350 million active accounts which includes over 25 million active merchants.

What payment methods can PayPal Assessment API evaluate?
The API is designed to help detect fraud related to “card not present” (CNP) transactions.

When should the merchants call the API?
Merchants should call the API before they authorize a credit or debit transaction from their issuing bank. They can be selective on the conditions, such as amount and geographic location, when calling the API.
What does the API return?
The API returns a risk score and associated reason code(s). The score ranges from 0-1000 (the higher the score, the riskier the transaction).

What action can a merchant take with the risk score and reason code?
Based on the returned values, a merchant can choose to reject the transaction or move forward with the payment authorization with the issuing bank. Merchants can also use this information to create user profiles on their system.

How much integration is required?
The simple REST API can be integrated using a few lines of code and is accompanied with comprehensive documentation that helps merchants evaluate the risk associated with each payment before authorizing it. Additionally, the merchants will need to integrate with two REST APIs – Payment Evaluation API and Lifecycle Event API – as well as one device data collector – Magnes for web apps and Fraudnet for mobile apps.

Does the API need device fingerprinting?
Yes, merchants must integrate with the PayPal device fingerprinting service (Magnes for web apps and Fraudnet for mobile apps) for the API to work.
About PayPal

PayPal has remained at the forefront of the digital payment revolution for more than 20 years. By leveraging technology to make financial services and commerce more convenient, affordable, and secure, the PayPal platform is empowering more than 330 million consumers and merchants in more than 200 markets to join and thrive in the global economy.