



Credit Card Acceptance & Chargeback Prevention

Tips for Travel Agents
July 2010

Tips for Agents

Credit Card Acceptance & Chargeback Prevention



About this Guidebook	3
Credit Card Acceptance	4
Fraud Prevention Tips	7
Credit Card Chargebacks Tips	11
Payment Card Industry Security Standards	12
Comments from ARC's Risk Management Department	13
Questions and Answers	14

About this Guidebook

This guidebook provides travel agents with the information they need to make informed decisions regarding credit card acceptance. Today, transactions take place, predominately, via the phone, e-mail or Internet. The processes for accepting credit cards also varies according to situation. When accepting credit cards it is strongly recommended that the travel agent confirm that the card is valid and active, that the cardholder identity can be authenticated, and that the transaction is legitimate.

A rising portion of travel sales are conducted with customers in a non face-to-face environment. Because of this, the risk of accepting credit card transactions that are later identified as fraud has increased. In an attempt to remain competitive, and in a market where customers expect to purchase travel from the comfort of their home, travel agents often accept credit card payment from first-time customers with very little identifying information. By supporting this type of distribution, travel agents take the risk that customers are perpetrating fraud, so weigh the pros and cons.

This guide does not supersede the information contained in the Credit Card Chargeback policy found in Section 8.4 of the ARC *Industry Agents' Handbook* or the ARC Travel Agency Service Fee (TASF) Processing Agreement. Section 8.4 provides agents with the procedures the agency must follow in order to be absolved of liability in the event of a fraud-related chargeback from an airline. Agents are fully liable for any and all TASF transactions that result in a chargeback. In general, the policy states that to support a fraud chargeback, within 5 days of the notice, an agent must provide the airline with a signed and imprinted Universal Credit Card Charge Form (UCCCF) for the specific transaction in question, along with a valid approval code. It is important to note that when charging a customer a Travel Agency Service Fee (TASF), a separate UCCCF must be obtained so the dollar amount identified on the UCCCF for each transaction is valid.



Credit Card Acceptance

Validate Acceptance of Form of Payment by Carrier

Most consumers already know where they want to go when they contact a travel agent. They usually know how they want to pay as well. When a customer presents payment, it is important to verify that the payment is valid for the selected carrier. The best way to verify this information is through IAR, the ARC *Industry Agents' Handbook* available on-line at arccop.com or through the ARC Travel Agency Communication (TAC) messages.

Disclosure of Terms and Conditions

At the time of sale, it is important to provide customers with the Terms and Conditions of the sale. This is generally completed either verbally or in writing. However in a situation where the customer is disputing something outlined in the Terms and Conditions, only a signed disclosure form acts as verification that the customer acknowledged receipt of the disclosure. In a case where the credit card is accepted via the internet, proof that the customer was required to "click to accept" is also valid acknowledgement.

TIP: Important information to include in Terms and Conditions

- Can the ticket be refunded or exchanged? Are there penalties?
- Can changes to the ticket be made? Are there fees?
- What are the procedures for making changes?

Credit Card Authorizations

A credit card authorization is required for every credit card transaction. The purpose of an authorization is to verify available credit (aka, open to buy), and validate that the card and/or card number have not been reported lost or stolen. Credit card authorizations should be obtained through the system provider. Continue with the transaction only when an "approved" authorization response is received. If a response other than "approved" is received, request that the customer provide another form of payment. When charging a customer a Travel Agency Service Fee (TASF) a separate authorization must be obtained.

If the system provider authorization system is unavailable, a Voice Authorization Service is available.

The instructions for use are as follows:

American Express (800) 528-2121

UATP (800) 638-6510

JCB International (800) 522-8788
Merchant #: 0002016020

Visa (800) 231-1754

MasterCard (800) 231-1754

Discover (800) 347-1111
Merchant # 6011 0160 1101 601

The voice authorization service should not be used as an alternative to obtain an authorization when the automated process through the system provider resulted in a “decline” (or message other than “approved”). When accepting a sale from an unknown customer, difficulty obtaining an approval code could be a sign of a problem.

RED FLAG: If the initial authorization attempt through the system provider resulted in a “decline” (or message other than “approved”), think twice before attempting to obtain another approval code or seeking an alternative avenue for obtaining a valid authorization using the same credit card. You can receive a “no approval code obtained” chargeback if any of the authorization requests resulted in a “decline” response.

TIP: If you suspect fraud at the time the transaction is taking place, MasterCard, Visa, Discover and American Express offer a service called “Code 10”. A Code 10 authorization request allows you to obtain additional information about the cardholder and the transaction when you suspect fraud. This service is supported through the Voice Authorization Services of the card companies.

Complete Universal Credit Card Charge Form (UCCCF) - face-to-face only

After obtaining a credit card authorization, complete a UCCCF. Be sure to do the following:

- Include the approval code of the authorization
- Obtain an imprint of the credit card
- Include the dollar amount to be billed to the credit card
- Have the customer sign the form
- Verify the signature on the form to the signature on the credit card. If the card is not signed, request a driver’s license or other form of government issued photo identification to verify the signatures.
- If you are charging a Travel Agency Service Fee (TASF) in addition to the ticket, you must complete a separate UCCCF for the TASF. Never combine an airline ticket and a TASF on the same UCCCF. They are separate transactions from separate merchants.

RED FLAG: An unsigned card could be a sign of fraud. With a fake identification, it is easy to use an unsigned card. For information about how to obtain a guide to spotting fake government issued identification go to <http://www.idcheckingguide.com/arc>

Credit Card Authorization Forms

The credit card companies do not recognize a generic credit card authorization form as a valid document to support a transaction, therefore, they are not a valid substitute for a signed, imprinted UCCCF.

Credit Card Security Features

All credit cards have security features that are designed to help identify counterfeit cards. The following are some of the features across all cards.

- Embossed card number on the front matches number located on the signature strip on the back (not including the card verification code).
- Expiration Date
- Magnetic stripe on the back of the card is above the signature box

Tips for Agents

Credit Card Acceptance & Chargeback Prevention



Individual credit card companies have unique security features. The following PDF provides information about the security features for American Express, MasterCard, Visa, and Discover.

https://www209.americanexpress.com/merchant/singlevoice/resources/card_identification%20rev%20072505.pdf

The following links provide additional information by card type:

American Express

https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&page=cardSecurityFeatures

MasterCard

http://www.mastercard.com/us/merchant/security/what_can_do/card_features.html

Visa

http://usa.visa.com/merchants/risk_management/card_present.html

Discover

<http://www.discovernetwork.com/fraudsecurity/fraud.html>



Fraud Prevention Tips

“Know your Customer”

The best way to be protected against credit card fraud is to “know your customer.” Whenever possible, have the customer come to the office. In a face-to-face environment, complete a Universal Credit Card Charge Form (UCCCF), obtain a valid approval code for the transaction amount, obtain an imprint of the credit card and have the customer sign the form. Maintain a copy of this form in a safe location that meets the Payment Card Industry (PCI) data security standards. It is not sufficient to have customers fax or e-mail a copy of a credit card charge form, they must be imprinted and signed in person.

In a non face-to-face environment, there is always a risk of fraud so obtain as much information about the customer as possible and maintain the information for future reference. Even if the personal information does not include credit card numbers, it is equally important to keep this personal customer information secure.

TIP: It is important to know that at least one of the people traveling is also the cardholder. If they are not, are you willing to risk that the cardholder will dispute the transaction?

The following information can help you validate the identity of a customer and/or cardholder. It is helpful to use this information to cross reference against other available resources and to call the phone numbers to confirm that they are valid. In addition, in the event of a credit card dispute or chargeback, you have information that will help you contact the customer for collections if necessary.

Passenger Name:

Billing Street Address:

Billing Address - City:

Billing Address - State

Billing Address - Zip code:

Home Phone number:

Work Phone number:

Cell Phone number:

Cardholder Name:

RED FLAG: IF YOU SUSPECT FRAUD, PLEASE REPORT THIS TO ARC’s FRAUD TEAM AS SOON AS POSSIBLE AT :

Phone: 703-816-8137
Fax: 703-816-8138
Email: FIFP@ARCcorp.com

Address Verification Service (AVS)

The Address Verification Service allows you to verify that the billing address provided by the customer matches the billing address associated with the card. Address Verification has proven to be an effective tool for validating customer identity because in many instances the individual perpetrating fraud will not know the customer billing address.

AVS is available through the following System providers using these commands:

Galileo S*BRF/CC ADDR
Sabre format-finder.sabre.com, keyword "AVS"
Amadeus HEDE
Worldspan INFO CK/ADDR

An Address Verification Service is also available directly through American Express, Visa, MasterCard and Discover by calling them directly. The phone numbers are as follows:

American Express (800)528-2121
MasterCard (800)MC-ASSIST
Discover (800)347-1111
Visa (800)847-2750

RED FLAG: If the address from the credit card company does not match the address you have on file, this could be an indication of a problem.

Note: Use of Address Verification does not provide for a shift in liability in the event of a fraud chargeback.

Card Identification Digits (CID), Card Verification Value (CVV2) and Card Verification Code (CVC2)

Visa, MasterCard, Discover, and American Express each provide a valuable service that allows agents to validate the un-embossed code on a credit card. Validating that the un-embossed number matches the number associated with the card helps to confirm that the customer has a valid card in his/her possession. This prevents individuals with stolen credit card numbers from using the numbers to make fraudulent purchases. This tool has proven to be a valuable risk management tool. However, as with the Address Verification Service, use of this tool does not provide for a shift in liability in the event of a chargeback.

This tool is available for most card types through the system providers. Check the help screens for information about how to use CID, CVV2 and CVC2. For additional information, the following resources are available:

American Express

See American Express Fraud Prevention Brochures under Additional Resources or follow link.

https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&page=fraudPreventionBrochures

MasterCard

See MasterCard Tools for Security Success – Getting Started located under Additional Resources or follow link.

http://www.mastercard.com/us/merchant/security/what_can_do/getting_started.html

Visa

http://usa.visa.com/personal/security/visa_security_program/3_digit_security_code.html

Discover

<http://www.discovernetwork.com/fraudsecurity/fraud.html>

Note: *It is important to note that this code can never be stored. Immediately following receipt of the code from the customer, it must be discarded.*

Online Fraud Prevention Tools - Verified by Visa and MasterCard SecureCode

Visa and MasterCard each developed an online tool that allows merchants to authenticate the identity of a cardholder through a secret pin associated with an account. These online tools facilitate authentication by providing an interface directly to the credit card issuer so that a secret pin can be validated therefore authenticating the cardholder. Online travel agents interested in getting additional information about these tools are encouraged to access the following links.

Verified by Visa

https://usa.visa.com/personal/security/vbv/index.html?it=121/personal/security/visa_security_program/3_digit_security_code.html|Verified%20by%20Visa

MasterCard SecureCode

<http://www.mastercard.com/us/personal/en/cardholderservices/securecode/index.html>

RED FLAG CHECKLIST FOR ACCEPTANCE OF CREDIT CARDS

There is risk associated with accepting any credit card transaction. You need to decide what level of risk you are comfortable with prior to issuing a ticket. The following are guidelines created to assist you in evaluating the risk associated with a credit card transaction:

http://www.arccorp.com/news/news_avoid_fraud.html/

LOW RISK

- Caller ID identifies caller as local
- Passenger is also cardholder
- Agent obtains manual imprint of unexpired and unaltered credit card in the travel agency
- Agent obtains valid signature and approval code
- Signature is an approximate match to that on back of the credit card
- Originating airport is in the same region as the travel agency
- Destination is in the same region as the travel agency
- Established customer
- Domestic travel
- Date of departure is more than one month from date of issue

MEDIUM RISK

- Caller ID identifies caller as local
- Originating airport is in the same region as the travel agency
- Destination is in the same region as the travel agency
- Passenger may or may not be cardholder
- Customer is new
- Could be domestic or international travel
- Date of departure is less than one month from date of issue

HIGH RISK

- Caller ID identifies caller as out of area or with no information at all
- Agents are usually contacted for the first time via, website, e-mail or the TTY service (for the hearing impaired)
- Cardholder is not the passenger
- Credit card, driver's license, passport faxed/e-mailed because cardholder is never present in the agency
- Several tickets are purchased with different routings, travel dates and passenger last names using a single credit card
- "Customer" may use a religious title (e.g., Pastor Robert) or a religious premise (Missionaries to Africa) or other socially respected profession, e.g., doctors, to establish credibility
- E-mail requests contain obvious spelling errors (e.g. cities and states)
- "Customer" uses airport codes in their e-mails, i.e., asking for tickets from ACC to LHR rather than Accra to London
- "Customer" provides fictitious address and phone number in the U.S.
- E-mail address is from a free service (Yahoo, Hotmail, Gmail, etc.)
- Customer/passenger name is new to agency
- Could be domestic or international travel
- Customer not concerned with ticket price or service fee amount
- Last minute travel
- Highly flexible travel schedule
- Customer offers multiple credit cards as payment if first credit card is rejected
- Customer can be contacted only via a cell phone with an area code not in the same region

Credit Card Chargebacks

Credit Card Chargebacks is one of the most unpopular subjects in the travel industry. As consumers using a credit card, we have a guarantee that if we were not involved in a transaction that has been billed to our account, or we did not receive the product or service promised, we can question the charge and/or charge it back. Merchants (carriers) and travel agents engage in a process that must be managed to respond to these inquiries, or chargebacks. The following is a list of suggestions for travel agents to respond to inquiries or debit memos received from a carrier:

- Contact your 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 chargeback.
- In all cases, provide the most professional, legible, and detailed documentation available to back up the charge. It helps to include a typed letter on company letterhead that provides details of what the transaction represents and what the customer received. In addition, include all relevant documents such as itineraries, invoices, copies of tickets, e-mails, etc.
- Respond as quickly as possible and within 5 business days.
- If you believe your customer has perpetrated fraud and received services for something that has not been paid, seek legal council to identify the best way to manage the customer.

TIP: If no response is received within 5 business days the agent will almost always be liable for a chargeback debit memo. It is always in your best interest to respond quickly to the carrier.

Things to include in your response to the carrier:

- Copy of ticket
- Details of itinerary
- Copies of invoices provided to customer
- Signed acknowledgement of Terms and Conditions
- Signed and imprinted Universal Credit Card Charge Form (face-to-face)
- On your agency letterhead, typed details of experience with the customer, including dates



Payment Card Industry Security Standards

Security of credit card and other personal customer information is of paramount importance for the security of customer information and the integrity of the credit card process. Any entity that comes in contact with credit card numbers is expected to be compliant with the Payment Card Industry (PCI) Security standards. The following link will provide you with the information you need to ensure that you are PCI compliant:

<https://www.pcisecuritystandards.org/>

Comments from ARC's Risk Management Department

Credit Card Fraud Tricks of the Trade

Often when individuals are trying to use a stolen or compromised credit card there is a sense of urgency. There have been incidents involving ministers requiring members of the congregation to travel the next day, or doctors arranging emergency travel for patients, and dispatchers requiring truck drivers in another state quickly. As proof of identity, the perpetrators of fraud offer to send copies, front and back, of their credit card, driver's license and/or passport. Remember, it is easy to alter documents and especially easy to hide the changes in a photocopied, facsimile transmittal. In other cases, travel was arranged for weeks in the future, making the travel agent believe that the credit card transaction would be cleared before any usage. Airlines sometimes allow passengers to exchange tickets, and travel early in order to fill seats. This results in travel agencies losing thousands of dollars.

For additional information or questions concerning credit card fraud schemes contact the ARC fraud department at (703)816-8137 or via e-mail at fifp@arccorp.com.

Questions and Answers

If I obtain a credit card authorization, am I protected against a chargeback?

No, obtaining a credit card authorization is an important step in the credit card acceptance process, however you can still be held liable for the transaction if you don't also:

- Obtain an imprint of the card and a signature
- Disclose the terms and conditions of the sale and obtain acknowledgement from the customer
- Respond to carrier requests for information within the time frame required

Additional Resources

Visa Risk Management

http://usa.visa.com/merchants/risk_management/index.html?it=h31/merchants/risk_management/fraud_control_basics.html | Risk%20Management

Visa Fraud Basics

http://usa.visa.com/merchants/risk_management/fraud_control_basics.html?it=c1/merchants/index.html | Fraud%20Control%20Basics

American Express Reduce Risk FAQ's

https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&page=reduceRiskFAQ

American Express Fraud FAQ's

https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&page=fraudPreventionFAQ

American Express Fraud Prevention Brochures

https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&page=fraudPreventionBrochures

MasterCard Tools for Security Success – Getting Started

http://www.mastercard.com/us/merchant/security/what_can_do/getting_started.html

Discover Fraud Reduction Best Practices

<http://www.discovernetwork.com/fraudsecurity/fraud.html>



FOR MORE INFORMATION

4100 North Fairfax Drive, Suite 600

Arlington, VA 22203-1629 | USA

+1 703.816.8000

www.arccorp.com

ARC is a technology solutions company providing transaction settlement and data information services. Airlines, travel agencies, corporate travel departments, railroads, and other travel suppliers process up to \$70 billion annually through ARC's world-class settlement system, making it the financial backbone of travel distribution.

© 2010 by Airlines Reporting Corporation (ARC). All rights reserved.