CREDIT CARD CHARGEBACK GUIDELINES

ADM PREVENTION

Version 2.0

IATA ADM User Group

June 2018

CARD CHARGEBACK MANAGEMENT GUIDELINES- ADM PREVENTION

CONTENTS

CARD CHARGEBACK MANAGEMENT GUIDELINES- ADM PREVENTION

OBJECTIVE OF PAPER

The following guidelines are consolidated as a result of the ADM Management & Reduction Project's effort in identifying root causes of ADMs. During 2015, 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 Working Group discussed the difficulty in managing tight timeframes in 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: Within the below 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 attempted prevention, and remediation, of any chargeback received directly by an Agent who is the Merchant of Record for the transaction.

DISCLAIMER

International card schemes and especially Visa International and Mastercard are in the process of rolling out globally chargeback reforms aiming to reduce the number of incorrect chargebacks, shorten timelines and simplify processes. While this document reflects information available at time of editing, those reforms are too recent for their impact to be factored in.

The card acceptance merchant contract is the legal document stipulating the terms and conditions the airline is subject to with its card acquirer.

THE PROCESS

ONE: PRIOR TO PROCESSING CARD TRANSACTIONS

Prior to processing card transactions, it is recommendable 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.
(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.

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.

However, it is not possible for any merchant to control how information is shown on the cardholder's statement. 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 been to. 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, and airlines are invited to explore that possibility with their PSPs and acquirers.

Flight Details: not all acquirers and/or PSPs support flight data for all card types. The airline must be clearly aware of the capability of its PSPs and acquirers.

AGENT

The Travel 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 presented for the purchase. This information can be validated with the Card Acceptance query in BSPlink.

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

The Travel Agent should anticipate the risk of cardholders' confusion by informing them at time of sale that it is the airline which will show as the merchant in the transaction.

Any additional charges that may be billed to the customer's card should be clearly stated before the air travel purchase takes place.

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 request a card authorization through the Global Distribution System. In some countries the Travel Agent can also ask for a manual authorization by placing a phone to the call center of a merchant bank, 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 secure.

Remember: an approval code is not enough!

For 'non face to face' or remote transaction, the receipt of an authorization approval code is never equivalent to a 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), he 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 of sale (i.e., deadlines, penalties and/or fees for canceling, 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. 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. OTAs are encouraged to clearly and concisely state the terms and conditions of the sale and require cardholders to "click to accept" them before moving to the payment page.

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 pursing with the payment.

Tip 1 - Card Verification Value 2 (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 card, and follows (not always) the 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.
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:
o "M – Match": cardholder's provided CVV2 was verified and validated by the issuer

[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.

o “N – No Match”: cardholder’s provided CVV2 does not match

o “P – Request not Processed”: the verification was not performed (technical issue)

o “U – Issuer does not support feature”: in rare cases, the issuer is not registered with the card scheme to use this security feature

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.

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.

Remember that:
As a rule, a CVV2 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. CVV2 is an additional element, besides other fraud prevention tools, which enables a card accepting entity to evaluate the fraud risk in 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. 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.

Remember that storing CVV2 is absolutely forbidden under any circumstance.
For that reason, CVV2 does not apply to instances such as ‘lodge cards’, whose details are stored at the Agent for use when the cardholder, a regular client, books a trip. However, one assumes that the user of a lodge card is known personally by the Agent, thus making the payment with the lodge card safer than a card payment from a first time, unknown customer.

Tip 2 - Address Verification System (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 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 result before deciding to finalize or not the sale.

Remember that
As a rule, an 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. AVS is an additional element, besides other fraud prevention tools, which enables a card accepting entity to evaluate the fraud risk in 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. 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.

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

When cards are issued in other countries than Canada, the UK and the USA, AVS does not apply. 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].

Tip 3 - 3D-Secure and EMV

EMV is the technical standard for smart payment cards (also called chip cards or IC cards) and for 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 EMV terminal.

At present, usage of electronic payment terminals is not supported for the making of BSP card sales, though developments have been made in the past to accommodate the necessary information in GDS files submitted to BSP.

[2] Managing payment card fraud – a guide for airlines by Visa Europe

3-D Secure 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.

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 verified.

While 3-D Secure is not supported at present for the making of BSP card sales, the 2019 mandatory roll-out of an updated BSP reporting format (DISH 23.0) will allow Travel Agents to report having conducted transactions in such a way if they made the necessary arrangements with the GDSs supporting them.

While card schemes rule differ slightly, a merchant capable of 3D Secure at time of transaction should not receive a fraud chargeback. If he does, he has a re-presentment right allowing him to dispute successfully the fraud chargeback.

THREE: CUSTOMER RAISES A DISPUTE

The Dispute is a query about a transaction on the cardholder statement which he either does not recognize, or that he disagrees with. Common reasons for which a cardholder raises a Dispute:

- A credit has not been processed when the customer expected it would be.
- Merchandise ordered was never received.
- A service was not performed as expected.
- The customer did not make the purchase; it was fraudulent.

Did You Know

Global studies indicate that our biggest issue is the so-called **"Friendly Fraud"** or **"First Party Fraud"** (60-80% of all Chargebacks across all industries).
The other top sources of Chargebacks are: Merchant Errors (20-40%) and Criminal Frauds (1-10%)

*Source: *Understanding the Sources of Chargebacks* by Chargebacks911.

<u>So what is Friendly Fraud?</u>

The term "Friendly Fraud" is somewhat a misnomer as it trivializes actual financial losses incurred by the card accepting merchant. Visa refers to this action as "First Party Fraud", which provides an apt description of the actual event.

"In today's instant gratification society, consumers have learned that obtaining a bank-issued refund is often quicker and easier than dealing with the merchant. This abuse of the chargeback process is called friendly fraud…These customers authorized the transaction, received the purchased item with satisfaction, and later disputed the transaction"
* Quote: *Understanding the Sources of Chargebacks* by Chargebacks911.

Why?

"The real reasoning behind the cardholders' actions is likely one of the following: the consumer experienced buyer's remorse and regretted making the purchase, an authorized family member made the purchase but the primary cardholder didn't want to pay for the transaction, or the original intention was to get something for free.
Other times, friendly fraud chargebacks are the result of a misunderstanding. The consumer might have simply asked the bank about a certain charge or requested additional information about a purchase. Some consumers have admitted they mistakenly thought the bank could cancel a recurring transaction. In these situations, the bank misinterpreted the consumer's request."

Agents: A tip to help your customers (the cardholders) recognize the card transaction

Inform your customer 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.

FOUR: CARD ISSUER WILL CONTACT THE MERCHANT FOR INFORMATION TO RESOLVE THE DISPUTE RAISED BY THE CARDHOLDER.

The cardholder may initially inquire with his issuer about a transaction he does not recognize. At this stage he would not claim not having made the transaction, he is 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 a 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, he will notify the issuer that the dispute is closed. Otherwise, he may then claim he did not engage in the transaction.

Quick Win

When receiving a request for information on the transaction, it may be more efficient for the Agent to contact directly his client and ascertain what the nature of his 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 ensure he notifies his card issuer that he withdraws his inquiry.

FIVE: IF DISPUTE COULD NOT BE RESOLVED BY PROVIDING INFORMATION TO THE CARDHOLDER, IT WILL BECOME A CHARGEBACK.

Note: 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.

Step 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.

If the chargeback has been sent by the card issuer beyond the permitted period, the chargeback may be challenged as invalid.
The Airline 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.

Step 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[3]

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

Step 3: Provide useful documents to increase the chances of fighting successfully a chargeback.

On average, an Airline merchant is given 14-21 days by its acquirer to challenge a chargeback and provide any supporting documents. When required, the Airlines would in turn request the Agents to provide any missing information within 7 days (as stipulated in Passenger Agency Conference Resolution 890) to complement their reply. Given the 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);
- and route requests and responses with the greatest expediency possible.

AIRLINE

Type of information an Airline may contribute in the resolution of a chargeback

• 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

Additional information Airline can provide – Compelling Evidence.

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 traveler's name it has in its possession, and the cardholder's actual name.

When attempting to verify a cardholder's name with the issuer, when reviewing either a suspect transaction or a chargeback, one can increase the odds of getting information back by not asking what the name of the true cardholder is, but by asking confirmation if the name of the true cardholder is 'Joe Smith'.

Passenger information is only useful when the cardholder is the traveler, unless other information (such as lifted from social network) can prove a personal link between the cardholder and the traveler.

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

The examples below are some compelling evidences that historically have been used successfully to answer to a cardholder's dispute.

- ✓ Information on additional transactions connected to the disputed flight:
  The e-ticket issued for an accompanying minor (infant or child) was not disputed, while the ticket

[3] A merchant can ask the acquirer for the list of fraudulent transactions that were reported as having taken place at his business.

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.

Or

Transactions for excess baggage or seat upgrades or in-flight purchases[4], that were not disputed, allow to challenge the dispute on the flight ticket.

- ✓ Customer disputing the card transaction but not the Frequent Flyer Miles that he was 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 travelers[5]. As flight manifests are voluminous records, it is important to:
    - only provide the relevant section,
    - explain how to read the document
    - highlight the relevant sections,

  so that the provided information is clearly readable by a third party unfamiliar with the layout of such document (such as an employee of the card issuer, the cardholder or a case reviewer at a card scheme).

*NOTE: PNR or reservation information is not sufficient. Information must be obtained from flight manifest/ticket usage system once boarding pass is scanned, in order to certify that the person had boarded the plane.

AGENT

Type of information an Agent may contribute in the resolution of a chargeback

- 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; and the Agent can take the opportunity to clear up the issue and invite the customer to revert to his 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:

• Clearly Signed (if applicable) Itemized Invoice / Receipt that supports the transaction including a copy of the booking and reservation notice

• Proof of confirmation for booking or reservation

[4] If an airline completely outsources the management of in-flight purchases, it may not have access to any details of the card transactions

[5] 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 traveler's name match the name of the true cardholder, it must rely on the issuer to conduct this verification.

• 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 of the agent (who is the alleged owner of the card) and the traveler can also be sourced and provided.

• A copy of your Terms and Conditions including your cancellation, return, refund and no show policy.

Whilst providing the Terms & Conditions it is important to also provide proof that such information was provided to the customer at the time of sale. This can be achieved through several manners, a few being:

✓ 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".

✓ For telephone and face to face sales, 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.

✓ Specific to face to face sales

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.

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 in the airline industry (Universal Credit Card Charge Form), 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[6].

[6] Save rare local exceptions which rely on a single local acquirer capturing the totality of airline BSP card sales.

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 argued to be 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 there is no way of verifying the name of a cardholder in a card transaction. The billing address, however, can be verified in some cases, as mentioned in section 1.

SIX: ARBITRATION

If all possible information has been provided and if the issuer maintains the chargeback, the Airline, as any merchant, has the right to go to an arbitration phase through which 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, such procedure usually requires the loser to also forfeit to the card scheme a deposit meant to cover administrative fees. Hence this requires a party to be absolutely certain in the solidity of its argument before undergoing that final step.

SEVEN: 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.

Note that as per IATA Resolution R812, 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. The industry must work together to combat fraud and abuse.

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

1 the Agent should also request the airline to issue a complete refund[7] 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 commercial 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.

Remember that

- Even if the card refund is issued promptly, it may come too late to appear on the same cardholder statement where the original purchase transaction is posted, thus leading the cardholder to raise a dispute, as he is not aware that a card refund is 'on the way'. This is remedied with the airline proving that a full 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 remedied by showing that the amount refunded was for the full amount in the original purchasing currency.

[7] Agents can use BSPLink or GDS functionalities to issue a card refund; depending on situation, a BSP card refund may require the airline's confirmation before being completed, or may be raised immediately.

FOR ADDITIONAL INFORMATION AND RESOURCES

The sources quoted below are the most recent we found available at editing time. International card schemes are in the process of rolling out globally chargeback reforms aiming to reduce the number of incorrect chargebacks, shorten timelines and simplify processes. Hence new information may become public at any time.

Airlines- American Express Disputes Guide 2015 by American Express

Understanding the Sources of Chargebacks by Chargebacks911, http://thechargebackcompany.com/merchant-solutions/

Chargeback guide, 16/01/2018, MasterCard https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html

Visa Core Rules and Visa Product and Service Rules- 14 October 2017, https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf

Card acceptance guidelines for Visa merchants, 2017 https://usa.visa.com/dam/VCOM/global/support-legal/documents/card-acceptance-guidelines-visa-merchants.pdf

Managing payment card fraud – a guide for airlines by Visa Europe (2016 (distributed on request only)

Training courses:

http://www.iata.org/training/courses/Pages/card-fraud-prevention-talf44.aspx

Industry Fraud Prevention initiatives:

http://www.iata.org/whatwedo/airline-distribution/Pages/industry-fraud-prevention-initiative.aspx

IATA FraudClear - Review sales and flag for review the suspect ones:

http://www.iata.org/services/finance/Pages/fraudclear.aspx

IATA Perseuss - A platform to report customer data associated to card fraud, and share them with other Airlines and Agents in order to detect fraud attempts re-using data that defrauded others before:

http://www.iata.org/services/finance/Pages/perseuss.aspx