Global Airline Merchant Best Practices Guide

Global Airline Merchant Best Practices Guide

Table of Contents

Introduction

For today's Visa® airline merchant, accepting Visa payment cards has become simultaneously easier and more complex. Electronic terminals and card acceptance devices make transaction processing automatic and seemingly effortless, raising potential profitability. However, they also create increased possibilities for processing mistakes and fraudulent transactions that can result in copy requests and chargebacks.

In addition, the walls between card-present and card-absent transactions have become less obvious as growing numbers of traditional airline merchants launch e-commerce websites, transforming themselves into "click and mortar" businesses. Airline merchants must, in effect, be "bilingual"—familiar with both card-present and card-absent best practices.

The purpose of the *Global Airline Merchant Best Practices Guide* is to provide airline merchants with accurate, up-to-date information on fraud prevention while minimizing the risk of loss from fraud and chargebacks. This guide is targeted at both card-present and card-absent transactions, and includes requirements and best practices for doing business on the Internet. It also contains detailed information on the most common types of chargebacks airline merchants receive and what can be done to remedy or prevent them.

Disclaimer

The information in this guide is current as of the date of printing. However, fraud prevention best practices, and chargeback procedures are subject to change. This guide contains information based on the current *Visa Operating Regulations*. If there are any technical differences between the *Visa Operating Regulations* and this guide, the *Visa Operating Regulations* will prevail in every instance. Your merchant agreement and the *Visa Operating Regulations* take precedence over this guide or any updates to its information.

For further information about the rules or practices covered in this guide, contact your airline acquirer.

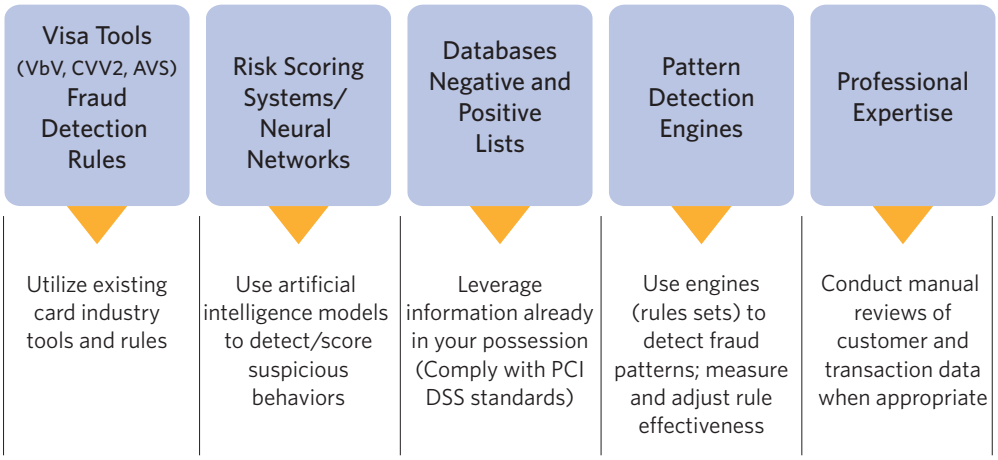
Airline Card-Not-Present Fraud Prevention and Best Practices

Introduction

Increasingly, airlines and travel services merchants are being targeted by fraud rings, as criminal groups view the airline industry's services (i.e., air travel sold online) as a valued commodity for resale on the black market. This trend has become more prevalent as airlines focus their sales efforts toward the online card-not-present sales channel. Therefore, it is important that airline merchants work with their acquirer to ensure that adequate risk controls are in place.

Many airlines use a combination of data, fraud tools, and security practices to help them manage online fraud. However, some air carriers may lack a comprehensive, layered fraud reduction strategy, creating the potential for significant financial losses.

The key to an effective and successful fraud mitigation strategy requires continuous care to track and analyze fraud trends; enhance your transaction risk indicators based on the trends and ensure risk mitigation actions are enhanced accordingly. The following depicts a model for an effective Airline card-not-present sales fraud mitigation strategy:



To help airline merchants avoid becoming the target of a fraud ring, Visa has developed a set of best practices to guide the booking of online air travel. These best practices have been organized into the three primary stages that occur during an online air travel transaction.

Best Practices for Online Air Travel Transactions

Stage 1: At Point of Booking—Website and Reservation Centers

The first step in completing an online air travel transaction begins with the booking process. At this stage, the key risk objective should be to gather information that will authenticate passenger identity, cardholder identity and prevent fraudsters from readily impersonating a legitimate cardholder or selling fraudulently purchased tickets to unsuspecting victims. Key best practices at this stage include:

- **Mandating or encouraging customer registration.** This should include gathering customer information (i.e., cardholder name, billing address, contact details, nationality, and date of birth)[1] that will allow merchants to build a comprehensive database of genuine "positive list" customers (passengers who frequently travel and do not generate fraudulent transactions) and "negative list" customers (i.e., those traveling on fraudulently purchased airline tickets). These databases can then be used to monitor transactions, reducing the impact to legitimate customers and mitigating any future fraud incidents.

  Note: All stored sensitive cardholder account information must comply with the Payment Card Industry Data Security Standard (PCI DSS) and *Visa Operating Regulations*. For more information, please visit *www.pcissc.org* or contact your acquiring bank.

- **Identify third party purchases.** Third party purchases occur when the cardholder is not part of the traveling party. Legitimate third party sales are a revenue opportunity for the airline but require stringent risk mitigation controls. However, these transactions should be carefully scrutinized because they can be a potential indicator of fraud. Criminals may use the information from a legitimate card to obtain a ticket in their own name, or for another individual that they plan to sell the ticket to for cash. Stringent passenger authentication controls should be implemented for passengers not traveling with the cardholder. Implementing the ability to identify a third party transaction prior to completing the purchase is a key step in evaluating overall transaction risk and is an important factor for merchants to input into any proprietary or commercially available risk-scoring system. In cases where high-risk transactions are involved, airline merchants may want to consider implementing additional restrictions such as allowing only retail face-to-face purchases to be made for third party tickets or excluding third party sales for short book to fly timeframes, directing the purchaser to a face-to-face payment location such as airport ticket office (ATO) or city ticket office (CTO).

- **Perform real-time authorization** whenever possible for below floor limit transactions, when transaction flagged as high risk by airline's customized risk rules.

[1] Sensitive customer information must be secured from compromise. For more information, contact your acquiring bank or refer to the PCI Data Security Standards, or visit *www.pcissc.org*.

Best Practices for Online Air Travel Transactions (continued)

- **Perform negative file check**, including listing prior fraud related chargebacks, reported fraud, etc.
- **Utilize a suite of authentication tools.** Airlines are encouraged to implement a comprehensive suite of authentication tools to make more effective transaction risk assessments and decisions. When used in a layered approach for card-not-present transactions, tools such as Visa's CVV2, Address Verification Service (AVS), and Verified by Visa can greatly reduce the incidence of fraudulent transactions and increase merchant profitability. However, no single risk tool should be considered the definitive answer to combating criminal exploitation.
  - **CVV2** [2], a 3-digit code on the back of a credit card, is a tool used to determine if the user has possession of the physical card and will effectively detect fraudulent attempts using software-generated account numbers or situations where a card number was stolen, but the card remains in the legitimate cardholder's possession. Airlines should incorporate CVV2 response codes into their overall transaction risk assessment process. "No Match" response codes coupled with other red flags may be strong indicators of a fraudulent transaction.
  - **AVS** allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available in the U.S. and Canada. The United Kingdom also supports a domestic version of this service.
  - **Verified by Visa** is an online service designed to secure Internet purchases by authenticating the cardholder's identity at the time of purchase. Additionally, Verified by Visa-enabled merchants are protected from chargebacks for Reason Code 83 (Fraud—Card Absent Environment), even when the cardholder and/or the issuing bank are not participating in the service.

    Additional best practices for CVV2, AVS and VbV include:

    - Use the CVV2 and AVS response codes correctly. Require additional checks or screening for "no match" responses.
    - CVV2 "no match" transactions are five times more risky than a transaction with a "match" response.[3]
    - CVV2 and AVS "no match" transactions are seven times more risky than "match" activity.[3]
    - Fraud on VbV fully authenticated transactions (ECI 5) is lower than on non-authenticated transactions (ECI 6).[4]

2 In some markets CVV2 is required to be present for all card-not-present transactions. Additionally, in some markets if the transaction is approved but the CVV2 response is a no match the merchant is protected against fraud chargebacks.

3 Fraud reported to Visa by issuers and sales reported via quarterly client operating certificates.

4 VisaNet settlement data CY2008

Best Practices for Online Air Travel Transactions (continued)

- **Establish a minimum time frame from the point of booking to the date of travel.** Fraudsters often exploit shortened travel windows to perpetrate fraud against unsuspecting airline and travel service merchants. Tickets purchased just before a flight may indicate fraud risk. To protect your airline from potential losses, you need adequate time to verify the validity of the customer and Visa card before travel begins. Verification may include presentment of the card at check-in, additional form of traveler identification provided at time of booking matches identification presented at check-in. Additionally, a best practice for transactions that have other identified fraud attributes is to limit the time frame for online purchases from the point of "booking" to the "date of travel" to a minimum of 48 hours to provide sufficient time for transaction monitoring and other fraud prevention measures to be completed. In some cases, (i.e., high-risk travel routes), this period should be extended to a minimum of 72 hours.
- **Publish disclaimers and risk management requirements.** Provide a notice on your website stating that any passenger found to be traveling on a fraudulently purchased ticket will not be allowed to board. Market-specific laws and penalties governing travel on fraudulently purchased tickets should also be displayed prominently.

Stage 2: Processing and Monitoring of Online Transactions

Once a booking is completed, ensure that the airline is capable of extracting relevant transaction details for analysis and risk assessment purposes. In certain cases, system adjustments may be required to allow the acquiring financial institution or Global Distribution System (GDS) to send relevant details to the airline immediately following the sale of the ticket, but prior to the flight departure date. Best practices in this area include:

- **Implementing a real time Fraud Detection System (FDS).** A real time FDS can detect high-risk transactions using previously identified fraud attributes and flag them for further action by the risk management team. This is especially useful for airlines with large e-commerce volumes because it helps ensure that transactions are monitored on a daily basis. Key risk filters that should be deployed within the FDS are:
  - Account number and IP address velocity checks
  - IP address comparative checks, compare to:
    - departure or arrival country does not match IP address
    - previous fraudulent sales made
    - multiple tickets purchased using the same account number, different routes with same dates of travel
    - multiple tickets purchased using different account numbers
    - high risk country
  - Blocks IP addresses from which fraudulent transactions or fraud-related chargebacks have previously been made
  - Previous fraud related chargeback history for the same customer

Best Practices for Online Air Travel Transactions (continued)

- Checking the passenger's name against the airline's frequent flyer data
- BIN velocity checks
- BIN country verification checks
- High-value ticket transactions
- Immediate travel tickets
- Free or anonymous e-mail accounts
- Country of e-mail or IP address vs. country of departure or country of destination
- High fraud risk flight routes
- Short book to departure time frame
- One way travel
- Ticket changes following initial purchase
- Multiple purchases on the same account in the same timeframe
- Multiple purchases on the same account through multiple channels (e.g. e-commerce and call center)
- First time customer-fraud is less likely to occur when the cardholder and merchant have a long term relationship

- **Verification against positive list and negative list.** As mentioned previously, airlines should maintain a positive list of passengers who frequently travel and do not generate fraudulent transactions. To avoid unnecessary service delays and undue expense, transactions from these customers could be routed through fewer risk filters. Similarly, a negative list of passengers and the transaction attributes (i.e., IP address, passenger name, card account number, cardholder name and e-mail addresses) of previously identified fraudulent transactions should also be maintained. Incoming fraud-related chargebacks should also be included on the negative list. Transactions with these negative list attributes should be declined or flagged for further review by your risk management staff. Airlines should also monitor transactions reported by the card issuer as fraudulent. (Contact your acquiring bank for more information.)

  Note: All stored sensitive card account information must comply with the PCI DSS and *Visa Operating Regulations*. For more information, please visit *www.pcissc.org* or contact your acquiring bank.

- **Analysis of fraud patterns.** If an automated FDS is not available, airlines should analyze fraud patterns by isolating high-risk routes, IP addresses, account numbers, and time of booking. This information can be used as a manual filter for incoming transactions, allowing stricter controls to be implemented for high-risk routes (or for transactions only). This will also help limit any reduction in sales volumes for legitimate transactions.

Best Practices for Online Air Travel Transactions (continued)

- **Shared intelligence.** Where applicable and in accordance with law, airlines should proactively share information on fraud patterns and negative list attributes with other airlines and/or acquiring financial institutions. (**Note:** card numbers may not be shared.) This will benefit the industry as a whole as crime syndicates will have greater difficulty attacking other airlines.

Stage 3: Passenger Check-in at the Airport

Controls should be implemented at airline check-in to provide a final layer of transaction authentication and to educate passengers to be wary of tickets purchased via informal channels (especially tickets offered at drastically discounted rates). For transactions identified as requiring further scrutiny at check-in key best practices at this stage include:

- **Check the physical card used for payment (also known as "card-sighting").** For online booking transactions that have been deemed or scored as high risk, determine whether or not to require a Visa card presentment at the time of travel. You can effectively manage risk by asking customers at the time of travel to present the Visa card that was used to purchase tickets through the Internet. However, this practice can lead to extreme dissatisfaction among customers who do not carry the card, have a Visa account where no card is issued, or are not aware of the policy. If you decide to require Visa card presentment, be sure that this policy is clearly communicated to customers at the time of ticket reservation and purchase. At time of check-in physically verify the payment card and ensure that proper resources and mechanisms for doing so are in place. All check-in staff must be trained to ask for the physical card and processes should be in place to ensure effectiveness. For example, equip check-in counters with "read and compare" card reader equipment so that check-in counter staff can key in the last few digits from the physical card before a passenger is checked in. Implement a process to ensure that this practice can only be overridden by an onsite supervisor.

  If you decide not to require Visa card presentment, use other fraud screening procedures instead. For example, you might require the customer at the time of travel to present identification with an address that matches the billing address.

  Note: This process should be used as an exception recognizing the manual intervention this presents to airlines automated check-in processes. All verification attempts should be made at the time of purchase. For example, if it is a third party sale and the cardholder will not be traveling, additional authentication/verification should be made online or worked by an offline process after purchase (but prior to flight departure). Airlines that participated at the Visa Airlines CNP Fraud Reduction workshop cited the implementation of a card-sighting process as an effective method for combating airline card-not-present fraud.

Best Practices for Online Air Travel Transactions (continued)

- **Provide anti-fraud publicity materials.** Education materials should be prominently displayed at the check-in area to warn passengers against purchasing tickets from unknown or informal channels. Local laws or penalties against passengers traveling on fraudulently purchased tickets should also be clearly displayed. It has been observed from previous investigations that criminal groups may loiter near check-in counters and approach unsuspecting passengers with offers of cheaper tickets purchased fraudulently over the Internet. Having ample notification of such practices, and penalties against such behavior, can potentially curb fraudulent activity.

Airline merchants are reminded that developing and implementing a comprehensive fraud prevention strategy is essential to proactively defeating fraud exploitation and reducing financial losses.

Continuous Monitoring

With knowledge, tools and continuous monitoring airline merchants can reduce their exposure to fraudulent transactions. Continuously track and analyze fraud trends. Enhance your transaction risk indicators based on the trends and ensure risk mitigation actions are enhanced accordingly.

Following are some of the key pieces of information to capture. This information can the be used post-sale for transactions flagged as high-risk to create negative lists based on various pieces of information such ticket source, e-mail address, IP address etc.

- **Track fraud by ticket source.** This practice can help you identify your airline's greatest areas of risk exposure and develop strategies to reduce risk in these areas. When tracking fraud, compare it to the volume of tickets sold by source, such as the Internet, central reservations, ticket counters, and travel agencies.
- **Track fraud by flight route.** This practice can help you identify your airline's greatest areas of risk exposure and develop strategies to reduce risk in these areas. When tracking fraud, compare it to the volume of tickets sold by source, such as the Internet, central reservations, ticket counters, and travel agencies.
- **Capture and retain Internet Protocol (IP) addresses.** It is important to know the IP addresses of the Internet Service Providers (ISPs) from which your customers make purchases. With a database of these addresses, you can develop fraud-screening tools based on transaction characteristics.
- **Capture, verify, and retain e-mail address.** During the reservation and sales process, ask the customer to provide an e-mail address. This vital link between you and the customer can be stored with other data in the booking record and customer profile for future communications, and ongoing risk analysis. Be sure to verify each e-mail address that you receive because an invalid e-mail address may be an indicator of risk.
- **Track fraud chargeback activity and use this as an additional risk filter.**

Details on Managing Disputes

This section provides an overview of the types of chargebacks most associated with airline merchants. It provides recommendations on how to best minimize the chargeback from occurring, effective dispute management best practices, how to refute chargebacks that occur.

Overview

Airline merchants tend to have higher rates of chargebacks than other merchant types, largely due to the fact that most airline transactions occur in the card-absent environment, making them more susceptible to fraud.

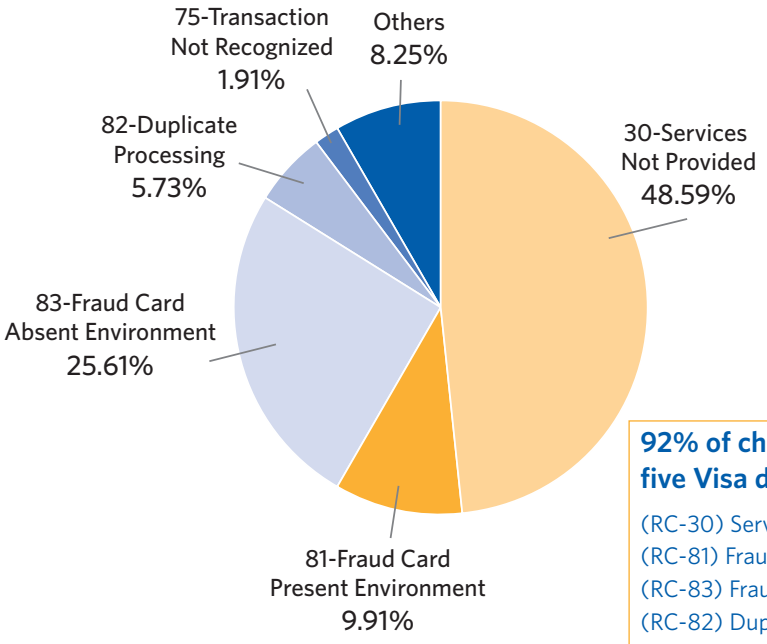
In general, chargeback activity as a percentage of sales should not vary from month to month. However, there may be seasonal fluctuations, especially during peak holiday travel periods or when an airline ceases operations.

Chargeback reason codes should be monitored; changes can indicate point-of-sale errors or procedural changes made by the merchant.

Copy Fulfillment requests from issuing banks should remain constant from month to month. Settlement data should remain consistent among sales sources.

The following charts show the top five chargeback reason codes processed by airlines.[5]

Airline Chargeback Distribution By Chargeback Reason Code Domestic Transactions

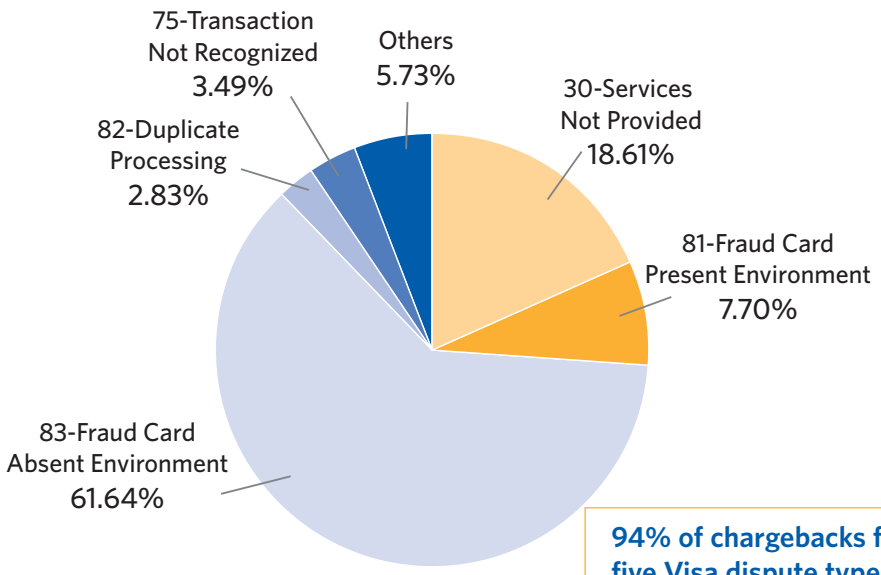


92% of chargebacks fall within five Visa dispute types:

(RC-30) Services Not Provided
(RC-81) Fraud Card Present Env.
(RC-83) Fraud Card Absent Env.
(RC-82) Duplicate Processing
(RC-75) Transaction Not Recognized

5 Average 12 months ending December 2008, based on chargebacks processed through VisaNet.

Airline Chargeback Distribution By Chargeback Reason Code International Transactions [6]



94% of chargebacks fall within five Visa dispute types:

(RC-30) Services Not Provided
(RC-81) Fraud Card Present Env.
(RC-83) Fraud Card Absent Env.
(RC-82) Duplicate Processing
(RC-75) Transaction Not Recognized

The Major Chargeback Codes

The following provides the five major reasons (on a global basis) for chargebacks of airline transactions.

Chargeback Reason Code 30—Services Not Provided or Merchandise Not Received

Chargeback for Reason Code 30 may apply if the cardholder claims that the airline merchant was unable or unwilling to provide services, or the cardholder or authorized person did not receive the service at the agreed location or by the agreed upon date. Liability may arise for airline transactions if the cardholder did not receive the airline tickets on time, or if the cardholder did not receive the service as agreed. For airline merchants, disputes for services not provided are usually caused when an airline cancels flights or ceases to provide service due to bankruptcy.

Acceptance Procedures

Proof of Delivery

If tickets are to be mailed, use certified mail or carrier's certification for proof that the tickets were delivered to the correct address and received by the cardholder. Proof of delivery information should be saved in the event of a chargeback and included in the documentation you provide in any subsequent representment.

6 Average 12 months ending December 2008, based on chargebacks processed through VisaNet.

The Major Chargeback Codes (continued)

Non-Refundable Tickets

Dissatisfied customers may attempt to chargeback non-refundable tickets. A cardholder who does not use a non-refundable ticket may claim that the services were not provided by the airline, when in fact the cardholder wants a refund or let the ticket expire without using it.

It is extremely important you provide clear disclosure of your non-refundable ticket policies to the cardholder at the time of purchase and include this information on the ticket, transaction receipt or web-site. Implement cardholder acknowledgement of the policy and store this information in the event the cardholder initiates a dispute.

Ensure your acquiring bank is aware of your non-refundable ticket policies.

Unable to Provide Services

When an airline merchant is unwilling or unable to provide services, the merchant can avoid a chargeback for services not provided by issuing a credit to the cardholder for the full transaction amount.

Note: For disputes involving non-receipt of services (i.e., airline has ceased operations or filed bankruptcy), airline merchants are required to issue credit for tickets that were sold as "non-refundable." Restrictions and limitations on refunds only apply to disputes involving buyer's remorse.

Effective Dispute Management

An airline merchant can use all the card acceptance procedures, but still receive a chargeback for Reason Code 30 with the cardholder claiming that they did not receive any services. In this case, it is important to ensure effective dispute management.

Representment

In the event that the chargeback is not valid, it is important to provide documentation that proves either:

- The cardholder received the services or
- The ticket and the services were available but the cardholder did not use the services

Evidence that the cardholder received the services may include:

- Flight manifest (matching the cardholder's name)
- Boarding pass (matching the cardholder's name)
- Additional transactions related to the ticket in dispute, such as purchase of seat upgrades, payment of extra baggage, or purchases made on board the aircraft

The Major Chargeback Codes (continued)

Evidence that the services were available, but the cardholder did not use the services may include:

- Proof of delivery showing that the ticket was received by the customer or authorized person at the address provided and on the agreed date
- Confirmation of e-ticket to an e-mail address provided by the cardholder
- Mileage credit made to the cardholder's air miles for the associated flight
- Disclosure to the cardholder that the ticket was non-refundable

Chargeback Reason Code 75—Transaction Not Recognized

Airline merchants can reduce their exposure to cardholder transaction recognition issues by ensuring transaction data is accurate and complete. A cardholder who does not recognize the transaction, based on information available on the cardholder's statement, may contact their issuer who in turn may initiate a chargeback for Reason Code 75.

Transaction Detail

Multiple Ticket Purchases

When a cardholder purchases multiple tickets with a single purchase, each ticket may appear on the cardholder statement as a separate transaction. An airline merchant can help avoid this problem by informing the cardholder at the time of the transaction how the purchase will appear on their billing statement.

Airline Ticket Number

For airline ticket sales the airline ticket number is the single most important piece of data because it enables the cardholder to provide the ticket number to the airline if they call to inquire about the transaction. Work with your acquiring bank to ensure that the airline ticket number is included in the clearing record.

Incorrect Airline Name and Location

Airlines should work with their banks to ensure their merchant name, city and state is properly identified in the clearing record. It is critical that the airline name be clearly recognizable to the cardholder. Merchant location in the transaction record should be the city and country where the transaction occurred. Ensure that this is accurately provided to your acquiring bank. For airline direct internet sales, clearly indicate the country location on the website at the time of purchase.

Transaction Amount

The transaction amount in the transaction record must be the amount approved by the cardholder at the time of purchase. For MO/TO and e-commerce transactions ensure the total amount of the purchase, inclusive of any additional charges such as airport taxes, security fees etc. is presented to and approved by the cardholder and accurately shown in confirmations and receipts.

The Major Chargeback Codes (continued)

Effective Dispute Management

Retrieval Request Fulfillment

Prior to submission of a chargeback for Reason Code 75 an issuer is required to make a retrieval request for a card present transaction, or if the transaction environment cannot be determined. If the transaction occurred in the card absent environment, then no retrieval request is required; the issuer can simply exercise the chargeback. Make sure you respond to all retrieval requests as specified in your merchant agreement. The merchant has no representment rights if the request is not fulfilled.

Visa recommends that merchants always send a response within the number of days specified in their merchant agreement to ensure acquirers have adequate time to respond to the retrieval request.

Provide all the information you have available to enable the cardholder to recognize the transaction. If the transaction was authenticated using VbV, proof of authentication or attempted authentication is not required at this stage. However, you may need to provide this proof later if the issuer challenges a completed or attempted authentication by raising a separate compliance case with Visa.

Representment

If the issuer proceeds to chargeback, it will identify the Transaction Data field(s) that is unrecognizable to the cardholder using the Member Message Text (MMT) in the chargeback clearing message.

Visa recommends that the following information be provided in the representment:

- A detailed description of the goods or services provided
- A description of how the merchant confirmed the cardholder's participation (e.g., cardholder signature, PIN, or other authentication method)
- A description of how the delivery address was confirmed, if applicable
- A copy of a transaction receipt or shipping invoice

Use the information provided in the MMT to provide any additional data needed. This must be more than was provided in the clearing message of the original presentment to resolve the chargeback. Identify any data integrity problems and take corrective action to avoid future chargebacks.

Chargeback Reason Code 81—Fraud Card-Present Environment

Chargeback for Reason Code 81 applies when a cardholder did not authorize or participate in the transaction, or the transaction was processed using a fictitious account number.

Acceptance Procedures

Imprint and Verification

Merchants that obtain an imprint and signature/PIN are protected against chargeback for fraud under Reason Code 81. The chargeback is invalid if a merchant obtains:

- An imprint and
- Cardholder verification (signature or PIN)

An imprint is card data transferred to the transaction receipt – either electronically or manually.

It is recommended that airlines use electronic card reading capability at the point of sale to produce an electronic imprint. In environments where this is not possible, a manual imprint of the card should always be obtained from the details embossed on the card.

The cardholder should always be required to sign the transaction receipt (or enter PIN if appropriate) and the signature should resemble that on the card. If the signature does not match, do not process the transaction.

If a signature is required and the card is unsigned, ask for customer's identification and ask the customer to sign the card. Check that the signature resembles that on the ID and, where permissible by law, the identification serial number and expiration date should be written on the sales draft before you complete the transaction. A refusal to sign means that the card is invalid and cannot be accepted.

Visa recommends that merchants also use the following card acceptance procedures to reduce the risk of fraudulent transactions. These procedures are especially important in environments where it is not possible to obtain an imprint or cardholder verification.

Card Security Features

Every Visa card contains a set of unique design elements and security features developed by Visa to help merchants verify the legitimacy of the card. A visual check of these features should be the first step in all card-present transactions. Any indication that a card design element or security feature is not genuine or has been tampered with is a sign that the card may be counterfeit or invalid. In such situations, ask for another Visa card for payment and follow the same procedures.

Chip Cards

If a chip card is presented and the terminal has chip reading capability, process the transaction as a chip transaction. If the terminal cannot read the chip, the chip may have been deliberately disabled. Where permitted, follow proper procedure for processing the transaction using the magnetic stripe. Check all security features and request issuer authorization.

Magnetic Stripe Cards

In some instances, the terminal will not be able to read the magnetic stripe on the card.

Card damage can happen accidentally, but it may also indicate that the card is counterfeit or has been altered. When the magnetic stripe on the card cannot be read, where permitted follow proper procedures for key-entered transactions. Check all security features, request issuer authorization and obtain a manual imprint of the card. You may not key-enter a Visa Electron transaction.

The Floor Limit

A floor limit represents the transaction value above which issuer authorization is required.

Always seek an authorization request if the transaction amount exceeds the floor limit.

Merchants should compare the card account number to the current Card Recovery Bulletin (CRB) or check the Exception File for unauthorized transactions. If the account number is listed on the CRB or Exception File, you must:

- Not complete the transaction
- Hold the card by reasonable, peaceful means
- Call your authorization center, state that the card number is on the bulletin/ exception file, give the account number and ask for instructions

Authorization Responses

If an issuer authorization is requested, evaluate the issuer's response. Proceed with the transaction if it is authorized. For authorization requests made by telephone to the voice authorization center, write the authorization approval code on the sales transaction receipt.

If the response is a 'Decline', the transaction must not be completed. If the response is a 'Referral', the issuer will seek further information. Most referrals result in an authorization, so ensure your staff contacts the issuer (by calling your merchant bank). If the response is a decline with a 'Pick Up' message, do not complete the transaction, inform the cardholder that you have been instructed to retain the card and ask for an alternative form of payment. If your staff feels this would put them under threat, it is acceptable for them to return the card to the cardholder.

The Major Chargeback Codes (continued)

Suspected Fraud

Whether or not the issuer provides an authorization, if your staff suspects fraud they should keep the card in hand and call your voice authorization center to receive instructions.

Effective Dispute Management

An airline merchant can use all the fraud risk reduction measures available, but still receive a chargeback for Reason Code 81. In this case, it is important to ensure effective dispute management.

Retrieval Request Fulfillment

Make sure you respond to all retrieval requests as specified in your merchant agreement. The merchant has no representment rights if the request is not fulfilled.

Visa recommends that merchants always send a response within the number of days specified in their merchant agreement to ensure acquiring banks have adequate time to respond to the retrieval requests.

Representment

If you still receive a chargeback and have an imprint and signature or PIN, represent immediately providing the imprint and proof of verification as proof that the chargeback is invalid.

If you receive a chargeback and believe that the cardholder did participate in the transaction, represent the transaction and include all the evidence you have that demonstrates cardholder participation.

Evidence of cardholder participation may include:

- Proof of delivery of ticket to cardholder's billing address
- A copy or record of identification provided by the cardholder at check-in (such as a passport or driver's license) and miles credit for associated flight
- Details of frequent flyer miles claimed, including address and telephone number to establish link to the cardholder
- Flight manifest (matching the cardholder's name)
- Boarding pass (matching the cardholder's name)
- Additional transactions related to the ticket in dispute, such as purchase of seat upgrades, payment of extra baggage, or purchases made on board the aircraft

Chargeback Reason Code 82—Duplicate Processing

Chargeback for Reason Code 82 may apply if the cardholder claims that they were billed twice for the same transaction.

Sales Process

Point of Sale Procedures

It is important to ensure that sales staff is fully trained on the acceptance practices that prevent duplicate transactions:

- Enter a transaction into the point-of-sale terminal only once – always balance the terminal daily to avoid any discrepancies
- Make only one imprint of the card for each transaction
- Void incorrect sales receipts and destroy in front of the cardholder

Transaction Deposit Procedures

Most global airlines have multiple acquiring bank relationships. In this case, it is critical that transaction deposit procedures do not result in duplicate deposits:

- Do not deposit the merchant copy and the bank copy of the transaction receipt with your acquiring bank
- If transactions are sent electronically for processing, ensure each batch is sent only once and as a separate batch number
- Put in place systems to ensure a single transaction is only ever deposited once to a single acquiring bank.

Multiple Ticket Purchase

When a cardholder purchases multiple tickets in a single transaction, these transactions may appear on the cardholder's statement as separate transactions. Make sure the cardholder is informed that multiple ticket purchases may be billed separately to avoid the cardholder mistakenly believing that they have been billed multiple times for the same purchase.

Transaction Detail

Ensure your acquiring bank processes all airline data providing sufficient information for the cardholder to recognize airline transactions as separate.

Effective Dispute Management

On receipt of chargeback for Reason Code 82, it is important to ensure effective dispute management.

Chargeback

If you determine that the sales receipts are duplicates and you have not yet deposited a credit to correct the duplicate, accept the chargeback. Do not process a refund (credit) now as processing of the chargeback will also debit your merchant account.

Representment

If you determine that the transaction is not a duplicate, provide your acquiring bank with evidence documenting that the two transactions are separate, or send legible photocopies of the alleged duplicate sales receipts to your acquiring bank. The receipts should clearly indicate that the two transactions are not charges for the same items or services.

If you identified a duplicate transaction and processed an offsetting refund before you received the chargeback, inform your acquiring bank of the date the refund was issued. Ensure that your acquiring bank has processes in place to deal with such situations. Many acquiring banks automatically look to see if a refund has already been processed, so you may never see these chargebacks.

Chargeback Reason Code 83—Fraud Card-Absent Environment

The online channel has been growing rapidly in the past few years and presents significant cost benefits to airlines. Visa cards are particularly suited for the sale of airline tickets through electronic commerce or telephone order. However, validating the card and authenticating the cardholder present specific challenges in the card absent environment and fraud management is a key to managing acceptance costs. Airline merchants can reduce their exposure to fraudulent transactions through a combination of Visa-provided and third party fraud management tools, and use of proper acceptance procedures.

Chargebacks for Reason Code 83 make up a significant portion of all airline chargebacks processed through VisaNet. This chargeback applies to transactions in the card absent environment when:

- The cardholder did not authorize or participate in the transaction, or
- The transaction was not authorized by the card issuer and no valid card that bears the account number was issued or outstanding

Acceptance Procedures

When processing a transaction in card absent environment, at a minimum ensure that the following information is obtained from the cardholder:

- Cardholder name as it appears on the card
- Expiration date as it appears on the card
- Cardholder billing address (the address that appears on the billing statement)
- Card Verification Value 2 (CVV2)

You must obtain an authorization for all card not present transactions. If the response to the authorization request is a decline, do not complete the transaction.

Visa Authentication and Verification Services

Visa currently provides the following services for validating the card and authenticating the cardholder in the card absent environment:

- Verified by Visa (VbV)
- Card Verification Value 2 (CVV2)
- Address Verification Service (AVS)

VbV and CVV2 are globally available services. AVS is currently available in the US, UK, and Canada.

Verified by Visa

Verified by Visa (VbV) is the best authentication method available to electronic commerce merchants. VbV also protects the merchant from chargeback for Reason Code 83 both when the cardholder is authenticated and when the cardholder or the issuer are not participating.

Card Verification Value

The Card Verification Value 2 (CVV2) is a three-digit code printed on or next to the signature panel on Visa cards. The CVV2 code helps validate that the purchase is being made with a genuine, valid card that is linked to a legitimate account.

In general, all Visa cards are required to carry a CVV2 code, however the CVV2 is not printed on some emergency replacement cards. If the cardholder is unable to provide the CVV2 code it may indicate that the cardholder has account information but is not in possession of the card itself or that the card is not legitimate.

The Visa CVV2 service allows merchants to request that the issuer validate that the CVV2 is correct. Regardless of the CVV2 verification response received from the issuer, if the issuer provides a negative response to the authorization request, do not complete the transaction.[7]

Address Verification Service (AVS)

The Address Verification Service (AVS) allows merchants to validate the cardholder's billing address with the issuer. The service can help merchants determine the validity of the cardholder and should be used in combination with CVV2 to reduce the risk of fraudulent transactions.

Additional Risk Indicators and Airline Merchant Measures

Risk Indicators

Visa recommends that airline merchants use Management Information System (MIS) reporting, including historical sales and chargeback information on an ongoing basis to track and analyze fraud trends. Results of the analysis can be used by the airline to initiate additional checks to reduce their risk exposure.

7 For some regions, if the transaction is authorized, but the CVV2 does not match, the merchant is protected from Fraud Chargebacks. Acquirers in each region are advised to check with their Visa regional office regarding this liability shift.

The Major Chargeback Codes (continued)

Additional risk indicators for airline merchants may include:

- Larger than normal ticket value
- Multiple purchases conducted on one card over a short period of time
- Immediate travel tickets
- Multiple cards used from a single IP (Internet Protocol) address
- Departure or destination country does not match IP (Internet Protocol) address
- Tickets purchased for travel on high risk route based on previous fraudulent transactions
- Previous chargeback history for the same cardholder
- Cardholder fails frequent flyer or loyalty club screening
- Account listed on a negative file
- First time customer - fraud is less likely to occur when the cardholder and merchant have a long term relationship

Preventive Measures

If a transaction triggers one or a combination of high-risk indicators, additional measures may be required, including:

- Requesting the card at check-in[8]
- Requesting photo ID showing billing address at check-in
- Confirming the purchase with the cardholder:
  - For high priced tickets consider calling the cardholder to confirm the purchase
  - For future travel mail confirmation of the sale to the cardholder
- Routing a high risk customer to a low risk sales channel, such as face-to-face environment
- Requesting another Visa card

Effective Dispute Management

An airline merchant can use all the fraud risk reduction measures available, but may still receive a chargeback for Reason Code 83. In this case, it is important to ensure effective dispute management.

Retrieval Request Fulfillment

Make sure you respond to all retrieval requests as specified in your merchant agreement. The merchant has no representment rights if the request is not fulfilled.

Visa recommends that merchants always send a response within the number of days specified in their merchant agreement to ensure acquiring banks have adequate time to respond to the retrieval requests.

8 Not all Visa accounts have a physical card.

The Major Chargeback Codes (continued)

In order to prevent a subsequent chargeback, provide all transaction details available including passenger name and flight details. If the transaction was authenticated using VbV, proof of authentication or attempted authentication is not required at this stage. However, you may need to provide this proof later if the issuer challenges a completed or attempted authentication by raising a separate compliance case with Visa.

Representment

If you receive a chargeback and believe that the cardholder did participate in the transaction, represent the transaction and include all the evidence you have that demonstrates cardholder participation.

Evidence of cardholder participation may include:

- Proof of delivery of ticket to the cardholder's billing address along with AVS match for same address
- A copy or record of identification provided by the cardholder at check-in (such as a passport)
- Details of frequent flyer miles claimed, including address and telephone number to establish a link to the cardholder
- Flight manifest (matching the cardholder's name)
- Boarding pass (matching the cardholder's name)
- Additional transactions related to the ticket in dispute, such as purchase of seat upgrades, payment of extra baggage, or purchases made on-board the aircraft

Additional Information

Please contact your acquiring bank for more detailed information regarding the practices and Visa tools referenced in these guidelines, including Visa acceptance procedures, AVS, CVV2, VbV, and Visa dispute management.

Chargeback Handling

Many airlines manage the cost of chargebacks by attempting to respond to their acquirers with information supporting the charge. It is crucial that the acquirer and the airline be familiar with Visa rules pertaining to chargebacks and the airline's business practices. Acquirer's must recommend business process changes where appropriate and acquirers must help the airline focus the airline's staffing efforts on chargeback types that can truly be reversed. To maximize efficiency in resolving these issues, many airlines automate this process through the use of web-based tools.

Common Best Practices

- **Clearly display your change fee policy and pricing.** You can reduce customer inquiries and disputes by informing your customers in advance of the terms and conditions of your change fee policy and the amounts of fees that will be assessed if booked itineraries are changed. This information should be prominently displayed on your website so that customers can review it before purchasing tickets.
- **Display refund rules on both your booking and confirmation pages.** This practice can help you preserve customer relations in cases where customers cancel their flights. By showing refund rules on your confirmation page, as well as on your booking page, you can educate customers about the refund policy prior to ticket purchase and then reinforce this policy after the booking has been made.
- **Clearly disclose all terms and conditions of the sale.** Before making the decision to buy, your customers should know all of the terms and conditions of the booking at hand. Always tell your customers the following details:
  - The amount of an itinerary change fee
  - How the fee will appear on the cardholder's statement (in total or billed separately)
  - When the fee will be billed
  - What name will appear on the cardholder's statement

  By clearly disclosing this information, you can ensure quality of service and avoid unnecessary customer disputes later. For best results, require the customer to "click and accept" the disclosure statement displayed on your site.
- **Clearly disclose all policies for baggage and any other ancillary fees.** You should also explain when and how the fees will be collected.
- Respond to all request for copies in a timely manner, and in accordance with your merchant agreement.
- Consider representing any fraud chargeback with compelling or preponderance of evidence of cardholder participation.
- Ensure sales and back office staff are trained in all aspects of transaction acceptance, including Visa risk tools, acceptance procedures and the Visa dispute management processes to maximize opportunities staff training .

Internet Disclosure Best Practices

- Visa considers a "click to accept" or other affirmative button the cardholder must select as full disclosure of refund policies for electronic commerce transactions.
- Refund policy must be shown during the purchase process.
- The refund policy must be displayed:
  - on the same screen view as the checkout screen used to present the transaction details, or
  - within the same sequence of web pages the cardholder accesses during the checkout process
- Refund policy cannot be a separate link.
- The website must have either a "click to accept" button, or the cardholder can type in is or her initials to accept the refund policy.
- The refund policy cannot be bypassed and must be accepted before the transaction is completed and payment is processed.

Merchant Outlet

An Electronic Commerce or Mail/Phone Order Merchant must disclose the Merchant Outlet country at the time of presenting payment options to the cardholder. By disclosing the Merchant Outlet country the merchant will reduce cardholder inquiries related to the transaction when posted to the cardholder's statement.

Transaction Receipt Retrieval Process

The transaction receipt retrieval process allows an issuer to request a copy of a transaction receipt for a cardholder or for dispute resolution purposes. When an issuer makes a retrieval request, the merchant must fulfill the request with a copy of the actual receipt used to complete the transaction, or a substitute document that provides specific information about the transaction.

Airline Measures

Make sure you respond to all retrieval requests as specified in your merchant agreement. When a merchant fails to fulfill a retrieval request within Visa required timeframes, the issuer may exercise a chargeback and depending on the chargeback reason, the merchant forfeits its representment rights to refute the dispute.

Research indicates a strong correlation between low retrieval fulfillment rates and high fraud chargeback rates. Responding to retrieval requests in time will help prevent subsequent chargebacks and reduce back-office airline disputes.

Transaction Receipt Data Requirements for Airline Merchants

When an airline merchant receives a request for a transaction receipt, it must fulfill the request with either a copy of the original transaction receipt or a substitute transaction receipt.

The substitute transaction receipt must contain the following data:

- Account number
- Cardholder name, if applicable
- Passenger or guest name, if different than the cardholder name
- Address where tickets were sent (if available and applicable)
- Transaction date
- Transaction amount
- Authorization code, if applicable
- Travel agent name and address, if applicable
- Flight information

In case of an electronic commerce transaction, the substitute transaction receipt must contain the following data:

- Account number
- Cardholder name
- Transaction date
- Transaction amount
- Transaction currency
- Authorization code
- Merchant name
- Merchant location
- Description of services

Visa Support Services and Resources for Airline Merchants

The Visa resources listed in this section can be used to help educate your customer service associates and provide additional program information to meet the global needs for the airline industry.

The Visa International Airline Program

The Visa International Airline Program (IAP) allows cross border acquiring for an International Airline*. This provides the airline with the opportunity to consolidate their Visa contract and deposit relationships in one or a limited number of Acquirer locations. Through consolidation of acquirer relationships benefits to the airline include:

- Increased flexibility in contracting, deposit and settlement services
- Improved efficiency
- Reduced administrative costs
- Streamlined back office processes
- Enhanced service to customers

* An International Airline either:

- sells tickets directly in 2 or more countries, or operates scheduled flights between 2 or more countries, or both
- its authorized agent that sells airline tickets on behalf of the Airline

For more information regarding the IAP program, contact your airline acquirer.

Training Materials

For global merchant publications, please visit your respective regional website at *www.visa.com*. The materials that follow are available for merchants that support U.S. domestic transactions:

Card Acceptance Guide for Visa Merchants

The Card Acceptance and Chargeback Management Guidelines is a comprehensive manual for all businesses that accept Visa transactions. The purpose of this guide is to provide merchants and their sales staff with accurate, up-to-date information on processing Visa transactions, while minimizing risk of loss from fraud and chargebacks.

VRM 07.31.08

E-Commerce Merchants' Guide to Risk Management

This 106-page book features risk management best practices for selling goods and services on the Internet. It covers a range of topics including e-commerce start-up, website utility, fraud prevention, Visa card acceptance, cardholder information security, and chargeback handling and loss recovery.

VRM 08.01.08

Protect Your E-Commerce Channel Against Fraud

This three-fold brochure is a fast and easy reference for Internet merchants. It contains best practices to help prevent fraud and fraud-related losses for online transactions.

VRM 03.15.07

Point-of-Sale Reminder Card

Designed for use at the point of sale, this six-panel card helps sales staff remember the correct steps for accepting and processing Visa cards.

VRM 09.08.07

Visa USA website (www.visa.com/merchant)

This website links to a comprehensive range of products and services for Visa merchants.

To order any of the training materials listed in this chapter, call Visa Fulfillment at (800) VISA-311 or visit *www.visa.com/merchant.*

Glossary of Terms

Agent	Travel agent or airline employee responsible for distributing an airline ticket or service.
Address Verification Service (AVS)	The method by which a merchant transmits address data to an issuing bank, which responds with a "match", "partial match", or "no match". Airlines and travel agents in some countries use AVS to help ensure transaction validity in ticket-by-mail (TBM) sales, although AVS is not widely available for CRS transactions.
Airline Reporting Corporation (ARC)	Owned by U.S. airlines, the ARC establishes policies and procedures for the travel agency community in the U.S. Its Board is comprised of airline marketing senior managers. The ARC is responsible for all billing and reporting of travel agency sales activity from CRS vendors in travel and entertainment (T&E) markets.
Airport Ticket Office (ATO)	Ticket counter or gate where transaction processing takes place for airline direct sales.
ARC	See *Airline Reporting Corporation*.
City Ticket Office	Airline sales offices located in buildings and hotels where direct sales occur.
Computerized Reservation System (CRS)	A reservation system owned and run by an airline or third party processor that handles the airline's inventory of seats, reservations, and card transactions for direct ticket sales.
CRS	See *Computerized Reservation System*.
CTO	See *City Ticket Office*.
Electronic Ticket/ E-ticket	Most airlines refer to an electronic ticket as an "E-ticket". With an E-ticket, a paper ticket is not generated for the passenger; instead, an electronic Passenger Name Record (PNR) is generated in the CRS. With E-tickets, the airline benefits from reduced distribution costs (i.e., no ticket stock, reduced necessity of customer having to go to a travel agent). E-tickets also have the potential to reduce fraud by preventing the on-selling of tickets; however, they also remove such safety measures as ensuring that a ticket booked by phone or over the Internet is only delivered to the cardholder's verified address. Given that there is no signed transaction receipt or T&E document, there is less protection if a chargeback occurs.
Global Distribution System (GDS)	GDSs handle reservation activity for the T&E industry. First initiated by the airlines, GDSs have since expanded into reservations for car rentals, hotels, and cruises. Eighty-five percent of all travel agent activity is handled via a GDS. Each GDS seeks authorization directly through a dedicated Base I VAP and transmits billing files to the ARC or to an appropriate BSP.

Passenger Name Record (PNR)	Reservation data held by a CRS on an individual reservation record level. Used by airlines to drive automated tickets on the CRS and to store historical data on traveler and individual flights.
Refund	Refunds granted directly from the airlines are transmitted daily with the carrier's direct sales activity. Refunds from travel agents go through the ARC or BSP reporting process. The latter process can result in lengthy refund processing time frames.
T&E	Acronym for "travel and entertainment".
Ticket Number	A 13-digit number commencing with a code denoting the issuing carrier, followed by a number unique to that ticket. Found in the PNR and TCN records, Visa requires the acquirer to insert the ticket number in the last 13 places of the Merchant Name field in several regions in order to qualify for a preferred airline IRF rate.
Visa Access Point (VAP)	Computer software that allows a U.S. processor, merchant, or Visa member access to VisaNet. **Note:** The functionality of GDS VAPs is restricted to seeking authorization.