outpayce from amadeus

PAYMENTS SECURITY
FRAUD SCREENING (RESELLER)

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.

3.2 Customer Selected Provider will provide one (1) training session to Customer.

3.3 This solution can be combined with 3DS 2.0 authentication.

3.4 This solution is PCI DSS compliant.

3.5 Automatic CPM.

3.5.1 CPM (Credit card Presentation Manager) functionality allows to set a PCC (Present Credit Card) indicator during the issuance or reissuance of e-ticket/EMD (Electronic Miscellaneous Document), to highlight that the passenger will need to present their credit card for verification before boarding.

3.5.2 If CPM fraud screening is activated, then:

(a) If payment with fraud screening is activated in the issuance channel and our system has analysed each credit card to determine if it is denied, challenged or accepted, then:

(i) **If at least one (1) credit card is denied**: issuance is rejected.

(ii) **If no credit card is denied, but at least one (1) credit card is challenged**: issuance is accepted, and PCC indicator is set to 'ON'.

(iii) **If all credit cards are accepted**: issuance is accepted, and PCC indicator is set to 'OFF'

(b) If payment with fraud screening is not activated in the issuance channel or our system is down, PCC indicator is set to 'OFF' automatically.

3.6 Manual CPM.

3.6.1 As per standard process, all fraud challenged (amber) transactions will be counted as sold bookings but at the same time transaction details will be pushed to fraud management interface.

3.6.2 Customer's agents can manually review these transactions and take decisions on the result, which is forwarded back to us:

(a) If final decision is negative, the transaction is considered fraudulent and, apart from any other automatic operation, PCC indicator will remain to 'ON'.

(b) If final decision is positive and manual review is completed before check-in, we will automatically waive PCC value and put it back to 'OFF'. Passenger will not need to present their credit card for verification before boarding.

3.6.3 Customer must provide a robotic user at implementation time. Robotic user will be assigned with an Office ID.

3.6.4 EMDs are out of scope.

3.7 Determine functionality.

3.7.1 The determine functionality allows the Customer's agent to know which credit card needs to be verified. It returns to the Customer's agent the last four (4) digits of the credit card that needs to be verified.

3.7.2 Depending on CPM chosen solution (baseline or fraud screening) and on the use case (first issuance or exchange), the credit card returned by this functionality is:

	CPM baseline	**CPM fraud screening**
First issuance	The credit card with the highest amount, among the credit cards	The credit card with the highest amount, among all the challenged credit cards
Exchange	The credit card with the highest amount, among the old and new credit cards	The credit card with the highest amount, among all the old and new challenged credit cards

3.7.3 Then the Customer's agent has the following possibilities:

(a) Verify the credit card: the Customer's agent needs to enter the credit card numbers so that the system compares if they match with the credit card returned by this functionality. If yes, the verification is successful, and PCC indicator is set to 'OFF'.

(b) Override credit card verification: to do so, the Customer's agent needs to enter a reason for override and PCC indicator is directly set to 'OFF'.

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. Integrations

5.1 This solution can be integrated with the PNR.

5.1.1 Once Customer has completed the manual review of the payment transaction and we receive the tieback notification:

(a) If result equals to 'OK', no further action is taken, and we update the payment record accordingly.

(b) If result equals to 'KO', the following options are available for configuration:

(i) Ignore: no further action is taken.

(ii) PNR queue: the PNR is forwarded to a dedicated Customer's queue.

(iii) Ticket void: ticketing backend is called to cancel the ticket. The payment transaction is possible only if review is done before sales closure, in case the opposite is valid, we redirect the transaction to PNR queue.

5.1.2 Comments conveyed within tieback notification are added to the PNR so that Customer's agents not managing fraud analysis can immediately recognized risky reservations and take counteractions. The following options are available for configuration:

(a) RM (General Remark): comment(s) visible to all. Customer's agents can perform manual actions based on the information conveyed via this remark.

(b) RX (Corporate Remark): comment(s) which allow sharing the fraud tie back information within the offices having an Amadeus extended ownership agreement.

(c) OSI (Other Service Information): element(s) allows comments to be transferred to the airport control system in case some actions need to be conducted at the airport.

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