outpayce from amadeus

PAYMENTS SECURITY
FRAUD MANAGEMENT SERVICES (RESELLER)

1. Description

1.1 This solution provides the functionalities to support fraud screening services provided by Customer Selected Provider (CyberSource) to Customer, for payment transactions processed through our Payment Platform.

1.2 This solution is an add-on to our Fraud Screening solution.

1.3 This solution enables Customer to submit in real-time, via its front end a fraud screening request to Customer Selected Provider.

2. How does this solution work?

2.1 Customer Selected Provider (CyberSource) allocates a fraud consultant who will configure and review the Business Rules previously established by Customer on a timely basis depending on the level of the service.

3. Key features

3.1 For PNR integration transactions, the result of the fraud screening request is automatically added to the PNR, and the sales reporting is enriched with the corresponding payment transaction details.

3.2 Customer Selected Provider (CyberSource) will provide two (2) training sessions (Jump Start) to Customer.

4. Services

4.1 This solution is available at three different levels, Gold, Platinum and Screening management.

4.2 The key features of each level are the following:

Service / Level	Gold	Platinum	Screening management
Access to the managed services team for consultation	Monday to Friday from 09:00 to 17:30 GMT, except public holidays		
Screeninig management	×	×	24 hours a day, 7 days a week
Confer with Customer to review the performance of Decision Manager, specifically payment transaction acceptance or rejections, reviewed payment transactions, chargebacks and Customer's fraud specifics	On a monthly basis		
Consult with Customer for for the purpose of testing and providing fraud strategy configuration updates to Decision Manager rules, transaction profiles, including tuning for situational, seasonal, and product-related screening	On as a needed basis	On as a needed basis Customer Selected Provider will make good faith efforts (no obligation) to update Customer prior to such changes	
Business reviews to include benchmark data related to payment transaction acceptance and rejection rates, review rates, and high level chargeback metrics if applicable. Quarterly chargeback analysis and rule tuning exercise as applicable	×	On a quartlery basis	
Monitor Customer's transactions submitted to Decision Manager in regard to acceptance, review and chargeback rates relative to the transaction profiles	✓	×	×
Provide reports and analysis of the performance of the solution, specifically payment transaction acceptance or rejections and reviewed payment transactions	✓	×	×

Service / Level	Gold	Platinum	Screening management
Meetings with Customer to review the performance of the solution	✓	×	×
Review payment transactions flagged by Decision Manager as requiring further review and either clear such transactions for further processing or reject them within 24 hours of receipt through Decision Manager (excluding those identified as priority transactions) at a 98% pachievement rate	×	×	✓

5. Customer's obligations

5.1 General obligations.

5.1.1 Customer must use the Decision Manager in conformance with the "Decision Manager Developers Guide" and "Decision Manager User Guide".

5.1.2 For each transaction submitted to Decision Manager, Customer must provide to Customer Selected Provider (CyberSource) with all information necessary to process and review the transaction.

5.1.3 Customer must provide to Customer Selected Provider the request IDs monthly in a secure format on or before the 15th calendar day of each month (Gregorian calendar) following the month in which Customer received the chargeback information.

5.1.4 Customer may provide the request IDs by identifying each transaction, that is a confirmed fraud chargeback, by using:

(a) the "Mark As Suspect" function in Customer Selected Provider's business center;

(b) the transaction search screen within Customer Selected Provider's business center; or

(c) Customer Selected Provider's API, through the file upload function within Decision Manager.

5.1.5 Customer must assist consumers whose payment transactions have been rejected and handle chargebacks.

5.1.6 Customer must assume all responsibility for fraud strategy configuration, creating Decision Manager rules and transaction profiles.

5.2 Specific obligations for Gold level.

5.2.1 Customer must timely review and update Decision Manager rules and transaction profiles based on Customer Selected Provider recommendations. If Customer fails to comply with this obligation, Customer shall provide Customer Selected Provider feedback and reasons why.

5.3 Specific obligations for Platinum and Screening management levels.

5.3.1 Customer must manage its negative and positive lists of cards, cardholders and transactions information. Customer Selected Provider will not be responsible for managing, adding or removing information or items from either of these lists.

5.3.2 Customer must give Customer Selected Provider thirty (30) days advanced written notice if Customer wishes to add a new ID within the same line of business.

5.4 Specific obligations for Platinum level.

5.4.1 Customer must accept Customer Selected Provider recommendations regarding fraud strategy and configuration of Decision Manager and not make changes to the foregoing without Customer Selected Provider prior written consent.

5.5 Specific obligations for Screening management level.

5.5.1 Customer must provide to Customer Selected Provider, at least four (4) calendar weeks in advance, as necessary to plan for the resources required to screen Customer's expected increase in transaction volume, the following:

(a) Customer's managed services analyst assigned to its account;

(b) the reasonably accurate transaction forecast (that is, the actual transaction volume did not vary more than a 15% plus or minus from the forecast); and

(c) information related to upcoming promotional events (as it pertains to transactions volume impact).

Notwithstanding the foregoing, for any peak season (that is, any period in which transaction volume is expected to increase by 20% or more for at least 1 month), Customer must provide to Customer Selected Provider the reasonably accurate transaction forecast three (3) months in advance.

Failure by Customer to provide any reasonably accurate transaction forecast could result in missed service level targets (for under-forecasting) and/or additional costs (for under-forecasting or over-forecasting).

5.5.2 Customer must provide to Customer Selected Provider Customer's monthly chargeback rate as reported by the relevant acquirer on or before the 15th calendar day of each month (Gregorian calendar).

6. Disclaimers and limitations

6.1 Customer must have contracted and implemented our Merchant Portal – Essential XPP or Merchant Portal – Premium XPP solutions.

6.2 Customer must configure the Business Rules.

6.3 Customer must ensure that the data required for fraud screening, following the Business Rules, is always available on our Payment Platform and/or the PNR. We will not be responsible for not transmitting any data not made available by Customer.

6.4 We and the Customer Selected Provider (CyberSource) will not be responsible for determining whether a payment transaction should be cleared up for further processing or rejected.

6.5 Customer Selected Provider will not assist consumers' orders what have been rejected.

6.6 Customer Selected Provider will not handle chargebacks, chargebacks' documentation re-presentment, or negotiation or arbitration with financial institutions or Card Schemes.

6.7 Customer must configure Decision Manager rules based on the template provided by Customer Selected Provider.

6.8 We will create eight (8) administrative users in Decision Manager. Any new users must be created by the Customer.

6.9 For the screening management level:

6.9.1 Customer Selected Provider may provide its services from any one of its global review sites, including without limitation, Brazil, Costa Rica, Philippines, Portugal, the United Kingdom and the United States.

6.9.2 If Customer Selected Provider deems it is necessary to contact a consumer to verify the consumer's identity and/or other information, such communication shall be managed by Customer and shall be in accordance with the "Customer Screening Management Process" document to be mutually agreed upon by Customer and Customer Selected Provider.

If a consumer does not respond to Customer's inquiry within of the timeframe set forth in such document, the transaction will be rejected.

7. Dependencies

7.1 Customer must have contracted and implemented our Fraud Screening solution, either in referral or reseller mode.

8. Integrations

8.1 This solution can be integrated with the PNR.

8.2 Other integrations with Customer's front and back ends may be available, subject to further scoping.