Card Chargeback Guidelines

ADM Prevention

Version 3.0 | November 2020

Paper Objective

The following guidelines are consolidated as a result of the ADM User Group's effort in identifying root causes of ADMs. During 2019, Card Chargebacks represented a mere 3% of all ADMs that could be categorized with a reason for issuance, yet they represented approximately 20% of the total value of ADMs issued globally. Whilst in the ADMs there is a lack of description for the reasons of the Chargebacks, the ADM User Group discussed the difficulty in managing tight timeframes for providing the evidence that allows the Airline to challenge the chargeback and remedy the cardholder Dispute that caused it.

The following guideline aims to lay out the process and to consolidate the best practices and useful information that may help the industry to prevent the occurrence of card chargeback ADMs.

NOTE: In the present paper, the Merchant is assumed to be the Airline, as such is always the case for BSP Card Sales, which is the scenario in where ADMs apply. However, the same guiding principles apply in the prevention, and remediation, of any chargeback received directly by an Agent who is the Merchant of Record for the transaction.

Disclaimer

This document reflects information available at time of editing. The card acceptance merchant contract is the legal document stipulating the terms and conditions the airline is subject to with its card acquirer.

Table of Contents

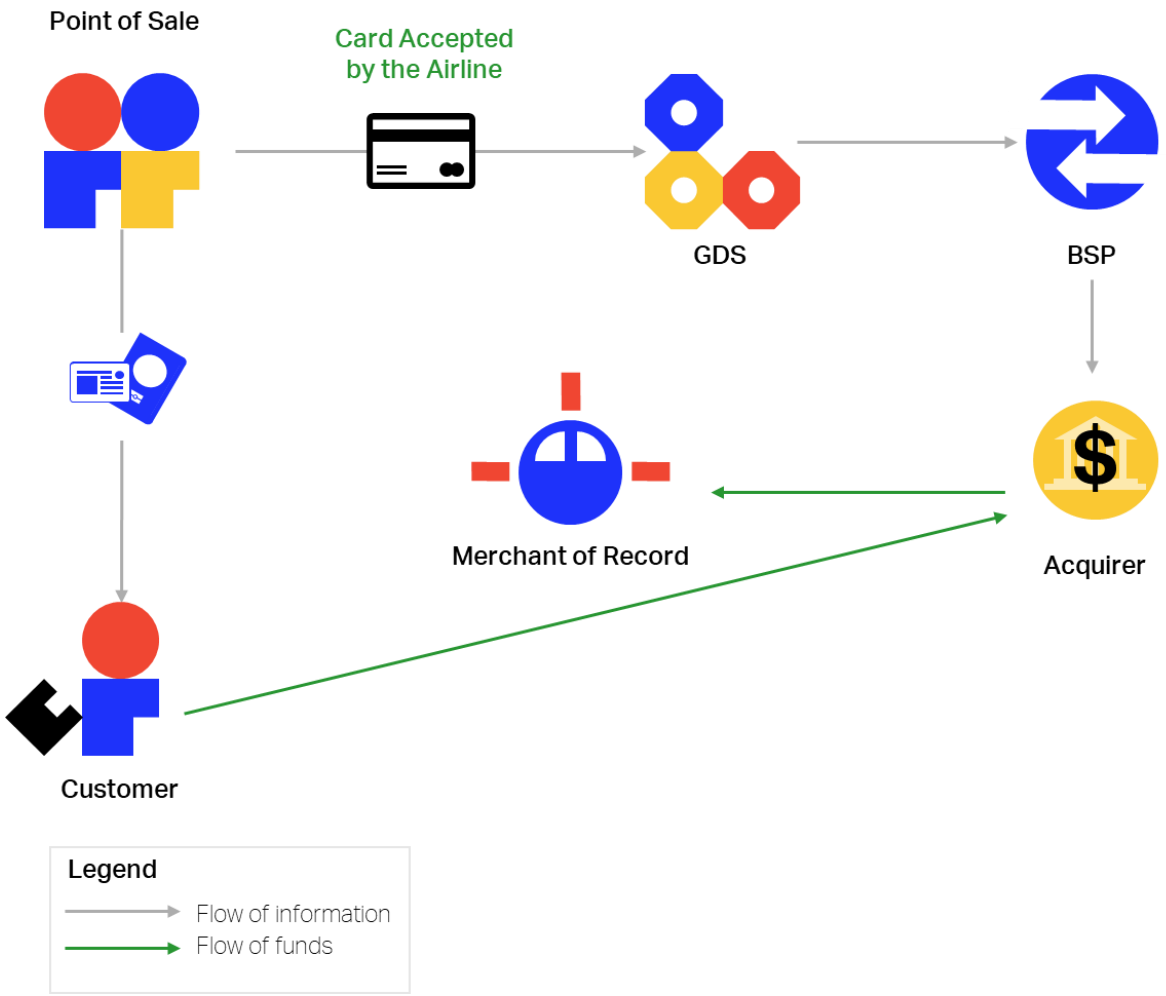
Overview: The Process

GDS Intermediated process

The BSP Card process starts when the purchase is conducted through an IATA Accredited Agent. Being the point of sale, the Agent decides if a card can be accepted. This includes checking if the airline accepts the card brand in the BSP country where the sale takes place, verifying the identity of the customer, even, if possible, use strong customer authentication. All the information is entered into the GDS system of the Agent and reported on a daily basis to the BSP with the rest of the transaction details.

Once processed, all the information is passed on to the merchant of the record – in this case, the Airline. Optionally, the card transactions will be sent for clearing to the acquirer / PSP either by the BSP, or the Airline.

This card acceptance process is unique to the Airline industry as the Agent, who is the purchase touchpoint for the customer, the card 'acceptor', is different from the merchant of record for the transaction, who is the Airline. If at a later stage the cardholder raises a dispute with their issuing bank, such information will reach the merchant – the airline, and not the card acceptor, the Agent.

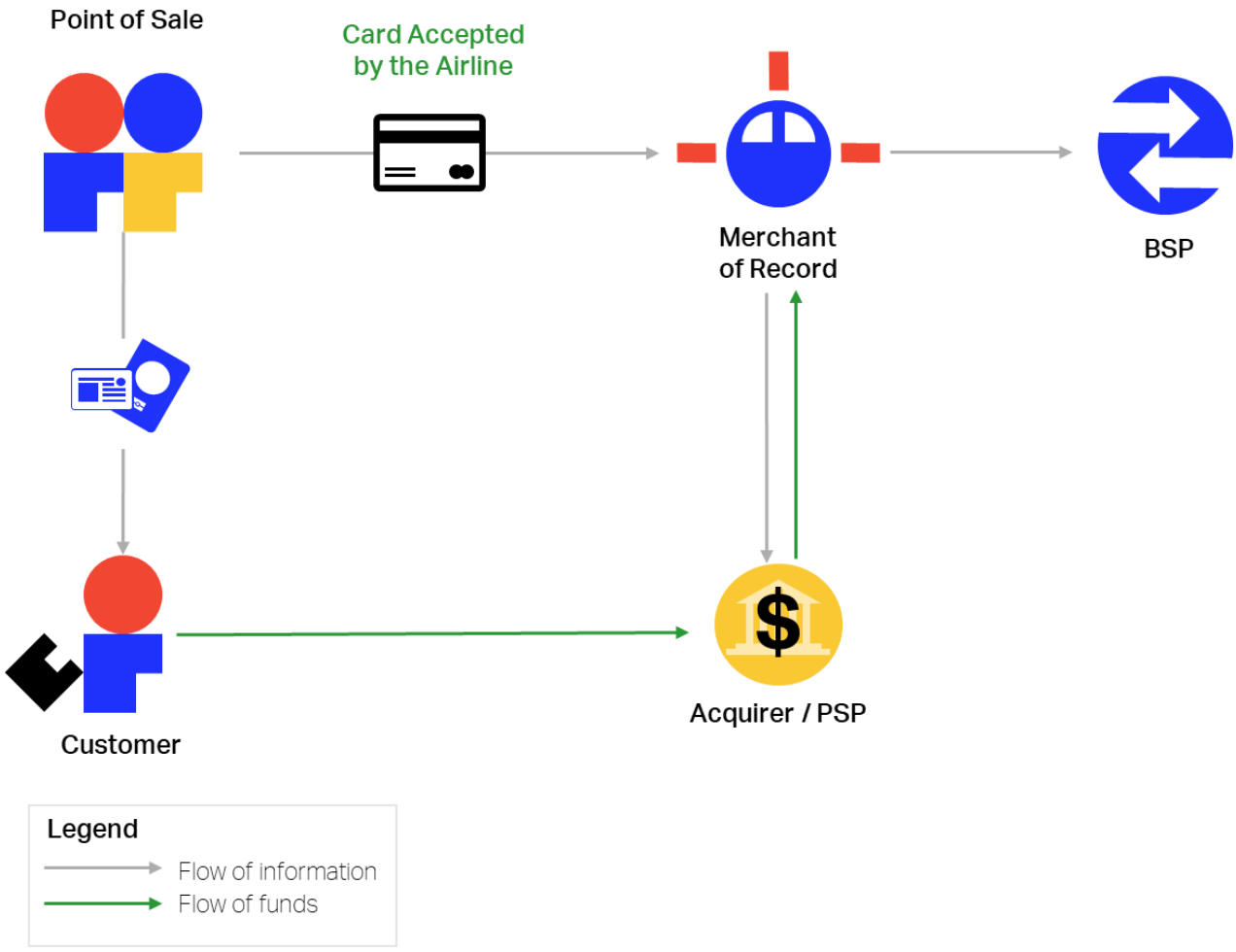


NDC process for card-paid sales

NDC (New Distribution Capability) enables the travel industry to transform the way air products are retailed to clients and offers a new way for the Travel Agent, called now 'Seller' in a more generic fashion, to work with the airline.

In an NDC transaction, the Travel Agent no longer accept the card payment on behalf of the airline by triggering a card authorization request that is transported by the GDS. With NDC, the seller merely forwards to the Airline the set of card and cardholder details. It allows the airline, still the merchant of record for the transaction, to initiate the card acceptance by creating the authorization request. With NDC, the Airline is now in full control of the card acceptance process, instead of learning about it when receiving the BSP billing reports after the card transaction already took place.

At transaction time, the Airline can revert to the Seller/Travel Agent and ask about more details (such as a missing CVV2, or a missing customer address and telephone number that the airline fraud prevention system requires to compare with the country of issuance of the card) or for an extra transaction step to be taken.



Prior to Transaction

Step One: Prior to Processing Card Transactions

Prior to processing card transactions, it is recommended that:

(1) The Airline Merchant verifies with its payment processors and acquirers how they populate the data fields in a card transaction and the card acceptance configuration it has set up in each BSP where Travel Agents will accept card payment on its behalf.

(2) The Travel Agent verifies the card acceptance policy of the airline and ensures that the customer is duly informed before any card transaction takes place that it will be the airline that charges the card.

Airline

Airlines should ensure that their Card Acceptance Policy is available and clearly communicated to the Travel Agents in BSPlink before starting to accept BSP card transactions. In these markets where the module is not available, the Airline should clearly communicate to the Travel Agent their policy.

It is not possible for any merchant to control how information is displayed in the end on the cardholder's monthly statement. Still, Airlines should confirm with their acquirers and Payment Service Providers (PSPs) that the standard data fields in the clearing transaction are correctly populated and are providing enough details for the cardholder to recognize the transaction.

Data fields

- **Merchant Name:** The merchant name is an essential information for the cardholder. Advisable practice is to report the commercial name of the Airline ("Doing business as") to avoid confusion when the transaction is received and posted by the card issuer on the cardholder statement.
- **Country of Transaction:** In the case of BSP card sales, the country of transaction is the one where the Travel Agent is located.
- **City of Transaction:** If the reported city name is the one where the Airline's headquarter is located, this could create confusion in case the cardholder has never visited this city. Some card schemes allow for Agency card sales that the Agent name be placed in the city data field in order to provide more information on the cardholder's statement. Airlines are invited to explore this possibility with their PSPs and acquirers.
- **Flight Details:** Not all acquirers and/or PSPs may be able to support the presentation of the ticket details in the body of the card transaction, as required by the card schemes. The Airline must be clearly aware of the capability of its PSPs and acquirers in that regards, as this may influence some components of the merchant fee.

Agent

The Agent plays an important role in being the point of sale. The Agent is the party accepting the card from the customer on behalf of the Airline. For this reason, the Agent shall determine if the Airline accepts the card brand presented for the purchase. This information can be validated with the Card Acceptance query in BSPlink. In case the module is not available in the market, the Agent should check directly with the Airline.

Anticipating how the transaction information will be reported on the cardholder's statement can help to reduce the occurrence of unrecognized transactions and unwarranted disputes.

The Agent should anticipate the risk of cardholder's confusion by informing them at time of sale that it is the Airline which will show as the merchant of record in the transaction reported on the cardholder's billing statement.

Any additional charges that may be billed to the customer's card, such as the Travel Agent own service fee or commission, should be clearly stated before the air travel purchase takes place.

Step Two: Accepting a Card as a Form of Payment for Air Travel Purchase

As a second step to prevent a Chargeback from taking place, the Agent must always request a card authorization, a task normally performed through the GDS. In some countries the Agent can also obtain an authorization approval code by other means and report it into the GDS tool. However, this process is more time consuming and error-prone than relying on the GDS.

As a rule, a regular authorization request is valid for 7 days only[1] . Hence, it is important to present the transaction promptly once the authorization approval has been secured. If the authorization approval code has expired, the transaction is considered as un-authorized and can be rejected by the card issuer for any reason **and without any possibility of remediation**

Reminder: an approval code is not enough!

For 'non face to face' or remote transactions, the receipt of an authorization approval code is never equivalent to a complete payment guarantee and does not guarantee that a chargeback will not be presented at a later stage. Hence, the Travel Agent must think of protecting himself by applying all possible precautionary measures.

As the Agent is the customer-facing part of the process (either physically or virtually), they can gather information at the time of sale in order to evaluate the risk associated to making the transaction, and to prevent a Chargeback-caused ADM.

The Terms and Conditions (T&C) of sale (i.e., deadlines, penalties and/or fees for cancelling, refunding, or exchanging tickets) must be disclosed to the customer prior to the transaction taking place. To minimize the risk of financial liability in the event of a chargeback associated with the uncertain disclosure of terms and conditions, obtain acknowledgement in writing from the client that the terms and conditions of sale have been disclosed and accepted.

Travel Agents may be required to show proof that the cardholder, prior to the completion of the sale, accepted the terms and conditions of the sale.

This is especially true for sales initiated via the Internet or the telephone, i.e. card not present transactions. Online Travel Agencies (OTAs) are encouraged to clearly and concisely state the terms and conditions of the sale and require cardholders to go through a mandatory "click to accept" or "tick the box" process before moving to the payment page. It is also imperative that such proof be retained and stored, so as to be communicable several weeks or even months after the sale if a dispute with the cardholder arises.

E-mail or verbal disclosure of the terms and conditions of sale to the cardholder may not be sufficient as a legitimate remedy against card chargebacks related to a cardholder's claim that the terms and conditions of sale were not disclosed prior to the sale taking place.

Reference to a separate document listing the terms and conditions, distinct from the payment process, is not acceptable. The Travel Agent must be able to prove that the client was 'forced' to contemplate the terms and conditions before pursuing with the payment.

Before reviewing the Tips, remember that:

As a rule, a CVV2 or AVS Match response does not provide a payment guarantee, or allow to challenge a fraud chargeback, as such data may have been hacked alongside the original card number. These are an additional element, besides other fraud prevention tools, which enables a card accepting entity to evaluate the fraud risk for a given transaction.

However, there are domestic or regional instances where a card scheme may grant the right to the merchant to defend itself against a fraud chargeback with an AVS response or if the issuer approved on a 'CVV2 mismatch'. Hence the Agent should store the details of the response in order to supply this to the airline, in case this offers a chance to challenge the fraud chargeback.

Tip 1

CVV2

Card security codes are known under different terminologies by the card schemes: Visa - CVV2, MasterCard - CVC2, American Express - CID, Discover - CMID, Union Pay - CVN2, JCB - CAV2.

In most cases, the card security code corresponds to a 3-digit number printed on the signature panel on the back of the car, and follows (not always) the printed last four digits of the Primary Account Number (PAN). For American Express, the card security code is composed of 4 digits, located on the front of the card, above the card number on the right hand side.

Passenger Agency Conference Resolution 890 stipulating how BSP card sales must be conducted demands that, in view of the risk posed by a cardholder not being able to provide the correct CVV2, the Agent does **not** complete the sale and seek another means of payment from the client.

When conducting a card payment authorization request, it is important to add this security value to the other card details, and to take note, alongside the approval code, of the CVV2 verification result. Possible responses are:

"M – Match": cardholder's provided CVV2 was verified and validated by the issuer
N – No Match": cardholder's provided CVV2 does not match
"P – Request not Processed": the verification was not performed (technical issue)
"U – Issuer does not support feature": in rare cases, the issuer is not registered with the card scheme to use this security feature

An Agent should always submit the security code when soliciting a card authorization request.

An Agent should ensure it always receives the CVV2 verification result before deciding to finalize or not the sale, and is invited to inquire with its GDS providers what information they make available.

Reminder: Storing the CVV2 is absolutely forbidden under any circumstance!

The above discussion is only about storing the CVV2 response. For that reason, CVV2 does not apply to instances such as 'lodged cards' or 'card on file' scenario, whose details are stored at the Agent or in on-line booking tool for use when the cardholder, a regular client, books a trip. It is assumed that the user of a lodged card is known personally by the Agent, or undergoes a rigorous internal approval process when booking a corporate trip, thus making the payment with the lodged card generally safer than a card payment from a first time and unknown customer.

Tip 2

AVS

When accepting a card issued in Canada, United Kingdom or the United States, remember that you can use AVS! Address Verification System (AVS) helps "Card-Not-Present" merchants prevent fraudulent card use by verifying that the client making a "card not present" transaction knows to which address the monthly billing card statement is mailed to.

While collecting the client's card billing address is not mandated by any industry standard, it is a useful step to identify discrepancies in a purchase that may point out to a fraud risk.

How does it work?

AVS is a security feature used by Visa, MasterCard and Discover, that verifies the billing address of the cardholder. AVS verifies the numeric components of the cardholder's billing address.

For example, if the address is "50 Montgomery Street, San Francisco, CA 94111, USA", AVS will check 50 and 94111. The issuer will insert into the authorization response message, alongside the approval code (and alongside the CVV2 verification result) an AVS response code.

An AVS mismatch coming alongside an authorization approval code should be seen as a warning sign.

American Express supports 2 fraud mitigation tool which differ slightly from AVS:

- Automated Address Verification (AAV) allows to verify the billing address of a customer from any country (and not only from Canada, United Kingdom and the United States)
- Enhanced Airline Authorization data refers to the submission of the ticket details in the authorization request, which enables American Express to make a better informed decision when approving or refusing a transaction.

An Agent should always submit AVS, AAV and Enhanced Airline Authorization data when soliciting an authorization request. An Agent should ensure it always receives the relevant verification results before deciding to finalize or not the sale.

Reminder: AVS does not apply for cards issued outside of Canada, UK & USA!

However, any card transaction made anywhere in the world with cards issued in those 3 countries should be conducted with AVS, given that such cards are among the most defrauded globally in the airline industry[2].

As AVS only checks the numeric portions of the address, certain anomalies may be caused by apartment numbers for example, which can cause false mismatches; however, this is reported to be a rare occurrence.

Tip 3

EMV Chip & 3D Secure

EMV is the technical standard for chip cards and for the payment terminals that can accept them.

Generally speaking, international card schemes grant fraud chargeback protection to the merchant who is accepting cards on a certified chip and PIN terminal. However, usage of electronic payment terminals is not supported for the making of BSP card sales, hence that concept can only apply when the Agent is the merchant of record for the card transaction and accepts card payment on a Point Of Sale payment terminal installed at one his physical locations.

3D Secure (3DS) is an XML-based protocol designed to be an additional security layer for online card transactions, by adding a cardholder authentication step. It is offered to customers under various commercial names such as Verified by Visa, MasterCard SecureCode, J/Secure (JCB) or American Express SafeKey. Company EMV Co has now taken over the management of that 3DS standard on behalf of the card industry, and newer versions of the standard (2.0 and higher) are collectively known as 'EMV 3DS'.

International card schemes grant fraud chargeback protection to the Internet merchant who has rolled out the capability to conduct 3D-Secure transactions, even if the cardholder is not enrolled and cannot be authenticated. While card schemes rule differ slightly, a merchant capable of 3D Secure at time of transaction should not receive a "Card Not Present" fraud chargeback. If they do, they have a re-presentment right allowing them to dispute successfully the fraud chargeback.

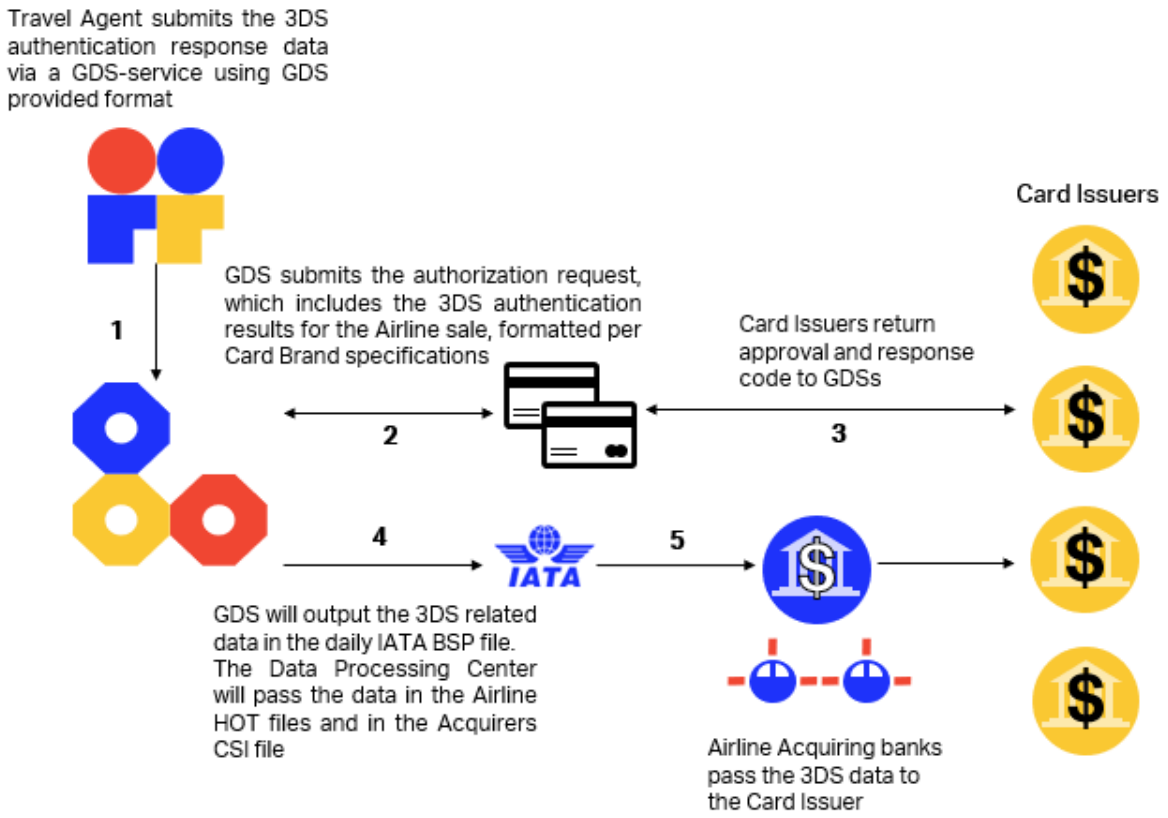
In Europe, a regulation mandating Strong Customer Authentication entered into force on 14/09/209, though enforcement is delayed until 31/12/2020 (14/09/2021 in the UK). Essentially, it mandates that all ecommerce transactions be authenticated through 3D Secure unless they qualify for a series of exemptions. Card issuers are expected to refuse to approve an authorization request conducted without SCA and that does not refer to an exemption case.

An exemption case that is most likely to be relevant for many BSP card sales is the Secure Corporate Payment Exemption, which may apply when the lodged card of a corporate client, stored in an on-line booking tool or at the TMC, is used to book a ticket. In Europe, Travel Agents are invited to discuss SCA readiness with their Distribution/Ticketing Service Providers and 3DS Secure providers in order to ensure the compliance of their transactions and avoid the risk of transaction refusal. Outside Europe (where SCA regulation does not apply), Travel Agents are invited to discuss with their providers how they could use 3D Secure for some of their BSP card sales in order to prevent fraud.

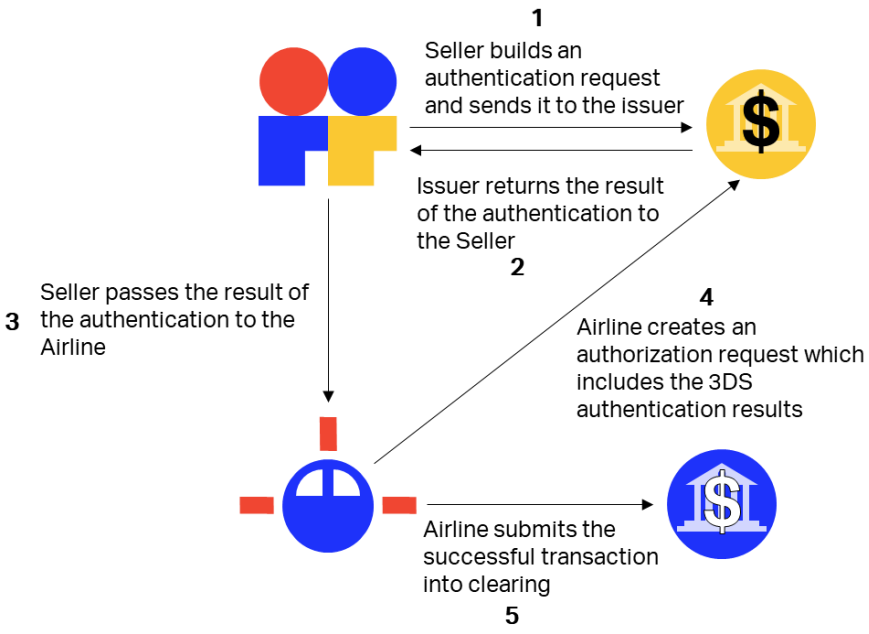
In Europe, the Travel Agent believing the transaction fits an SCA exemption case that does not warrant the application of 3DS must discuss with their Distribution/Ticketing Service Providers on what they have planned to cater for this situation.

3D Secure can be used for the issuance of both a BSP and an NDC transactions, however, the payment process may differ depending on the environment and technology used. Below are illustrated different scenarios.

Processing a 3DS transaction in the BSP



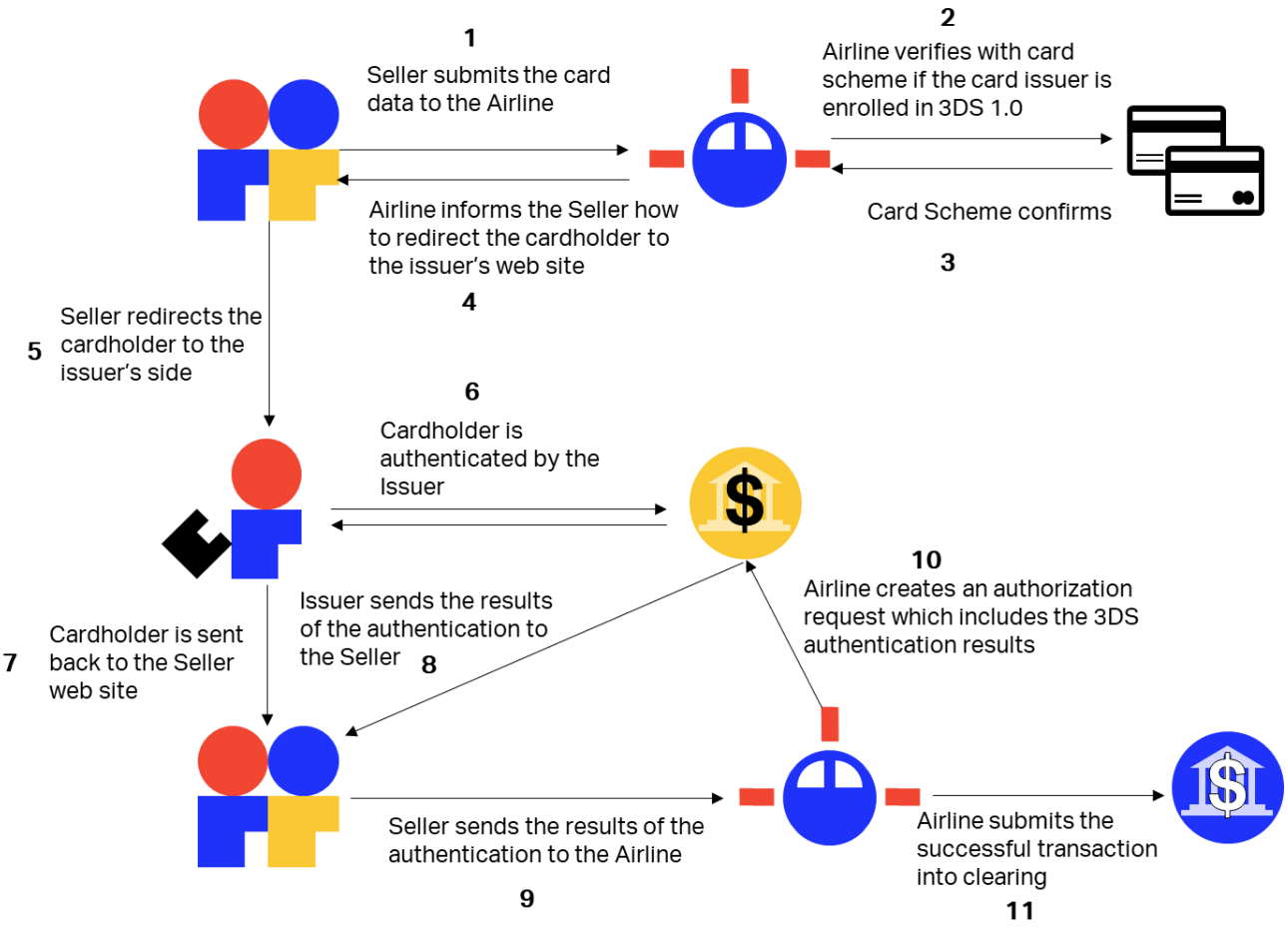
Processing a 3DS transaction in NDC



Scenario 1 for 3DS EMV Versions

Scenario 2 for 3DS 1.0 only

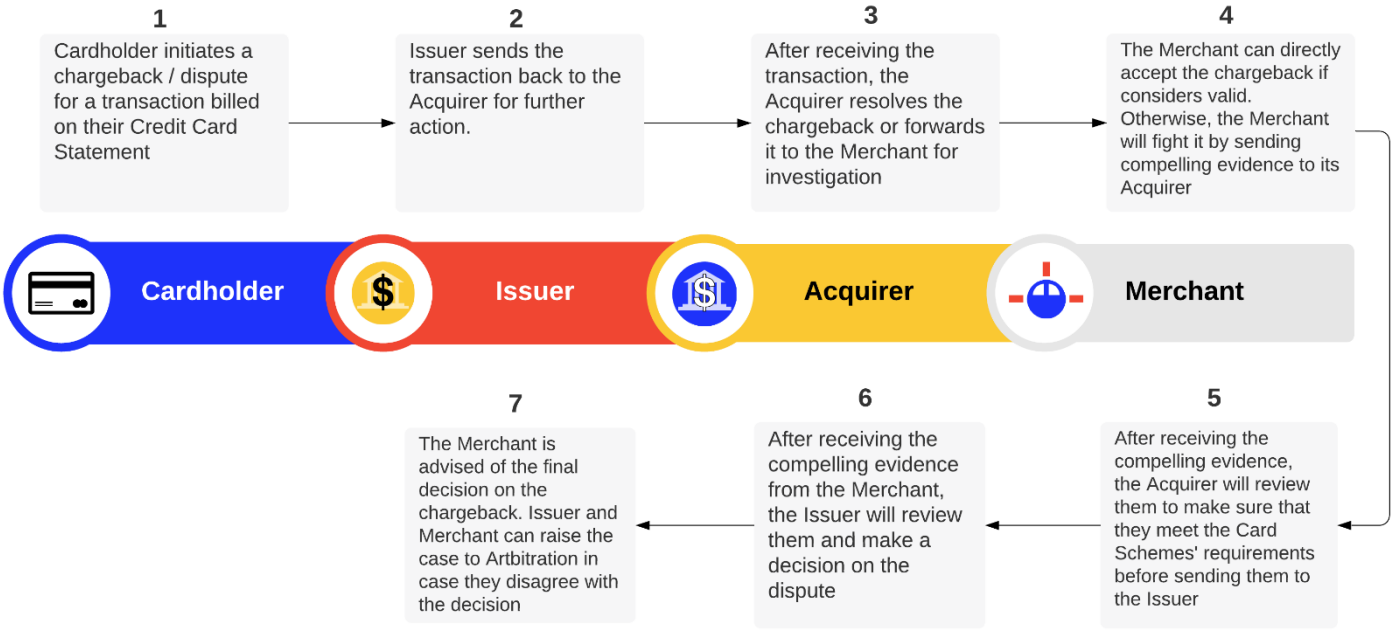
Processing a 3DS transaction in NDC



The NDC transaction format, called NDC schemas, allow the Seller/Travel Agent to forward to the airline the result of a 3DS authentication attempt, or the information that an SCA exemption may apply, which allows the airline to label adequately the card authorization request that it then creates.

Post Transaction

Once the cardholder has been billed for the transaction, they will receive the charge on their billing statement. They will be able to initiate a card dispute on such charges through their issuer. Below can be found the overall chargeback process.



Types of Chargebacks[3]

Criminal Fraud

A fraudster used a legitimate cardholder's information, to purchase an item from a merchant. The real cardholder, upon seeing this charge on their statement, files a fraud claim with their issuing bank against the charges. In cases of criminal fraud, there is little that merchants can do other than refund the sale amount, unless it was a 3D Secure transaction

First Party Fraud

First Party Fraud, also known as Friendly Fraud, refers to situation where the cardholder disputes seemingly legitimate charges. Reasons may be: the customer experienced buyer's remorse and regretted making the purchase, a relative made the purchase but the primary cardholder does not want to pay for the transaction, or the customer attempts to get something for free

Merchant Error

These chargebacks could be caused by system errors or problems arising from your business process such as duplicate transactions, insufficient customer service, unwanted recurring payments, authorization errors or faulty product fulfilment.

Authorization errors can occur when the merchant attempts to override a declined transaction, or from multiple deposits made to complete a single authorization.

Step Three: Card Issuer Contacts the Merchant for Information

The cardholder may initially inquire with their issuer about a transaction they do not recognize. At this stage they would deny having made the transaction, they are simply looking for more details about the nature of the unrecognized purchase.

The issuer will send a request for further information to the acquirer of the merchant, which in turns asks the merchant. The request for information is sometimes called "*retrieval request*" in card scheme language.

In the context of a BSP card sale, the airline may respond with the details it holds about the tickets sold, or revert to the Agent to ask him to provide information which may further help the cardholder.

As a best practice, this dialogue should take place between the Airline and the Agent PRIOR to issuing an ADM. This would enable a communication that is not restricted to the Resolution mandated timeframe of 15 days before the ADM is processed (Resolution 850m, section 4.5).

The relevant information must be sent back by the airline merchant to the issuer, via the acquirer, within specified timeframes.

If the submitted information satisfies the cardholder, they will notify the issuer that the enquiry is closed. Otherwise, they may then claim he did not engage in the transaction and raise the dispute.

Tip 4

Agents can help the customer recognize the card transaction

Inform your customer (the cardholder) that on their card billing statement they should not expect to see the name of your travel agency, but instead the name of the Airline that the ticket is issued upon, and remind them to try and verify the amount being charged before raising an inquiry or a Dispute with their card issuer.

Quick win

When receiving a request for information on the transaction, it may be more efficient for the Agent to contact directly their client and ascertain what the nature of their inquiry is.

The transmission of further details through the airline, acquirer, card scheme and ultimately the issuer, takes time and increases the chances of some information getting misplaced. Attempting to understand and solve the issue directly with the client may be the fastest way to resolve their problem and to ensure they notify their card issuer that he withdraws his inquiry.

Card Scheme specifics

Visa and MasterCard are streamlining their chargeback management rules by removing the concept of RFI/RR.

Visa will eliminate effective 17 October 2020 the Visa Retrieval Request for any transactions. The full removal of the functionality is planned for April 2021.

Mastercard has eliminated the Chargeback rights reason code 4863 "Cardholder Does Not Recognize" and it is now considered invalid.

Direct issuer to merchant communication

An important part of the Visa and MasterCard chargeback reform is to create the conditions for the merchant and issuer to have a direct dialogue (via APIs) prior to the raising of a chargeback, which should be the action of last resort.

The idea is that merchants and issuers can directly and more quickly exchange questions and answers to address the cardholder's claim and hopefully find a resolution that does not require a chargeback.

Step Four: Chargeback

The card issuer may raise a chargeback without going through a request for information/retrieval request if, at the time of the cardholder's enquiry, the card issuer feels the situation is clear and the cardholder disputes the transaction. Visa and Mastercard will eliminate the retrieval request step, thus, the merchant will have to directly manage the chargeback.

To address the chargeback, follow the below three steps:

1

Is the chargeback within the timeline imposed by the card acceptance merchant contract?

The general rule is that chargebacks related to fraudulent transactions must be raised by the issuer within 4 months (120 calendar days)from the transaction day.

If on the other hand the reason for chargeback was "Service not rendered", the timeframe to raise such chargebacks is 4 months **from the last date that the cardholder expected to receive the service**. As the card transaction to pay for the ticket may have been made several months before the flight date, the time elapsed between the card transaction and the raising of a chargeback may be considerably more than 4 months[4].

Still, if the chargeback has been sent by the card issuer beyond the permitted timeframe, the chargeback may be challenged as invalid. The Airline's merchant contract will stipulate what is the valid timeframe for receiving a chargeback. The first step in defending against a Chargeback should always be to ensure the chargeback is valid from a contractual point of view.

2

Is the chargeback within the other parameters defined in the merchant agreement?

Always check your merchant agreement, to make sure the chargeback is within the parameters defined in the contract, as the merchant agreement is the sole contractual document allowing financial losses to be passed onto the merchant. Besides the valid timeframe, it may have other stipulations, such as which are the valid reasons for a chargeback, or that the issuer must report the fraudulent transaction into the card scheme's fraud reporting system[5] prior to raising a chargeback (failure to do this invalidates the chargeback).

If you detect gaps within your merchant agreement, note them and ensure that these clauses are clarified.

3

Provide useful documents to increase the chances of fighting successfully a chargeback

Visa leaves 30 days to the acquirer for refuting a chargeback, and Mastercard 45 days.

Nonetheless, the actual amount of time left to the merchant to gather and transmit its evidence will depend on each individual merchant agreement. On average, an Airline merchant is given 14-21 days by its acquirer to challenge a chargeback and provide any supporting documents, so as to leave time for the acquirer to process the response it received. American Express leaves 20 days only[6]

When required, the Airlines will in turn request the Agents to provide any missing information within 7 days of being asked (as stipulated in Passenger Agency Conference Resolution 890 & 890x) to complement their reply.

Given the short and stringent timeframe, it is important that Agents and Airlines:

- preserve the availability of necessary data for as long as a valid Chargeback could be issued (Resolution 890 demands that such records be kept by the Agents for 13 months)
- route requests and responses with the greatest expediency possible.

Card schemes and acquirers provide merchants with checklists of documentation and compelling evidence they should provide to remedy the chargeback. Some of the resources that card schemes have publicly available can be found below and present the intent and details of their rules are, but only the card acceptance contract is legally binding for the merchant.

Compelling evidence is circumstantial evidence that is not direct proof of the transaction itself, or does not form part of the transaction being disputed. Nevertheless, it may lead the card issuer or the card scheme to review the cardholder's claim under a different angle.

Card Scheme	Checklist
Visa	https://usa.visa.com/dam/VCOM/download/merchants/chargeback-management-guidelines-for-visa-merchants.pdf
Mastercard	https://www.mastercard.us/content/dam/mccom/global/documents/chargeback-guide.pdf
American Express	https://www.americanexpress.com/content/dam/amex/us/merchant/pdf/gms_Compelling%20Evidence_final.pdf https://www.americanexpress.com/us/merchant/manage-disputes.html

Type of information that may contribute to the resolution of a chargeback

Airline

- → A copy of the Airline ticket
- → Proof that a correcting transaction that directly offsets the disputed transaction has already been processed (proof of a 'refund' or 'credit' transaction having been issued)
- → Transaction information, Billing Information and Journey Information
- → The e-ticket issued for an accompanying minor (infant or child) was not disputed, while the ticket of the adult passenger was. Since an infant or child ticket cannot be issued or consumed without travelling with an adult passenger, the lack of dispute on the infant/child ticket allows to challenge the dispute on the adult ticket.
- → Transactions for excess baggage or seat upgrades or in-flight purchases[7], that were not disputed, allow to challenge the dispute on the related flight ticket.
- → Customer disputing the card transaction but not the Frequent Flyer Miles that they were credited with. Since the policy of crediting mileages is based on flown segments only, a Chargeback should not lead to any associated mileage being credited to the account holder.

→ Flight manifest showing the names of the travellers[8]. In order for the provided information from the flight manifest to be clearly readable by a third party, it is extremely important to:

- only provide the relevant section of the flight manifest
- explain how to read the document
- highlight the most relevant parts

Issuer chargeback staff and card scheme case reviewers are not airline industry experts and cannot be expected to know how to read specific documents such as flight manifests, or what value such a document has. Without a comprehensive and step by step explanation, they are likely to dismiss the documents as not sustaining the argument presented by the merchant disputing the chargeback.

Additional Information

As a rule, card schemes do not mandate that the issuer share the name of the actual cardholder, for data privacy reasons. As a consequence, it is difficult for the Airline to prove a connection between the traveller's name it has in its possession, and the cardholder's actual name. When attempting to verify a cardholder's name with the issuer, whether reviewing a suspect transaction or a chargeback, one can increase the odds of getting information back by not asking the issuer what the name of the true cardholder is, but by asking confirmation if the name of the true cardholder is "Joe Smith" for example.

Compelling evidence can be provided when a cardholder purchased a flight ticket for another person, in order to prove the relationship between the cardholder disputing the transaction and the traveller who actually flew.

Reminder! PNR or reservation information is not sufficient to prove that a passenger flew. Information must be obtained from flight manifest/ticket usage system once the boarding pass is scanned, in order to certify that the person had boarded the plane.

Agent

A discussion with the customer at this stage may help reveal a misunderstanding or a query that was misinterpreted by the card issuer as a refusal to recognize and accept a charge. The Agent can take the opportunity to clear up the issue and invite the customer to revert to their card issuer and withdraw or amend the claim that was recorded. In these cases, the Agent should try to collect a confirmation or statement from the customer to this effect, in case it is required in the future.

In other cases, when efforts to contact the customer prove fruitless, the following information may also be useful in contributing to the resolution of a Chargeback:

- → Proof of confirmation for booking or reservation
- → Clearly Signed (if applicable) Itemized Invoice or Receipt that supports the transaction including a copy of the booking and reservation notice
- → Proof that the cardholder agreed to the transaction or authorized a 3rd party to make the purchase. Any additional information that can confirm the relationship between the customer (who is the alleged owner of the card) and the traveler can also be sourced and provided.
- → A copy of the T&C including the cancellation, return, refund and no show policy.
- → Proof that the T&C were provided and accepted by the customer **at the time of the sale**

Environment	T&C disclosure & acceptance proof
Online Sales	A copy or screenshots, or IT logs, that show the sequence of pages before final checkout and prove that before payment, the client was fully advised, and clearly expressed consent through a "click to accept" or other acknowledgement button, checkbox, or location for an electronic signature, or on the checkout screen before moving to the payment phase. Bear in mind that for internet sales, a simple link to a separate web page is not an acceptable "proper disclosure".
Telephone / Face-to-Face	The customer must have received (at the time of sale), a disclosure of the refund and credit policies via post, email or text message (SMS). You must be able to prove that such dispatch took place and was received by the client.
BSP Face-to-Face	BSP card sales are usually conducted through the manual entry by the Agent of the PAN (Personal Account Number) and other card data into the GDS work screen. In such process, there is nothing in the body of the resulting card transaction which differs from a 'card not present, cardholder not present' situation such as a telephone sale.

BSP Face-to-Face	Historically, the card schemes have allowed the subsequent production of a signed manual imprint to prove that a card and cardholder were present at time of transaction, thus remediating a 'card not present' type of fraud chargeback. As a result, in Resolution 890 it is recommended for the Agent to make such an imprint in the case of a 'face to face' sale. It is worth noting that effective 04/2017, a signed manual imprint, traditionally known as the UCCCF (Universal Credit Card Charge Form) in the airline industry, will no longer enable a merchant to remedy a MasterCard fraud chargeback worldwide. With the worldwide roll out of EMV chip and PIN terminal as the preferred and most secure way to conduct face to face card transactions, the taking and storing of a signed manual imprint, which was already an ungainly business requirement, becomes increasingly obsolete as a concept. However, as explained before in section 2, usage of electronic payment terminals is not supported for the making of BSP card sales[9].

Reminder: Often it is difficult to prove that the cardholder agreed to the transaction

A letter signed by the cardholder authorizing a transaction, or the accompanying copy of an ID, often has no value in these circumstances, as it can be easily forged. As a rule, a copy of the card and alleged cardholder ID, or of a letter allegedly coming from the genuine cardholder, do not allow to successfully remedy a Chargeback; anyone can pretend to be the legitimate holder of a given card, and it is not possible to verify the name of a cardholder in a card transaction. The billing address, however, can be verified in some cases, as mentioned in section 1 (see AVS).

Step Five: Pre-Arbitration and Arbitration

If all possible information has been provided and if the issuer maintains the chargeback despite the merchant argument, the issuer will request the scheme to arbitrate. Upon the issuer filing, the merchant's acquirer is given the opportunity to accept liability or let it continue to arbitration, where the card scheme will act as a 'judge of last resort' and adjudicate the dispute between the issuer and the merchant.

However, in order to deter spurious cases, the losing party is responsible for arbitration-related fees. Hence, this requires a party to be absolutely certain in the solidity of its argument before undergoing that final step.

Step Six: Agency Debit Memo

After every effort to fight a chargeback has been exhausted, the final step to the process would be for an Airline to issue an Agency Debit Memo (ADM) to the Travel Agent in order to recover the lost funds.

	GDS Sale	NDC Sale
Framework	BSP Card sales reported to the BSP by the GDS where the Airline is the Merchant of record for the transaction	Card sales reported to the BSP by the Offer Managing Airline who is the Merchant of record for the transaction
Applicable Resolution for Card Sales Rules	Resolution 890 (link)	Resolution 890x (link)
Agent's Responsibility and Liability	- Be PCI DSS compliant - Ensure that the Card brand is accepted for payment by the Airline - Obtain an authorization approval code for each transaction and record it.	- If the Agent was not party to the card transaction, and if the customer was directed to the Airline's own payment page, the Agent will not be liable for any eventual fraud chargebacks received by the Airlines - If the Agent assisted in conducting the transaction, which was created in a secure manner (for example: using 3DS), there will be no liability on the Agent - If the Agent assisted in conducting the transaction, which was not created in a secure manner, the Agent will be liable for any eventual fraud chargebacks received by the Airline
Comments	As per IATA Passenger Agency Sales Rules, if an ADM is issued due to a Chargeback (and NOT due to a cardholder's inquiry, or potential Chargeback) the ADM is not eligible to Dispute. For that reason, it is important that all necessary steps in answering the cardholder's initial inquiry, and subsequent efforts to gather circumstantial documentation to fight the Chargeback, have been tried by the Airline, with the full support of the Travel Agent, in order to increase the chances of success.	As per IATA Passenger Agency Sales Rules, if an ADM is issued due to a Chargeback (and NOT due to a cardholder's inquiry, or potential Chargeback) the ADM is not eligible to Dispute. This would not be applicable in the scenarios where the Agent is not liable for any potential card fraud risk due to the lack of involvement in the card transaction.

Frequently Asked Questions

What should happen when the Agent suspects a fraud case and wants to cancel the transaction?

1. The Agent should request the Airline to issue a complete refund to the card, in order to make the cardholder 'whole' again.

2. The Agent must issue this refund for the full amount of the original transaction and not deduct cancellation penalty or sales commission adjustment, as such issues are strictly between the Agent and the Airline and the cardholder is not a party to them. Anything less than a full refund will lead the defrauded cardholder to raise a fraud claim for the full amount of the transaction he does not recognize, thus compounding the problem the airline and the Agent are facing.

3. A sale cancellation and refund by the Agent may trigger penalty fees, which may not factor in the very specific case of fraud prevention. The industry needs further discussion on how to ensure that commercial conditions do not inadvertently inhibit proactive fraud prevention measures by each concerned party.

Reminder!

Even if the card refund is issued promptly, it may come too late to appear on the same cardholder monthly statement where the original purchase transaction is posted, thus leading the cardholder to raise a dispute, as they are not aware that a card refund is 'on the way'. This is remediated with the airline proving that a full card refund was issued.

The refunded amount, once converted into the cardholder billing currency, may vary from the amount of the initial purchase because of daily currency fluctuations. This can also cause the cardholder to raise a dispute, which is remediated by showing that the amount refunded was for the full amount in the original purchasing currency.

Processing refunds on Customer Card

1. A transaction paid with a Customer Card must be refunded on the **card originally used for payment** in accordance to general Card Scheme Rules and as stipulated in Resolution 890, section 9.2.

2. A transaction paid with multiple forms of payment must be refunded by processing **the original amounts to each respective form of payment** as per Resolution 824r, 1.2.

   For example, if transaction is paid by a customer card and additional cash amount included in the Agent's billing, the refund should be processed in a manner that it reimburses the amount paid by card to the card originally used for payment and the amount paid in cash through BSP cash reflected on the Agent's Billing statement.

3. The issuer to whom the client raised a dispute may not accept a refund processed on another card or another form of payment as an acceptable remedy, as it may be difficult to prove that the refund actually went to the cardholder who raised the dispute[10].

References & Additional Resources

1- In some cases, a card scheme may extend the validity of an authorization request subject to specific conditions but as a rule, authorization requests for BSP card sales are flagged in the standard way only.
2- Managing payment card fraud – a guide for airlines by Visa Europe
3- Sources used: Understanding the Sources of Chargebacks by Chargebacks911 (https://www.chargebackgurus.com/blog/types-of-chargebacks) & https://www.signifyd.com/resources/fraud-101/chargebacks-a-history/
4- Mastercard and American Express do not set a time limit for raising a 'service not rendered' chargeback other than 120 days after the day the service was to be rendered. Visa on the other hand rules that a chargeback cannot come more than 540 days after the day the transaction was processed.
5- A merchant can ask the acquirer for the list of fraudulent transactions that were reported as having taken place at his business, in order to check if a transaction that is charged back for fraud was also separately reported as fraud by the issuer, as per card schemes demand.
6- American Express extended temporarily the deadline for merchants to challenge a chargeback from 20 to 30 days during the apex of the COVID crisis, as merchants were over-helmed by refund requests and chargebacks
7- If an airline completely outsources the management of in-flight purchases, it may not have access to any details of the ensuing card transactions
8- Often the issuer will not provide the name of the true cardholder. Hence, the airline cannot verify by itself if it is true that no traveller's name matches the name of the true cardholder, it must rely on the issuer to conduct this verification.
9- Usage of a card payment terminal to conduct BSP card sales is infrequent save rare local exceptions which rely on a single local acquirer capturing the totality of the airline BSP card sales.
10- If a refund is made on an expired card, the issuer can assign it to the customer account standing behind the expired card number.

- PSD2 Country specific information (Ayden): https://www.adyen.help/hc/en-us/articles/360016479159-PSD2-Country-specific-information
- Global Payment Trends and Market Guides (WorldPay): https://worldpay.globalpaymentsreport.com/#/en/home

CARD CHARGEBACK GUIDELINES | VERSION 3.0

www.iata.org/adm