ARC's Guide to Travel Agency Payment Card Acceptance, Risk Mitigation and Chargeback Management

A concise guide with useful advice, best practices and practical examples for travel payment professionals

Excerpted from Section 6 of the Industry Agents' Handbook (IAH)

ARC

Introduction

ARC has created this reference document to help travel agencies better navigate the industry's latest payment card acceptance, risk mitigation and chargeback management procedures. Whether you are new to the air travel industry or a seasoned expert, this valuable resource will help you and your agency:

- Develop a best practice mindset on payment acceptance procedures, including the handling and collecting of credit card information
- Learn how to make informed decisions about payment acceptance and managing the associated risk of fraud
- Get tips on how to effectively respond to and manage chargebacks

The contents of this guide have been excerpted from Section 6 of the Industry Agents' Handbook (IAH), pages 153–164, which outlines the responsibility of ARC-accredited agencies when accepting payment cards (credit, debit and charge cards) on behalf of ARC participating airlines. This section frames the expectation for ARC participating airlines and agencies when managing chargebacks procedures, best practices on payment card acceptance and risk management. To view this section or the full IAH, click here.

Please note that this guide will be updated by ARC as new technology, procedures and best practices are introduced or when payment card company rules change.

It is highly encouraged that you share this guide with your staff so you all can become familiar with the latest payment card acceptance and chargeback management procedures.

Table of Contents

Part 1: Payment Card Acceptance Procedures

Overview

The goal of Section 6 of the handbook is to:

- Outline the responsibility of ARC accredited agents when accepting payment cards (credit, debit, charge cards) on behalf of ARC participating airlines;
- Outline expectations for ARC participating airlines and agents when managing chargebacks;
- Provide best practices for card acceptance and the associated risk of fraud, and for chargeback management.

The procedures are based on payment card company rules for card acceptance and chargeback management in the travel industry. These procedures will be updated as new technology is introduced or payment card company rules change.

To reference terms in this document, search ARC's industry glossary.

The following outlines procedures for agents accepting payment cards on behalf of ARC participating airlines:

- Determine if the airline accepts the payment card provided by the customer and under what conditions. The Credit Card Acceptance Chart provides detailed airline card acceptance information. Given that the airline accepts the form of payment, travel agents must honor any payment card brand presented. Discrimination among payment card brands is prohibited.
- Validate the card expiration date and effective date, when available. Cards may only be accepted when they are active.
- Identify the ticketing airline and, at the time of ticketing, obtain an authorization (i.e., approval code) via the GDS for the exact amount of the transaction. Transactions that are not properly authorized may not be settled successfully and, as a result, the airline may not be paid. In addition, the airline could be subject to increased card acceptance costs or non-compliance fees, in which case the airline may contact the agent for reimbursement.
    - It is important to note that when doing a Travel Agency Service Fee (TASF) along with a ticket, two separate authorizations must be obtained.
    - When presented with an Alaska Airlines Commercial Card(AS), agents should call the AS voice authorization center at (206) 392-7720 to obtain an approval code. Please note that 50% of the total fare value must be on Alaska Airlines.
    - For ghost card accounts (aka, corporate accounts), travel agents must obtain identification from unknown customers and confirm that the customer is authorized to use the account.
- Process tickets issued against payment cards through Interactive Agent Reporting (IAR) in accordance with the procedures outlined in the Industry Agents' Handbook (IAH).
- Validate the identity of the cardholder, ensure that the cardholder has knowledge of and is participating in the transaction, and retain documentation demonstrating this in case of a chargeback. In the travel agency distribution channel, there isn't a way to absolutely validate that the cardholder is who they say they are and collect the evidence required to demonstrate this was done. Therefore, it is very important to review best practices for card acceptance.
- Clearly and concisely disclose applicable terms and conditions of sale (e.g., deadlines, penalties

and/or fees for canceling, refunding, or exchanging tickets) to the cardholder prior to completion of the sale. In the event of a service or refund related chargeback, retain proof that the terms and conditions of the sale were disclosed and accepted. Additional information about disclosure of terms and conditions is provided under best practices in this section.

- Keep payment card information secure and in compliance with Payment Card Industry Data Security Standards (PCI DSS). Travel agents must not disclose to, or otherwise give, any third party the name or account number appearing on any card, except as may be necessary for a travel agent to successfully settle and support the transaction as outlined in the Agent Reporting Agreement (ARA).

It is important for agents to follow the above procedures. If the procedures aren't followed, airlines may not be able to obtain payment from the payment card companies, which may result in fees associated with improperly authorized transactions or in a chargeback. The agent is financially responsible for the sale, associated fees and chargebacks.

To summarize, given the challenges in the travel industry with validating the identity of cardholders, agents are encouraged to review best practices for card acceptance risk management, and chargeback management. This information will help identify ways to attempt validation of the cardholder identity and obtain proof that the identity of the cardholder was validated in the event of a chargeback. The goal of the best practices outlined in this section is to help agents create a fraud prevention strategy and identify opportunities to obtain necessary documentation to reverse a chargeback should there be a claim of fraud or a dispute over the terms and conditions of the sale.

Types of Payment Cards

The following is a list of the payment cards processed by ARC and their respective two-character designator:

AS	Alaska Airlines Commercial Card
AX	American Express
CA	Mastercard
DS	Discover/Diners Club International
JC	Japan Credit Bureau (JCB) International
TP	Universal Air Travel Plan (UATP)
VI	Visa

Airline Payment Card Acceptance Chart

The Payment Card Acceptance Chart shows the acceptance of various payment cards by each ARC participating airline. The chart also shows the restrictions some airlines have for accepting payment cards on their behalf. A blank box indicates that the airline does not accept the payment card. The definition for each code immediately follows the chart. In some cases, the letter "**E**" follows the acceptance code. This means the airline accepts the payment card with additional exceptions to the acceptance criteria. The additional airlines' exceptions, when applicable, are listed immediately following the definition of the applicable code.

Agents should refer to the Airline Payment Card Acceptance Chart to ensure instructions are followed when accepting payment on behalf of airlines.

Please click here to view the Credit Card Acceptance Chart

Part 2: Chargeback Management Procedures

Under the Fair Credit Billing Act (FCBA), consumers in the United States are protected against "inaccurate and unfair credit billing and credit card practices." Therefore, cardholders not involved in a transaction billed to their account, or who did not receive the product or service promised, have the ability to initiate a dispute on a transaction or "charge- it-back." As a result, merchants* (airlines and their agents) must engage in a process to respond to chargebacks or risk financial responsibility for the associated loss.

When a cardholder initiates a chargeback, the dispute is submitted to the airline's payment processor who works with the airline to obtain the information necessary to support the transaction. The information provided must prove that the actual cardholder participated in, and/or authorized the transaction. Airlines maybe in the best position to respond to some chargebacks types (e.g., fraud or services not rendered) because they may have proof that the cardholder took the flight. If other evidence is required to attempt a chargeback reversal, the airline is expected to contact the agent prior to the close of the chargeback response window to obtain additional information about the customer and the transaction.

Agents are encouraged to review the best practices for chargeback management in this section to determine what documentation to provide the airline, and therefore the payment processor, to have the best chance to reverse a chargeback. Payment card chargeback response timeframes vary by payment card company. Therefore, to have the best chance of success in defending against a chargeback, agents are encouraged to immediately respond to airline requests for supporting documentation and no more than five days from receipt of notice.

* For purposes of this section, the merchant is the entity accepting the payment card for goods or services

How to Respond to a Chargeback

The payment card companies have regulations and requirements for the supporting documentation necessary to successfully dispute chargebacks. In addition, they allow for “compelling evidence” to be provided by the merchant for consideration in a chargeback dispute. For a fraud chargeback claim, merchants must provide proof that the cardholder was involved in, and authorized the transaction. For service related chargebacks (e.g., refund not received or services not rendered), proof that service was provided or that the terms and conditions of the sale were accepted prior to the transaction taking place is required.

When responding to chargebacks, in an attempt to reverse the chargeback, agents are encouraged to provide documentation that demonstrates:

1. The identity of the cardholder was validated;
2. The cardholder authorized the transaction;
3. The terms and conditions of the sale were accepted by the cardholder.

Obtaining proof demonstrating that these three things were done is very challenging for merchants, particularly in the travel industry, and there is no guaranty that the documentation will resolve the chargeback. Additional information about responding to chargebacks is included in Best Practices for Chargeback Management section below.

If the airline is unable to obtain a reversal of the chargeback from the payment card company, the agent assumes financial responsibility for the debit memo issued as a result.

Part 3: Best Practices for Card Acceptance and Risk Management

This section provides information to help agents make informed decisions about payment card acceptance and the associated risk of fraud. The best way to reduce the risk of fraud is to "know your customer" and to know the behavior of typical customers to the agency. When a customer is someone unknown, or falls outside the typical pattern, it can be a red flag depending on the agency business model. A red flag means additional verification will help in making an informed decision about accepting a transaction. Most agents don't know all of their customers, so agents are encouraged to put tools in place to collect information that assists in validating the identity of the cardholder and assesses the risk of fraud. This can be challenging in a card-not-present environment in general and particularly in the travel industry.

Travel agents and airlines sell services, so unlike a traditional retail merchant that sells shoes or electronics, there isn't a product to mail to the cardholder address. Mailing tangible goods to the cardholder is one way to demonstrate that the cardholder was involved in the transaction, but with e-tickets this option isn't available. Additionally, global distribution systems (GDSs) don't make credit card terminals available to travel agents in the U.S. In a brick and mortar retail environment, credit card terminals are available so electronic information can be collected via a "chip" card as proof that the card was present and valid. Because these tools aren't available in the travel agency distribution channel for airline ticket sales, agents aren't able to fully validate that the card was present and valid. Finally, the infrastructure to support 3-D Secure (Verified by Visa, MasterCard Identity Check, Discover ProtectBuy) isn't available via the GDSs, which means that online travel agents (OTAs) are unable to authenticate the cardholder identity and receive the associated protection against fraud chargeback claims. Additional information about 3-D Secure follows.

Validating the Cardholder – Card-Not-Present

The large majority of transactions in the travel agency distribution channel are card-not-present, which makes it challenging to validate that the customer is the cardholder and increases the risk of fraud. Agents are encouraged to have a risk management strategy in place to help manage the risk of fraud. The first step to creating a risk management strategy in a card-not-present environment is to become knowledgeable, or have someone within your organization that is knowledgeable about fraud prevention and the tools available to manage the risk of fraud. It is important to be aware of current trends and tactics used to perpetrate fraud, so the strategy can be consistently updated. The challenge for travel agencies is to weigh an acceptable level of risk against potential negative impacts (i.e., friction) to the customer.

Because liability for card-not-present transactions falls on the merchant (airline, and therefore, travel agent), many travel agents and airlines have developed sophisticated systems to manage risk. These systems generally include the following to assist the agent in making decisions about whether or not to accept a transaction:

1. The use of several (industry average is seven to nine) payment card company fraud management tools (e.g., Address Verification Service, CID validation) along with other third party tools available to manage risk (e.g., email validation tools, negative list tools, issuer fraud information, IP geolocation, device fingerprinting, machine learning technology);
2. Data about the cardholder and the transaction (e.g., time to travel, cardholder location, previous experience with the customer);
3. A transaction-scoring tool that ties the various data points together.

While fraud detection technology continues to evolve, this approach has become a best practice for managing the risk of fraud. The information that follows describes some of the tools that can be used to manage the risk of fraud and chargebacks. The use of these tools does not protect the agent from loss if a chargeback is received, but they are helpful to evaluate the risk of fraud.

In addition to managing the risks associated with payment fraud, agents should consider what information to collect about the customer or cardholder and the transaction in the event of a chargeback or a need to collect payment directly from the customer following a chargeback. This includes data such as proof that the terms and conditions of the sale were accepted by the cardholder and full address and contact information in the event a chargeback is received and the customer needs to be contacted.

Address Verification Service (AVS)

Address Verification Service (AVS) is a tool offered by American Express, Discover, Mastercard, Visa, JCB and Diners Club International. It allows merchants to verify that the numbers in the billing address provided by the customer match the billing address associated with the card. AVS can be an effective tool for validating customer identity because, in many instances, individuals perpetrating fraud do not know the customer billing address. However, it is important to note that in some cases individuals perpetrating fraud may know the customer billing address. Therefore, using AVS does not provide a merchant with protection against fraud or chargebacks.

AVS is available through the following GDSs by card type (Note that these tools may not be available on all platforms within the GDS; therefore, to obtain information about the availability of these tools on specific platform, contact the GDS):

GDS	American Express	Diners Club International	Discover	JCB	Mastercard	Visa	UATP
Amadeus	X		X		X	X	
Farelogix	X		X		X	X	
Sabre	X		X		X	X	
TravelPort	X		X		X	X	

Card Verification Number – Unembossed Number on Card

Visa (CVV2 - Card Verification Value 2), Mastercard (CVC2 - Card Verification Code 2), Discover (CID - Card Identification) and American Express (CID – Card Identification) each provide a valuable service that allows agents to validate the unembossed code (three or four digits) on a card. Validating that the unembossed number on the card matches the number associated with the card attempts to demonstrate (but isn't proof) that the customer has a valid card in his/her possession. This prevents individuals with stolen payment card numbers from using the numbers to make fraudulent purchases. This tool has been proven to be a valuable risk management tool; however, as with AVS, using CID, CVV2 or CVC2 does not provide protection against chargebacks. The following is an example of how CID is represented on a Discover card. It is similar with other cards, but as shown in the case of American Express, the CID is often on the front of the card.

Note: Never write down or retain the unembossed number associated with a customer's card.

Where is the Card Identification Data (CID)?

CID, CVV2 and CVC2 are supported by the GDS for the following card types (Note that like AVS, these tools may not be available on all platforms within the GDS; therefore, to obtain information about the availability of these tools on specific platform, contact the GDS):

GDS	American Express	Diners Club International	Discover	JCB	Mastercard	Visa	UATP
Amadeus	X		X		X	X	
Farelogix	X		X		X	X	
Sabre	X		X		X	X	
TravelPort	X		X		X	X	

Enhanced Payment Card Authorization

All payment card companies require merchants to obtain a payment card authorization for every transaction in the travel industry. In the travel agency distribution channel, authorizations are obtained via the GDS at the time of ticketing. Standard card authorization procedures are outlined in the Card Acceptance Procedures.

A standard authorization generally validates that the card number is valid and that the funds (i.e., "open to buy") are available on the account. American Express and Discover offer an enhanced authorization service that will allow a merchant to validate additional information about the cardholder. The following are phone numbers agents can use to obtain additional information about cardholders.

American Express **1 (800) 528-2121**

The American Express Voice Authorization Service offers the ability to verify information about the cardholder including cardholder name, street address, zip code, and phone number. To use the service, have the card number and the information to be verified. The system has intuitive prompts to walk through the validation.

Discover Network **1 (800) 347-1111**

The Discover Voice Authorization Service offers the ability to validate the Card Identification (CID) on the back of the card and to conduct a cardholder name verification. To use CID, have the three-digit code on the back of the card available. To use the cardholder name verification option, have the cardholder's first and last name.

When calling the Discover Voice Service, have the following information available and follow the voice prompts:

1. Merchant number: 6011 0160 1101 601
2. Card account number
3. Card Identification Data
4. Expiration date
5. Transaction amount

3-D Secure — On-line fraud management tools (Verified by Visa, MasterCard Identity Check, and Discover ProtectBuy)

The major payment card brands offer on-line merchants a tool called 3-D Secure, however only Visa, Mastercard, and Discover offer the tool for use through the travel agency distribution channel for airline ticket transactions. 3-D Secure allows on-line merchants to authenticate the identity of a cardholder through a cardholder-generated personal identification number (PIN), a one-time use code or other identifying information associated with the account. While the underlying technology of each system is called 3-D Secure, it is uniquely marketed by each card brand.

3-D Secure is available for on-line merchants with a direct interface to the customer. This means that the cardholder must be the one directly inputting the payment card information into the merchant website. 3-D Secure works by authenticating the cardholder on the merchant website through an interface between the cardholder and the entity that issued that card (e.g., card issuing bank, Discover). Online merchants that use 3-D Secure use third-party authentication providers, to directly interface with the card issuer so the cardholder can authenticate themselves.

The benefit of 3-D Secure is that when authentication occurs, or is attempted, merchants are protected if a cardholder claims the transaction was fraudulent. In other words, the liability for the fraud chargeback loss is taken by the card issuer rather than the merchant. For 3-D Secure to work in the travel agency distribution channel, infrastructure changes by online travel agents (OTAs), GDSs, ARC and payment card processors are required. ARC has made the necessary infrastructure changes to support 3-D Secure. Travel agents interested in using 3-D Secure are encouraged to contact their GDS representatives to request the that changes are made to support their needs. For additional information, please contact the ARC payments team at creditcardservices@arccorp.com.

Transaction Evaluation and Scoring Tools

Many merchants effectively manage their fraud risk through the use of transaction-scoring tools that analyze information available at the point of sale to identify transactions that appear high-risk. Some agents develop tools internally while others partner with third party providers of fraud scoring tools. Real-time (or near-real-time) transaction-scoring tools use four key sets of data to analyze risk:

1. Existing payment card company tools like AVS and Card Identification (i.e., Card Identification Code, Card Identification Value);
2. Data about the customer and cardholder, such as where they are located, who they are, how they behave online, previous experience with the customer and any additional data points, to attempt validation that the cardholder is the customer and they are who they say they are;
3. Data about the transaction including origin and destination, timing and class of service;
4. Data about the point of sale including card present versus card not present and the type of business typically done by the agency (e.g., international travel, corporate travel, domestic travel, specific destinations).

Analysis of this data provides merchants with information to manage risk. Scoring tools use the data available to expedite the processing of low-risk transactions and flag high-risk transactions for further analysis. Fraud scoring providers generally offer a user interface the merchant can use to quickly analyze high-risk transactions. Many of the largest travel industry merchants use fraud scoring tools, along with a set of other fraud prevention tools and tactics to identify and reject fraudulent bookings.

Risk Management for Corporate Relationships

Fraud against Travel Management Companies (TMCs and agents that manage corporate accounts) has grown in recent years as social engineering schemes have become more sophisticated. Fraudsters often manipulate agents managing corporate travel accounts by posing as an employee of the corporation. Agencies that manage corporate travel accounts need to have procedures in place to ensure that agents validate they are ticketing for the actual corporate customer. The following are tips to reduce the risk of fraud tied to managing corporate accounts:

1. Keep informed of the latest fraud schemes targeting TMCs;
2. Identify typical travel for a corporate customer and flag tickets that fall outside the normal pattern;
3. Verify referrals with the corporate client, particularly when travel patterns change;
4. Directly verify the telephone number of the caller with the contact at the corporate client;
5. Pay particular attention to transactions for passengers without existing profiles;
6. Make sure after-hours staff are aware of and closely follow procedures.

Validating the Cardholder – Card-Present

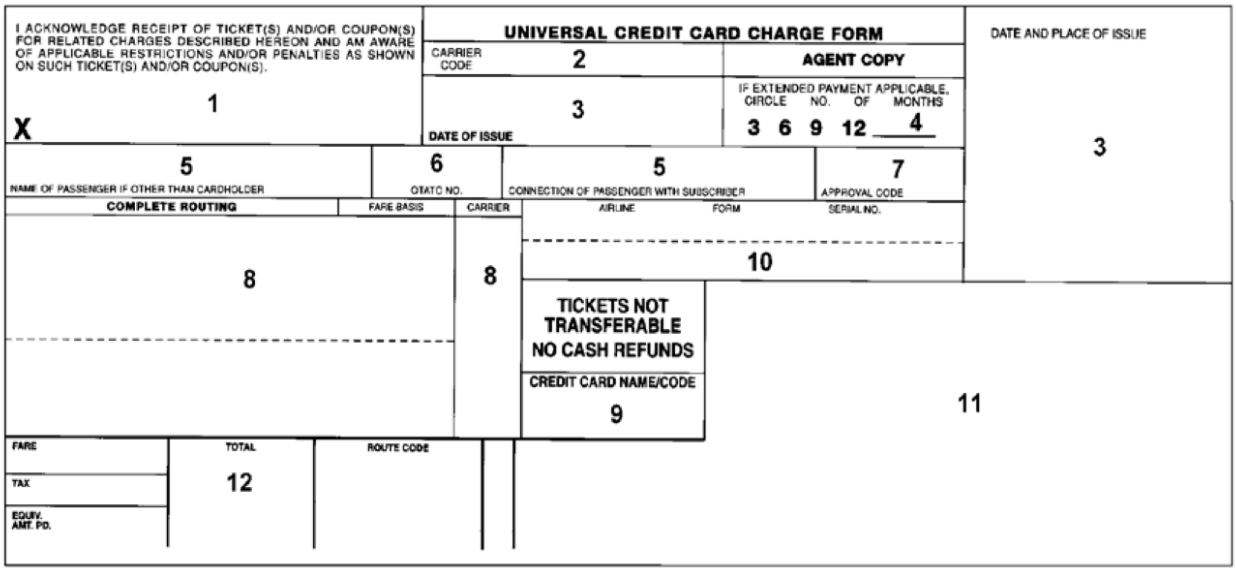
A small percentage of transactions take place face-to-face, and card-present fraud (aka counterfeit, lost/stolen) rates are low, however whenever accepting payment cards in a face-to-face environment, it is important to attempt validation of the cardholder identity and retain information about the cardholder that provides proof in the event a chargeback is received. To do this in an environment where the card is present, a chip card reading terminal is required. Given that the GDSs don't do not currently make card terminals available to support airline ticket sales through travel agents, the only way to demonstrate that the card and cardholder were present is to obtain a signed and imprinted Universal Credit Card Charge Form (UCCCF).

With the growth of Europay, Mastercard and Visa (EMV) chip card technology in the U.S., a manual card imprint on a charge form no longer meets the burden of proof that the card is valid if the cardholder claims fraud and therefore disputes the charge. In other words, a signed UCCCF is no longer considered proof that the cardholder is present and the card is valid. Payment card company rules state that liability for card-present fraud (i.e., counterfeit or lost/stolen) loss falls to the entity (card issuing company, e.g. American Express, bank or merchant) that doesn't support the chip technology. Therefore, since GDSs don't offer chip reading terminals to travel agents, the agency is responsible in the event of a loss due to the agent's acceptance of a counterfeit or lost/stolen card.

Although a UCCCF no longer provides a remedy for a card-present fraud chargeback, it can be provided as "compelling evidence" in an attempt to reverse the chargeback. This is why it is still considered a best practice to obtain a signed and imprinted UCCCF.

The following includes instructions for completing a UCCCF.

Guide to the Preparation of the Universal Credit Card Charge Form



1. Obtain the signature of the cardholder and compare i t with the signature on the card;
2. Enter the three (3) digit airline code;
3. Imprint the date of sale;
4. No longer applicable;
5. Enter the name of the passenger and connection with the subscriber, if other than the cardholder;
6. No longer applicable;
7. Enter the authorization/ approval code received via the GDS;
8. Enter the airport/city code, fare basis and airline codes of the ticket routing (if applicable);
9. Enter the payment card name or two-letter alpha code;
10. Enter the airline code and ticket number(s) of tickets issued;
11. Imprint card;
12. Enter fare, tax and total of all tickets issued.

Note: Retain the signed, imprinted form in a secured location so it can be provided as compelling evidence in the event of a fraud chargeback.

Other Tips for Detecting Fraud

Agents who know their customers have a lower risk of fraud than agents accepting transactions from unknown individuals. Information is critical when evaluating the risk of fraud. A merchant (airline, and therefore, agent) can start to evaluate the risk of fraud by evaluating the data available about a transaction and the customer.

The following are examples of data points often available about a transaction that can help evaluate the identity of a cardholder and/or the risk that the transaction could result in a chargeback. Please note, none of these items alone provide a full evaluation of the customer or the transaction, but when used together paint a more complete picture that can be used to evaluate risk. For additional information about red flags for fraud prevention the “Payment Card Acceptance Red Flags” guide is available on the ARC website at https://www2.arccorp.com/support-training/fraud-prevention/best-practices/.

Customer information

- Passenger name — Validate that the passenger name matches the cardholder name. This can be done by calling one of the enhanced voice authorization phone numbers or by calling the number on the back of the card. If none of the passenger names match the cardholder name, the risk of fraud increases. Please note that fraudsters may work around this red flag when booking a group by including the cardholder name as one of the passengers for a ticket that will never be used.
- Customer history— Determine if the customer is a previous customer of the agency and if the experience was positive or negative. If the customer previously initiated a chargeback, it may not be worth the risk. If the history with the customer is positive, the risk that they will claim fraud is lower.
- Email address — Email addresses from free services are easy to obtain and can be difficult to trace. Therefore, they are easy for individuals perpetrating fraud to use. Employ a service to validate email addresses that determines how long it has been in use along with other information to help identify the risk of fraud.
- Caller ID — If Caller ID shows a customer calling using a Voice over Internet Protocol (VOIP) service, this could be an indication of a higher risk customer. With the use of VOIP, it is difficult to know more precisely where the customer is calling from. However, with the prevalence of VOIP for legitimate users, it can be difficult to identify good customers from fraudsters.
- New customer — Depending on the agency's business model, a new customer maybe considered higher risk, particularly when the initial contact is via email, Internet or TTY service (for the hearing impaired). Generally, individuals perpetrating fraud prefer to do so without making human contact, however there has been a trend toward the use of social engineering tactics to perpetrate fraud. If a new customer is requesting travel outside typical patterns for the agency, it could be a red flag.
- Customer not local — Depending on the business model, if a customer is calling the agency for the first time, determine how they heard about the agency and if they are available to come into the agency. If not, the risk of fraud increases. Beware of social engineering schemes that use information available via the internet (including social media sites like LinkedIn, Facebook or Twitter) to help build a relationship.
- Multiple payment card numbers provided — If the first card is declined and another card is provided, this could be an indication of a problem.

Transaction information

- Last-minute travel — A date of departure near the date of issue can indicate an increased risk of fraud. The challenge is that this is often the behavior of good customers. Please note there is a trend toward fraudsters purchasing a ticket several weeks or months in advance of the date of departure, but then contacting the airline to change the ticket to an immediate departure for a different itinerary.
- International travel — International travel tends to be higher risk than domestic travel, although domestic fraud is on the rise.
- High-risk cities — Some itineraries and cities have higher fraud rates.
- Departure city — A departure city that isn't near the cardholder billing address can be an indication of higher risk.

It is important to note that individuals perpetrating fraud are able to find ways to “work around” well-known red flags. Most travel agents know and understand typical customer travel behavior for their business. When travel trends fall outside the typical behavior, the risk tends to be higher. Agents are encouraged to stay informed of the latest fraud trends and be aware of customers that display behavior that is not typical for the agency.

Disclosure of the Terms and Conditions of the Sale

In addition to fraud related chargebacks, merchants can receive chargebacks for cardholder claims related to the service or a refund not received. When a service or refund related chargeback is received, the agent is required to provide proof that the terms and conditions of the sale were disclosed and accepted by the cardholder. As noted below, how the information is disclosed and accepted will differ depending on how the sale takes place (i.e. on-line, face-to-face, phone). Most “terms and conditions related disputes” are about the customer’s ability to refund or change a ticket and the associated fees. Therefore, regardless of how the transaction takes place, it is important to provide clear and concise disclosure of the rules at the time of purchase. Additionally, if a chargeback is received, the agent must provide proof that the cardholder was informed of the rules.

Face-to-face – Provide the customer with a written disclosure of the terms and conditions and ask them to sign it to acknowledge receipt. Retain it in case of a dispute.

Online – Include a “click-to-accept” of the terms and conditions of the sale. Include a clear and concise list of the key terms followed by an on-line check box. Obtain a screen print of your system in case of a dispute.

Phone – Read the key terms and conditions to the customer and request they acknowledge that they understand. Proof that this disclosure was completed is difficult to obtain, however merchants have some success providing a recording along with a transcript as proof in case of a dispute.

Part 4: Chargeback Management Best Practices

The ARC Debit Memo Working Group is a group of travel agencies, airlines, GDSs and other industry partners focused on reducing or eliminating debit memos. When looking at debit memo reasons by dollar amount, payment card chargebacks are the highest category. Chargebacks are a pain point for both agents and airlines. While the best way to reduce chargeback debit memos is to reduce fraud, there is also an opportunity to reduce debit memos by disputing chargebacks that are received. For example, in a "friendly fraud" situation, there is an opportunity to provide data that demonstrates the cardholder was involved in and authorized the transaction. Following are some key steps to help successfully reverse chargebacks.

Friendly Fraud (i.e., Chargeback Fraud) versus True Fraud

It is important to know the difference between friendly fraud and true fraud when deciding if, and how, to respond to chargebacks. It can be challenging because in both cases the chargeback is generally identified as "Fraud" or "No Knowledge" by the credit card issuer. Friendly fraud occurs when a cardholder participated in and authorized a transaction, but claims that the card was used without the cardholder's knowledge. True fraud occurs when payment card data is stolen and used to purchase tickets without the knowledge of the cardholder.

The distinction between true fraud and friendly fraud is important when managing chargebacks because it is impossible to provide proof that the cardholder was involved and authorized the transaction when their card information was stolen and used to make the purchase. Therefore, merchants are encouraged to attempt to determine which chargebacks are friendly fraud versus true fraud before taking the time to respond to fraud chargebacks. Unfortunately, only friendly fraud chargebacks can be won.

Responding to a chargeback

There are two ways to reverse a chargeback. First, provide a remedy which the card companies specifically define as evidence that the dispute is invalid. Second, provide "compelling evidence" that provides confirmation that the cardholder was involved in and authorized the transaction.

Chargeback Remedy

In the U.S. travel agency distribution channel for airline e-tickets, the information required to remedy (i.e., reverse) a fraud chargeback 100 percent% of the time is not currently available. There are two main reasons why this is the case:

1. Card-Present- In a card present transaction, proof that the card is not counterfeit or lost/stolen is required. With the implementation of chip card functionality in the US, the proof is only available by using a credit card terminal that reads the chip. Travel agents do not have chip card reading terminals.
2. Card-Not-Present– In a travel agency e-ticket environment, the infrastructure to support 3-D Secure is not currently available. In addition, since there aren't tangible goods to be delivered, there is no way to prove delivery to the cardholder address.

The good news is that in the event of a Visa fraud chargeback, if an airline provides proof that the cardholder was on the plane, the chargeback will be reversed. This can be a challenging for the airline because the name of the cardholder is not provided on the chargeback. Therefore, the airline would need to provide the documentation on all fraud chargebacks in the hope that some are reversed. Other payment card companies will consider proof that the cardholder was on the plane as "compelling evidence", but not a remedy which would reverse the chargeback.

In summary, to increase the odds of reversing a fraud chargeback, the agent needs to provide proof that the true cardholder was involved in, and authorized, the transaction. Absent this proof, it's unlikely that a fraud chargeback dispute will be settled in favor of the merchant (airline and, therefore, agent).

Compelling Evidence

The payment card companies use the term "compelling evidence" to describe the documentation merchants can provide to prove that the identity of the cardholder was validated and that the cardholder was involved in the transaction. While compelling evidence maybe considered by credit companies when reviewing a response to a chargeback, it does not provide a guarantee of remedy (i.e., reversal of the chargeback). The following are some examples of documentation that maybe considered "compelling evidence" by some credit card companies and, when presented together, may demonstrate that the cardholder was involved in, and authorized, the transaction:

- Email correspondence to an email address that matches the address the payment card company has on file for the cardholder;
- Emails, photographs or other evidence proving the relationship between the cardholder and the customer/passenger if they are different;
- An imprint of the card on a credit card charge form with a cardholder signature;
- Photographs or social media postings proving that the cardholder took the flight to a particular destination;
- Copy of the valid cardholder passport or driver's license (please note, however, that these documents can be easily forged and may not provide proof of cardholder participation in the transaction);
- Evidence of additional valid transactions tied to the chargeback transaction;
- Evidence of the customer's prior affiliation with the agency;
- Evidence that the passenger is, or was, a member of the cardholder's household.

Agency Chargeback Response Best Practices

When an agency receives a chargeback notice from an airline, in an attempt to reverse the chargeback and/or avoid the loss, they are encouraged to do the following:

1. If the transaction was refunded, provide the airline with an image of the refund from the Document Retrieval Service (DRS) along with the refund date and amount. Please note, do not issue a refund after the chargeback is received. It could result in two credits to the cardholder.
2. Contact the customer to explain the charge. If there has been a misunderstanding on the part of the customer, request that they contact their bank to rescind the inquiry or dispute/chargeback. Even if the customer agrees to withdraw the dispute, be sure to respond to the chargeback in case the customer does not contact the payment card company.
3. If the agency has been hit by fraud, where the customer/passenger was not the cardholder, therefore resulting in a cardholder receiving an unauthorized charge, there isn't any documentation that can be provided to reverse the chargeback. One good indication of true fraud is that the customer cannot be reached. The agent is encouraged to review fraud prevention procedures to avoid future occurrences.
4. If the agency believes the true cardholder was the passenger, indicating friendly fraud. Or, if the reason for the chargeback is authorization related or tied to the disclosure of the terms and conditions of the sale, (i.e., "services not rendered"), agents are encouraged to provide professional, legible and concise documentation to back up the agency's defense to the chargeback. A cover letter on company letterhead should be included with a clear and concise outline of what the transaction represents and what the customer received. The following are examples of evidence to include with the letter:
    - Any proof that the cardholder authorized the transaction (see: "Compelling Evidence");
    - Any proof that the customer is the true cardholder (see: "Compelling Evidence");
    - Copies of tickets or details of the itinerary to help the customer recognize the charge;
    - Copies of invoices provided to the customer including an email address that could be tied to the cardholder;
    - Signed acknowledgement of the terms and conditions, particularly referencing refund policy if the ticket is non-refundable;
    - Proof that a valid authorization was obtained;
    - Signed and imprinted UCCCF when available;
    - Anything that could be considered "compelling evidence" that the cardholder was involved in and authorized the transaction.
5. If the cardholder is disputing the charge and therefore initiating a chargeback because they believe there is a duplicate billing, and there are two separate and legitimate transactions, provide proof of both charges including both ticket numbers.
6. Respond to the airline as quickly as possible, and no longer than five (5) business days after receipt of the chargeback.
7. If you believe the customer has perpetrated fraud and received services for something that has not been paid, contact the police, seek legal counsel to determine the best way to manage the customer perpetrating fraud, and/or consider a collection service to obtain the funds.

Payment Card Industry Data Security Standards

Any ARC participant that accepts payment cards as payment must keep all payment card numbers and personal information secure, whether in hard copy or electronically, and be compliant with the Payment Card Industry Data Security Standard (PCI DSS). Additional information about PCI-DSS requirements can be found on the ARC website at https://www2.arccorp.com/pci-data-security-standards/

Conclusion

The best way to reduce the risks associated with payment card acceptance is to know your customer. Travel agents who meet customers face-to-face are in a better position to reduce exposure to fraud and chargebacks. It is important to keep in mind that as fraud prevention tools become more effective in card-not-present environments, fraudsters seek new avenues for perpetrating fraud. Therefore, it is important to remain vigilant and be on the lookout for customer behavior or ticketing patterns that are not usual for the agency.

There are many tools available to help merchants manage the risk of payment card fraud. For card-not-present transactions, tools like Address Verification (AVS) and Card Identification verification (CID, CVV2 and CVC2) are available through the GDS. These tools, when used in conjunction with other red flags for fraud, allow merchants to review transactions and evaluate risk at the basic level. Tools like 3-D Secure, along with others tools that do device fingerprinting, on-line or mobile behavior evaluation, and machine learning, allow travel agents to evaluate transactions by employing a more sophisticated set of tools.

If you experience fraud or suspect fraud, please contact the ARC fraud prevention team at (703) 816-8137 or via email at stopfraud@arccorp.com.