outpayce from amadeus

PAYMENTS SECURITY
FRAUD SCREENING (REFERRAL)

1. Description

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

1.2 This solution enables Customer to submit in real-time a fraud screening request to Customer Selected Provider.

2. How does this solution work?

2.1 This solution implements, in XML format, the web services messages listed below, allowing Customer's access to the fraud screening services of Customer Selected Provider:

2.1.1 Message 1: we send the fraud screening request to Customer Selected Provider.

2.1.2 Message 2: Customer Selected Provider sends to us the result of the fraud screening request, that is, 'OK' (green transaction), 'CHALLENGE' (amber transaction) or 'KO' (red transaction)'.

We continue the authorization process or stop it, in accordance with the Business Rules previously established by Customer.

Green transactions are ticketed automatically, amber transactions are sent to a queue to be checked manually, and red transactions are automatically rejected and the ticketing process is stopped.

2.1.3 Message 3: where the fraud screening response is an amber transaction, Customer Selected Provider sends the tieback notification to us including the result of Customer's manual review.

Customer Selected Provider follows the Business Rules.

2.1.4 Message 4: for payment transactions that are declined we send a notification to Customer Selected Provider.

2.2 Customer provides us with the data needed to be screened via our Payment Platform and/or the PNR, if applicable. We transmit such data to Customer Selected Provider on behalf of Customer.

2.3 We route all fraud screening requests to Customer Selected Provider in accordance with the Business Rules established by Customer.

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.

4. Disclaimers and limitations

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

4.2 Customer must configure the Business Rules.

4.3 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.

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

4.5 To process device data, a specific JavaScript provided by a Third-Party Provider must be included in all Customer's frontends exploiting fraud functionalities.

5. Dependencies

5.1 Customer must have a contract with the relevant Customer Selected Provider.

6. Integrations

6.1 This solution can be integrated with the PNR.

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