



Your Card Acceptance Guide



YOUR CARD ACCEPTANCE GUIDE

CONTENTS

Welcome

Part I

1. USE OF CARD ORGANIZATIONS BRANDS	5
2. POINT OF SALE REMINDERS	5
3. VALIDATING THE CARDS.....	6
4. TRANSACTION GUIDELINES.....	8
5. SECURITY	9
6. DATA PROTECTION AND TRANSARMOR SOLUTION.....	10
7. DEBIT CARDS	11
8. ELECTRONIC BENEFIT TRANSFER® (EBT) TRANSACTIONS	12

Part II

9. AUTHORIZATIONS	16
10. SPECIAL TYPES OF TRANSACTIONS.....	19
11. SALES DRAFTS	21
12. REFUNDS.....	23
13. EXCHANGES	24
14. CHARGEBACKS, RETRIEVALS AND OTHER DEBITS	24
15. SUSPECT/FRAUDULENT TRANSACTIONS.....	30

Part III

16. RETENTION OF RECORDS.....	33
17. RETURN OF EQUIPMENT	33
18. TIMEFRAMES	34
19. ADDITIONAL PROVISIONS FOR SPECIFIC INDUSTRIES.....	34

APPENDIX 1

ADDITIONAL PROVISIONS FOR WEX AND VOYAGER	39
---	----

APPENDIX 2

ADDITIONAL PROVISIONS FOR AMERICAN EXPRESS® TRANSACTIONS	42
--	----

APPENDIX 3

SPECIAL PROVISIONS FOR DISCOVER NETWORK®	59
--	----

WELCOME

From start to finish
A guide to accepting cards

Card acceptance solutions are an essential part of your business. As your partner, we want to make accepting cards as simple as possible for you. That's why we created Your Card Acceptance Guide. It's your quick reference to the guidelines for processing transactions. You'll also find recommendations and tips to help you prevent fraud, reduce chargebacks, and properly handle payments, refunds, exchanges, and most other situations you'll encounter in your day-to-day-business.

To help you navigate more easily and find the information you need when you need it, we've organized the guide into three parts. At the end of the guide, you'll also find information specific to processing Wex, Voyager, American Express, and Discover cards payments.



If you have questions about processing payments or any of your other business services, please contact Customer Service at the number listed on your merchant services statement. Your customer service team is here to make things easier so let us know what we can do to help.

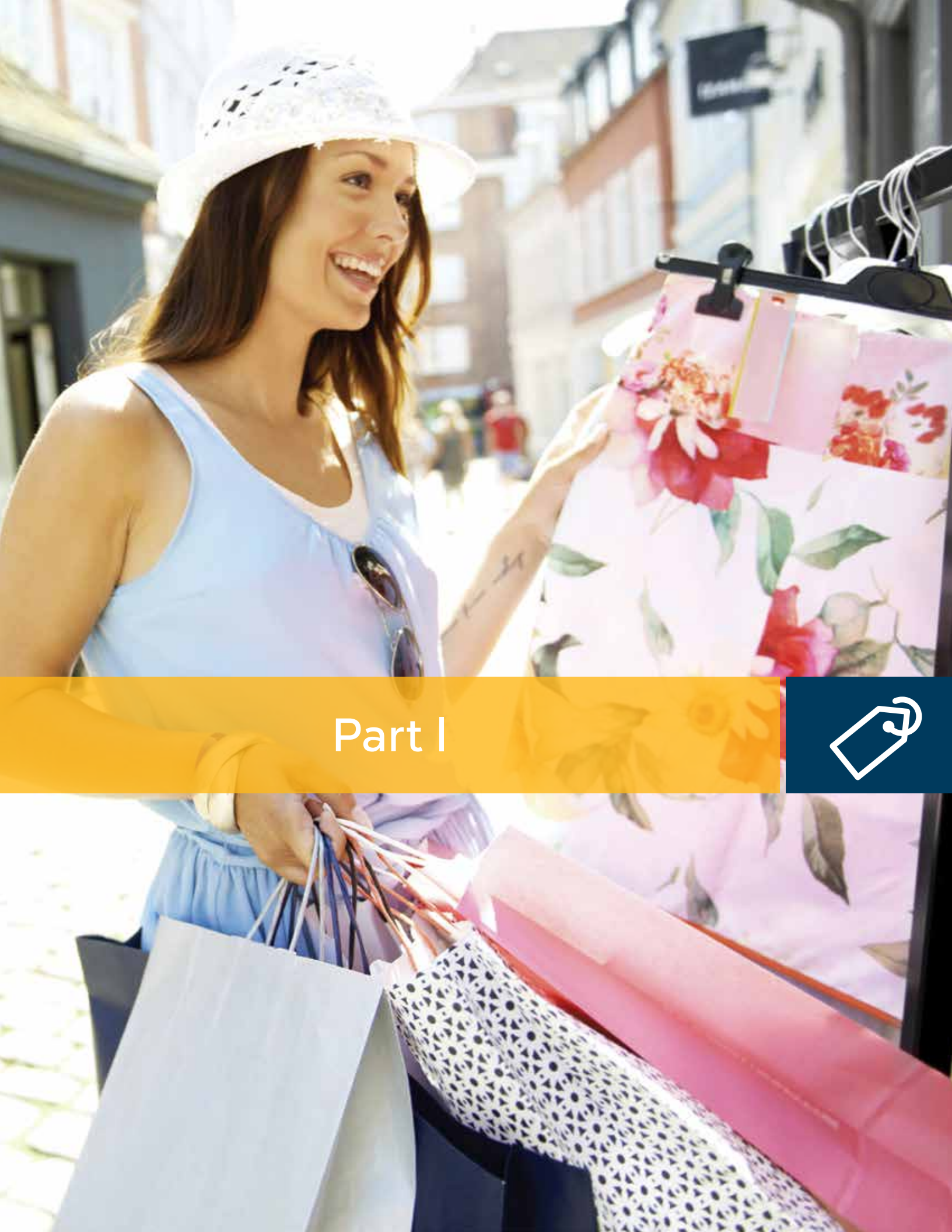
For more information about card acceptance, please go to:

American Express: www.americanexpress.com

Discover Financial Services: www.discovernetwork.com

MasterCard Worldwide: www.mastercard.com

Visa Inc: www.visa.com



Part I





The first step of a transaction actually begins before a customer even decides to make a purchase. This part of Your Card Acceptance Guide reviews steps you'll need to take to ensure customers are informed of their payment options and understand the terms of sale. You'll also find tips and important reminders for validating cards in order to reduce the risk of fraud. Finally, specific procedures for accepting debit and EBT payments are outlined. If you have questions about anything discussed in this guide, please contact Customer Service at the number located on your merchant services statement.

1. USE OF CARD ORGANIZATIONS BRANDS



DO'S

- do prominently display relevant trademarks of the card organizations at each of your locations, in catalogs, on websites and on other promotional material.
- do only use the official trademarks of ours and of the card organizations in the official format.



DON'TS

- don't indicate that we or any card organization endorses your goods or services.
- don't use the trademarks of any card organization after: your right to accept the cards of that card organization has ended; or that card organization has notified you to stop using their trademarks.
- don't use the trademarks of ours or of the card organizations in any way that injures or diminishes the goodwill associated with the trademarks.
- don't use our trademarks or the trademarks of the card organizations in any manner, including in any advertisements, displays, or press releases, without our prior written consent.

For special rules applying to the treatment of the American Express brand please refer to Appendix 2 page 42.

2. POINT OF SALE (POS) REMINDERS

You must clearly and conspicuously:

- disclose all material terms of sale prior to obtaining an authorization;
- at all points of interaction inform cardholders which entity is making the sales offer, so that the cardholders can clearly distinguish you from any other party involved in the interaction; and
- disclose any discount/incentive for customers to pay with cash, check, credit card or debit card and so on. Any such discount/incentive must be offered to all customers with no special treatment for any card brand or card-issuing bank.

If you accept orders via the Internet, your website must include the following information in a prominent manner:

- a complete description of the goods or services offered;
- details of your (i) delivery policy; (ii) consumer data privacy policy; (iii) cancellation policy; and (iv) returns policy;



- the transaction currency (US dollars, unless permission is otherwise received from Servicers);
- the customer service contact, including email address and/or telephone number;
- your address, including country;
- the transaction security used on your website;
- any applicable export or legal restrictions;
- your identity at all points of interaction with the cardholder; and
- the date on which any free trial period ends.

If you limit refund/exchange terms or impose other specific conditions for card sales, you must clearly print (in 1/4" letters) the words "No Exchange, No Refund," etc. on the sales draft near or above the cardholder's signature, both on the cardholder's copy and your copy.

During a liquidation and/or closure of any of your outlets, locations and/or businesses, you must post signs clearly visible to customers stating that "All Sales Are Final," and stamp the sales draft with a notice that "All Sales Are Final."

3. VALIDATING THE CARDS

Transactions where the cardholder is present – 'Card Present' transactions

You must check the card if the cardholder is present at the point of sale;

- verify that the card is legitimate and valid;
- verify that the card is not visibly altered or mutilated;
- capture the magnetic stripe by swiping the card or capture chip card data by inserting the card in the POS device, unless the card is a contactless chip card;
- ensure that the cardholder either enters their PIN using the keypad or provides their signature;
- verify that the signature is identical to the name and signature on the card (if a signature is provided);
- verify the card's valid from date (if applicable) and the expiration date;
- verify that the card number and expiration date on the card are the same as on the transaction receipt and the number displayed on the POS device;
- verify that the name on the transaction receipt is the same as the name on the front of the card (if applicable); and
- ensure that the cardholder appears to be the person shown in the photograph (for cards with a photograph of the cardholder).

If the signature panel on the card is blank, you must:

- review positive identification bearing the cardholder's signature (e.g. a current passport or driver's license) to validate the cardholder's identity;
- indicate the positive identification, including any serial number and expiration date (where permissible by law) on the sales draft; and
- require the cardholder to sign the signature panel of the card prior to completing the transaction.



Transactions where the cardholder is not present - 'Card Not Present' transactions

This section applies to any transaction where the cardholder is not present, such as mail, telephone, Internet and E-commerce.

You may only conduct Internet transactions if you have notified us in advance and received approval.



DO'S

- do obtain the card account number, name as it appears on the card, expiration date of the card, and the cardholder's statement address.
- do use the Address Verification Service (AVS). If you do not have AVS, contact Customer Service immediately. Please refer to page 8.
- do clearly print the following on the sales draft, and provide a copy to the cardholder at the time of delivery:
 - the last 4 digits of the cardholder's account number;
 - the date of transaction;
 - a description of the goods and services;
 - the amount of the transaction (including shipping, handling, insurance, etc.);
 - the cardholder's name, billing address and shipping address;
 - the authorization code;
 - your name and address (city and state required); and
 - for mail orders write "MO" and for telephone orders write "TO" on the cardholder's signature line.
- do obtain proof of delivery of the goods or services to the address designated by the cardholder or, if the cardholder collects the goods or services in person, obtain an imprint of the card and the cardholder's signature.
- do notify the cardholder of delivery time frames and special handling and/or cancellation policies.
- do ship goods within seven (7) days from the date on which authorization was obtained. If delays are incurred (e.g. out of stock) after the order has been taken, notify the cardholder and obtain fresh authorization of the transaction.
- do use separate Merchant Numbers provided to you for Internet orders in all your requests for authorization and submission of charges.
- do provide at least one (1) month's prior written notice to your acquirer of any change in your Internet address.



DON'TS

- don't exceed the percentage of your total payment card volume for Card Not Present sales, as set out in your application.
- don't submit a transaction for processing until after the goods have been shipped or the service has been provided to the cardholder - the only exception to this is where the goods have been manufactured to the cardholder's specifications and the cardholder has been advised of the billing details.



- don't accept card account numbers by electronic mail.
- don't require a cardholder to complete a postcard or other document that displays the cardholder's account number in clear view when mailed or send any mailing to a cardholder that displays personal information in clear view.

It is also recommended that, if feasible, you obtain and keep a copy on file of the cardholder's signature authorizing you to submit telephone and mail order transactions.

Address Verification Service (AVS) (and other fraud mitigation tools such as Verified by Visa®, MasterCard® Secure Code, Card Validation Codes and Card Identification) does not guarantee against chargebacks; but, if used properly, it assists you in reducing the risk of fraud by confirming whether certain elements of the billing address provided by your customer match the billing address maintained by the card-issuing bank. AVS also may help you avoid incurring additional interchange expenses. AVS is a separate process from obtaining an authorization and will provide a separate response. A transaction may not match addresses when submitted for AVS and still receive an authorization. It is your responsibility to monitor the AVS responses and use the information provided to avoid accepting high-risk transactions.

If a disputed charge arises for a transaction conducted over the Internet or electronically, a chargeback may be exercised for the full amount.

For Discover Network transactions, please refer to Appendix 3 page 59 for the Discover Network protocol for Internet transactions.

Customer activated terminals and self-service terminals

You must contact Customer Service for approval and further instructions before conducting customer activated terminal transactions or self-service terminal transactions.

4. TRANSACTION GUIDELINES



DO'S

- do only present for payment valid charges that arise from a transaction with a bona fide cardholder.



DON'TS

- don't set a minimum transaction amount of more than \$10 for any credit cards or of any amount for debit cards.
- don't set a maximum transaction amount for any credit cards.
- don't establish any special conditions for accepting a card.
- don't make any cash disbursements or cash advances to a cardholder as part of a transaction with the exception of the Discover Network Cash Over service.
- don't accept any direct payments from cardholders for goods or services which have been included on a sales draft;
- don't require a cardholder to supply any personal information for a transaction (e.g. phone number, address, driver's license number) unless (i) instructed by the Voice Authorization Center; (ii) presented an unsigned card; or (iii) processing a Card Not Present transaction.



- don't submit any transaction representing the refinance or transfer of an existing cardholder obligation which is deemed uncollectible, e.g. a transaction that has been previously charged back, or to cover a dishonored check.
- don't submit sales drafts or credit drafts transacted on the personal card of an owner, partner, officer or employee of your business establishment or of a guarantor who signed your application form, unless such transaction arises from a bona fide purchase of goods or services in the ordinary course of your business.
- don't carry out factoring, that is, the submission of authorization requests and/or sales drafts for card transactions transacted by another business.

For special prohibited activities relevant to the use of the American Express card please refer to Appendix 2 page 43.

5. SECURITY

You are responsible for maintaining the security of your POS devices and for instituting appropriate controls to prevent employees or others from submitting credits that do not reflect bona fide returns or reimbursements of earlier transactions.

Please comply with the data security requirements shown below:



DO'S

- do install and maintain a secure network firewall to protect data across public networks.
- do protect stored data and data sent across networks using methods indicated in the PCI DSS.
- do use and regularly update anti-virus software and keep security patches up-to-date.
- do restrict access to data by business "need to know". Assign a unique ID to each person with computer access to data and track access to data by unique ID.
- do regularly test security systems and processes.
- do maintain a policy that addresses information security for employees and contractors.
- do restrict physical access to cardholder information.
- do destroy or purge all media containing obsolete transaction data with cardholder information.
- do keep all systems and media containing card account, cardholder, or transaction information (whether physical or electronic) in a secure manner so as to prevent access by, or disclosure to any unauthorized party.
- do only use services and merchant equipment that have been certified as PCI-DSS compliant by the card organizations.



DON'TS

- don't use vendor-supplied defaults for system passwords and other security parameters.
- don't transmit cardholder account numbers to cardholders for Internet transactions.
- don't store or retain Card Validation Codes (three-digit values printed in the signature panel of most cards, and a four-digit code printed on the front of an American Express card) after final transaction authorization.
- don't store or retain magnetic stripe data, PIN data, chip data or AVS data - only cardholder account number, cardholder name and cardholder expiration date may be retained subsequent to transaction authorization.

For Internet transactions, copies of the transaction records may be delivered to cardholders in either electronic or paper format.

6. DATA PROTECTION AND TRANSARMOR SOLUTION

With the exception of data protection, the TransArmor Solution is only available in any calendar year if you process less than 1 million Visa card transactions and less than 1 million MasterCard card transactions in such year.

We will provide you with an encryption key to encrypt (make unreadable) card data for transmission from your POS devices to our systems for authorization. During such transmission to us, all historical transaction data, including card number and full magnetic stripe data (track data and expiration date), will be encrypted. We will then generate or retrieve a unique, randomly generated token assigned to the card number that will be returned to you in the authorization response.

Data Protection applies only to card transactions sent from you to us for authorization and settlement pursuant to the Agreement, and specifically excludes electronic check transactions.

You must comply with the requirements shown below for the data protection solution:



DO'S

- do comply with the card organization rules, including the Payment Card Industry Data Security Standards (PCI DSS).
- do demonstrate and maintain your current PCI DSS compliance certification. Compliance must be validated either by a Qualified Security Assessor (QSA) with corresponding Report on Compliance (ROC) or by successful completion of the applicable PCI DSS Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC), as applicable, and if applicable to your business, passing quarterly network scans performed by an Approved Scan Vendor, all in accordance with card organization rules and PCI DSS.
- do ensure that all third parties and software that you use for payment processing comply with PCI DSS.



- do deploy the data protection solution (including implementing any upgrades to such service within a commercially reasonable period of time after receipt of such upgrades) throughout your systems including replacing existing card numbers on your systems with tokens.
- do use the token in lieu of card numbers for ALL activities subsequent to receipt of the authorization response, including settlement processing, retrieval processing, chargeback and adjustment processing, and transaction reviews.
- do ensure that any POS device, gateway and/or VAR is certified by us for use with the data protection solution. If you are uncertain whether your equipment is compliant, contact a client service representative at 866-359-0978.
- if you send or receive batch files containing completed card transaction information to/from us, do use the service provided by us to enable such files to contain only tokens or truncated information.
- do use truncated report viewing and data extract creation within reporting tools provided by us.
- do follow rules or procedures we may provide to you from time to time regarding your use of the data protection solution.
- do promptly notify us of a breach of any these terms.



DON'TS

- don't retain full card numbers, whether in electronic form or hard copy.
- don't use altered version(s) of the data protection solution.
- don't use, operate or combine the data protection solution or any related software, materials or documentation, or any derivative works thereof with other products, materials or services in a manner inconsistent with the uses contemplated in this section.

7. DEBIT CARDS

When accepting debit cards, you'll need to follow the specific requirements for each PIN debit network as well as the general requirements set out in this section.



DO'S

- do read the account number electronically from the magnetic stripe. If the magnetic stripe is unreadable, you must request another form of payment from the cardholder.



DON'TS

- don't process a credit card transaction in order to provide a refund on a debit card transaction.
- don't complete a debit card transaction without entry of the PIN by the cardholder (and no one else) unless the transaction is a network supported PIN-less transaction.
- don't accept the PIN from the cardholder verbally or in written form.
- don't manually enter the account number.

The PIN debit network used to process your transaction (whether with a PIN or a PIN-less transaction) will depend upon, among other things, our own business considerations, the availability of the PIN debit network at the time of the transaction and whether a particular debit card is enabled for a particular PIN debit network.



The PIN debit network used to route your transaction may or may not be the lowest cost network available.

We may in our sole discretion:

- use any PIN debit network available to us for a given transaction (including any of our affiliated PIN debit networks); and
- add and/or remove PIN debit networks available to you based on a variety of factors including availability, features, functionality and our own business considerations.

YOU ARE RESPONSIBLE FOR SECURING YOUR POS DEVICES AND FOR IMPLEMENTING APPROPRIATE CONTROLS TO PREVENT EMPLOYEES OR OTHERS FROM SUBMITTING CREDITS AND VOIDS THAT DO NOT REFLECT BONA FIDE RETURNS OR REIMBURSEMENTS OF PRIOR TRANSACTIONS.

You may offer cash back to your customers when they make a PIN debit card purchase. You may set a minimum and maximum amount of cash back that you will allow. If you are not currently offering this service, your POS device may require additional programming to begin offering cash back as long as it is supported by the PIN debit network.

You must reconcile your accounts for each location daily and notify us within 24 hours of any issues.

An adjustment is a transaction that is initiated to correct a debit card transaction that has been processed in error. You are responsible for all applicable adjustment fees that may be charged by a debit card network. Some PIN debit networks may have established minimum amounts for adjustments. An adjustment may be initiated for several reasons:

- the cardholder was charged an incorrect amount, either too little or too much.
- the cardholder was charged more than once for the same transaction.
- a processing error may have occurred that caused the cardholder to be charged even though the transaction did not complete normally at the point of sale.

All parties involved in processing adjustments are regulated by time frames that are specified in the operating rules of the applicable PIN debit network, the Electronic Funds Transfer Act, Regulation E, and other applicable law.

8. ELECTRONIC BENEFIT TRANSFER (EBT) TRANSACTIONS

We offer electronic interfaces to Electronic Benefit Transfer (EBT) networks for the processing, settlement and switching of EBT transactions initiated through the use of a state-issued EBT card at your point of sale terminal(s) so that EBT recipients may receive EBT benefits.

EBT benefits may comprise:

- United States Department of Agriculture, Food and Nutrition Service (FNS),
- Supplemental Nutrition Assistance Program (SNAP),
- Women, Infants and Children Benefits (WIC Benefits), and/or
- Government delivered cash benefits.

If you accept EBT transactions and/or provide EBT benefits:



DO'S

- do provide EBT benefits to EBT recipients in accordance with applicable law and the procedures set out in the Quest rules, in the amount authorized through your terminal upon presentation by an EBT recipient of an EBT card and such EBT recipient's entry of a valid PIN.



- do use POS Terminals, PIN pad and printer or other equipment that meet required standards (including those set out in the Quest rules) during your normal business hours and in a manner consistent with your normal business practices.
- do comply with the procedures set out in the Quest rules for authorization of EBT benefits if your terminal fails to print EBT benefit issuance information as approved and validated as a legitimate transaction.
- do provide a receipt for each EBT transaction to the applicable EBT recipient.
- do provide EBT benefits for EBT recipients from all states.
- do notify us promptly if you plan to stop accepting EBT cards and providing EBT benefits or if you are unable to comply with this section or the Quest rules.
- do adequately display any applicable state's service marks or other licensed marks, including the Quest marks, and other materials supplied by us in accordance with the standards set by the applicable state.
- do use any marks only to indicate that EBT benefits are issued at your location(s).
- do maintain adequate cash on hand to issue EBT service provider authorized cash benefits.
- do issue cash benefits to EBT recipients in the same manner and to the same extent cash is provided to your other customers.



DON'TS

- don't accept EBT cards or provide EBT benefits at any time other than in compliance with this section or the Quest rules.
- don't designate and direct EBT recipients to special checkout lanes restricted to use by EBT recipients unless you also designate and direct other customers to special checkout lanes for debit cards or credit cards and/or other payment methods such as checks other than cash.
- don't resubmit any EBT card transaction except as specifically permitted by the applicable Quest rules and procedures.
- don't accept any EBT card for any purpose other than providing EBT benefits, including without limitation accepting an EBT card as security for repayment of any EBT recipient obligation to you. If you violate this requirement, you will be obligated to reimburse the state or us for any EBT benefits unlawfully received by either you or an EBT recipient to the extent permitted by law.
- don't dispense cash for FNS, SNAP and WIC Benefits.
- don't disclose individually identifiable information relating to an EBT recipient or applicant for EBT benefits without prior written approval of the applicable state.
- don't use the marks of any EBT service provider without prior written approval from such EBT service provider.
- don't indicate that we, any state, or its EBT service provider endorse your goods or services.
- don't require, or in your advertising suggest, that any EBT recipient must purchase goods or services from you as a condition to receiving cash benefits, unless such condition applies to other customers as well.

You must take sole responsibility for the provision of any EBT benefits other than in accordance with authorizations received from the EBT service provider.



If an authorized terminal is not working or the EBT system is not available:

DO'S

- do manually accept EBT cards and manually provide EBT benefits in the amount authorized through the applicable EBT service provider to the EBT recipients at no cost to the EBT recipients upon presentation by an EBT recipient of their EBT card.
- do obtain an authorization number for the amount of the purchase from the applicable EBT service provider while the respective EBT recipient is present and before you provide the EBT recipient with any FNS, SNAP and WIC benefits, or cash benefits, as applicable.
- do properly and legibly enter the specified EBT recipient, clerk and sales information, including the telephone authorization number, on the manual sales draft.
- do clear all manual vouchers authorizations on your point of sale terminal within fourteen (14) days after the date of applicable voice authorization. If a voucher expires before it has been cleared by your terminal for payment, no further action can be taken to obtain payment for the voucher.

DON'TS

- don't attempt to voice authorize a manual EBT transaction if the EBT recipient is not present to sign the voucher. The EBT recipient must sign the voucher. You must give a copy of the voucher to the EBT recipient at the time of authorization and retain one copy for your records.
- don't re-submit a manual sales draft for payment for a transaction if you have not received an authorization number.
- don't mail vouchers requesting payment.

You must take sole responsibility for (and you will not be reimbursed in respect of) a manual transaction if you fail to obtain an authorization number from the applicable EBT service provider in accordance with this section or otherwise fail to process the manual transaction in accordance with the Quest rules, except as specifically provided in the Quest rules.



Part II





This part of Your Card Acceptance Guide reviews essential elements of a transaction, including authorizations, issuing refunds and exchanges, and handling special transactions like recurring payments. You'll also find information about chargebacks and processes to put in place to avoid chargebacks. Feel free to contact Customer Service with any questions that arise as you review this information.

9. AUTHORIZATIONS

General

You must obtain an authorization approval code from us for all transactions.

A positive authorization response remains valid for the timeframe set out in section 18 page 34.

An authorization approval code only indicates the availability of credit on an account at the time the authorization is requested. It does not indicate that the person presenting the card is the rightful cardholder, nor is it a promise or guarantee that you will not be subject to a chargeback.

You must not attempt to obtain an authorization approval code from anyone other than us, unless we have authorized you to use a third party authorization system as set out in section 9 page 18. An authorization approval code from any other source may not be valid.

If you use Address Verification Services (AVS), you must review the AVS response separately from the authorization response and make your own decision about whether to accept the transaction. A transaction may receive an authorization approval code from the card-issuing bank even if AVS is unavailable or reflects that the address provided to you does not match the billing address on file at the card-issuing bank.

If you receive a referral response to an attempted authorization, you must not:

- submit the transaction without calling for and receiving a voice authorization; and
- attempt another authorization on the same card through your POS device.

You must not attempt to obtain multiple authorizations for a single transaction. If a sale is declined, do not take alternative measures with the same card to obtain an approval of the sale from other authorization sources. Instead, request another form of payment.

If you fail to obtain an authorization approval code or if you submit a card transaction after receiving a decline (even if a subsequent authorization attempt results in an authorization approval code), your transaction may result in a chargeback and it may be assessed fines or fees by the card organizations for which you will be responsible. Fees currently range from \$25 to \$150 per transaction.

You will be charged for a request for an authorization approval code (where applicable), whether or not the transaction is approved.

Card Not Present transactions

It is highly recommended that you obtain the 3-digit Card Validation Code on the back of the card (CVV2 for Visa and CVC2 for MasterCard), the 3-digit Card Identification (CID) on the back of the card for Discover Network, and the 4-digit Card Identification (CID) on the front of the card for American Express, include this code with each Card Not Present authorization request. The exception to this is for recurring transactions, for which you are only required to submit the Card Validation Code with the first authorization request and not with the subsequent authorization requests.

For American Express transactions please also refer to Appendix 2 page 44.



For Discover Network Card Not Present transaction, please also refer to Appendix 3 page 59.

Authorization via telephone (other than terminal/electronic device users)

You must call your designated Voice Authorization Toll Free Number and enter the authorization information into the VRU using a touch tone phone or hold for an authorization representative.

If the Voice Authorization Center asks you to obtain identification from the cardholder before issuing an approval code, you must clearly write the appropriate identification source and numbers in the space provided on the sales draft.

If the Voice Authorization Center asks you to confiscate a card, do not take any action that will alarm or embarrass the card presenter, and send the card to Rewards Department, P.O. Box 5019, Hagerstown, MD 21740. You may be paid a reward for the return of the card.

If the sale is declined, please remember that our operators are only relaying a message from the card-issuing bank. The fact that a sale has been declined must not be interpreted as a reflection of the cardholder's creditworthiness. You must instruct the cardholder to call the card-issuing bank.

Authorization via electronic devices

If you use an electronic terminal to obtain authorization approval codes, you must obtain the authorization approval codes for all sales through this equipment.

If your terminal malfunctions, please refer to your Quick Reference Guide or call the POS Help Desk. Please remember to check your terminal periodically because most terminal problems are temporary in nature and are quickly corrected.

If a terminal is moved or if wires are disconnected, causing malfunction, call the POS Help Desk immediately and follow their instructions. You may be responsible for any service charges incurred for reactivation of the terminal.

Until the terminal becomes operable, you must call your designated Voice Authorization Toll Free Number and enter authorization information into the VRU using a touchtone phone. During this time, each transaction must be imprinted using a manual Imprinter machine.

Third party authorization systems

If you have contracted to use one of our authorization services, you must not use another third party authorization system without notifying Customer Service. Otherwise, we will be unable to successfully research and defend any authorization related chargebacks on your behalf. This delay will significantly decrease your time to research and provide proof of authorization, thus reducing your opportunity to reverse a chargeback.

If you use another authorization network:

- you will be responsible for the downgrade of any transactions to a higher cost interchange that result from any mismatch of information to our systems and those of third party authorization networks.
- liability resulting from discrepancies with that network must be resolved between you and that network. We will not research chargebacks resulting from authorization approval codes obtained from another authorization service organization. Such chargebacks will be passed through to you for resolution. If an authorization provided by a third party authorization system is challenged in a chargeback, you must obtain proof (e.g. third party authorization logs) from the authorization source and submit it to us within the time frame specified on the chargeback documentation.



Call the following for other card types, each of which is available 24 hours/day; 7 days/week:

American Express/ESA or Direct	1-800-528-2121
JCB, International (For YEN and CAD currency only)	1-800-522-9345
TeleCheck	1-800-366-5010
Voyager	1-800-987-6589
WEX	1-800-842-0071

You must enter manually all approved sales that have been authorized in this manner as “post authorization” transactions into the terminal, once the terminal becomes operational. You must enter all credit transactions into the terminal for data capture. If you receive a referral and subsequently receive an approval, you may be subject to a chargeback. You must imprint the card using a manual imprinter machine to reduce the risk of such a chargeback. For specific procedures on electronic data capture, refer to the Terminal Operating Instructions/Users Guide. If the terminal malfunctions for more than twenty-four (24) hours, contact Customer Service for further instructions on processing your transactions.

Automated dispensing machines

You must produce records for all transactions originating with automated dispensing machines or limited amount terminals. Such records must include the last 4 digits of the cardholder account number, merchant’s name, terminal location, transaction date, identification of transaction currency, transaction type (purchase), authorization code, and amount.

For Discover Network transactions please refer to Appendix 3 page 59. for the procedure for request for cancellation of authorization.

Partial authorization and authorization reversal

Partial authorization provides an alternative to a declined transaction by permitting a card-issuing bank to return an authorization approval for a partial amount. This amount is less than the transaction amount requested because the available card balance is not sufficient to approve the transaction in full. The cardholder is able to use the funds remaining on the card to pay for a portion of the purchase and select another form of payment (i.e., another payment card, cash, check) for the remaining balance of the transaction.

- for MasterCard transactions, partial authorization is optional for batch authorized e-commerce transactions, mail order, telephone order transactions and recurring payment transactions.
- for Discover transactions, partial authorization support is optional for Card Not Present transactions. If you support partial authorizations, a partial authorization indicator must be included in each authorization request.

You must submit an authorization reversal if the authorization is no longer needed, a partial amount of the total authorized is submitted for the settled transaction, or the cardholder elects not to complete the purchase. The transaction sent for settlement must be no more than the amount approved in the partial authorization response. If you wish to support partial authorization functionality, you must contact Customer Service for additional rules and requirements.



10. SPECIAL TYPES OF TRANSACTIONS

Payment by installments

If a cardholder makes a deposit toward the full amount of the sale price and pays the balance on delivery, please follow the procedures set out in this section.



DO'S

- do execute two separate sales drafts and obtain an authorization for each sales draft on each transaction date;
- do indicate on each sales draft:
 - whether it is for the deposit or the balance of payment; and
 - the authorization date and approval code.
- do submit and seek authorization of each delayed delivery transaction under the same merchant number and treat deposits on the card no differently than you treat deposits on all other payment products.
- do complete Address Verification each “balance” authorization.
- do obtain proof of delivery upon delivery of the services/merchandise purchased.



DON'TS

- don't submit sales data to us relating to the “balance” until the goods have been completely delivered or the services fully provided.

If delivery occurs after the timeframes set out in section 18 page 34, you must obtain a new authorization for the unprocessed portion of the transaction prior to delivery. If the transaction is declined, contact the cardholder and request another form of payment.

For example: On January 1, a cardholder orders \$2,200 worth of furniture and you receive an authorization for the full amount; however, only a \$200 deposit is processed leaving a \$2,000 balance remaining on the furniture. An authorization reversal must be processed for \$2,000. When the goods are available to ship, the \$2,000 transaction balance must be reauthorized.

Advance payment charges

If you offer cardholders the option or require them to make advance payment charges for the following types of goods and/or services, please follow the procedures set out in this section:

- custom-orders e.g. orders for goods to be manufactured to a customer's specifications;
- entertainment / ticketing e.g. sporting events, concerts, season tickets;
- tuition, room and board, and other mandatory fees e.g. library fees of higher educational institutions;
- tickets for airlines, rail and cruise lines, lodging, and other travel-related services e.g. tours and guided expeditions; and
- vehicle rentals.



You must:

- state your full cancellation and refund policies;
- clearly disclose your intent;
- obtain written consent from the cardholder to bill the card for an advance payment charge before you request an authorization. The cardholder's consent must include his or her agreement to all the terms of the sale (including price and any cancellation and refund policies), and a detailed description and the expected delivery date of the goods and/or services to be provided (including, if applicable, expected arrival and departure dates);
- obtain an authorization approval; and
- complete a sales draft.

If the advance payment charge is for a Card Not Present transaction, you must also:

- ensure that the sales draft contains the words "Advance Payment,"; and
- within twenty-four (24) hours of the charge being incurred, provide the cardholder written confirmation (e.g. email or facsimile) of the advance payment charge, the amount, the confirmation number (if applicable), a detailed description and expected delivery date of the goods and/or services to be provided (including expected arrival and departure dates, if applicable) and details of your cancellation/ refund policy.

If you cannot deliver goods and/or services (e.g. because custom-ordered merchandise cannot be fulfilled) and cannot make alternate arrangements, you must immediately issue a credit for the full amount of the advance payment charge that cannot be fulfilled.

Recurring transactions

If you process recurring transactions and charge a cardholder's account periodically for recurring goods or services (e.g. monthly insurance premiums, yearly subscriptions, annual membership fees, etc.), please follow the procedures set out in this section.



- do obtain cardholder approval for such goods or services to be charged on an ongoing basis to the cardholder's account. Approval must at least specify:
 - the cardholder's name, address, account number and expiration date,
 - the transaction amounts,
 - the timing or frequency of recurring charges,
 - the duration of time for which the cardholder's approval is granted, and
 - for Discover Network transactions, the total amount of recurring charges to be billed to the cardholder's account, including taxes and tips and your merchant number.
- do obtain an authorization for each transaction.
- do include the recurring payment indicator in each authorization request, and as applicable, each batch submission entry.
- do indicate on the sales draft "Recurring Transaction" (or "P.O." for MasterCard transactions) in lieu of the cardholder's signature.



- for Discover Network recurring transactions, do include a toll-free Customer Service number that the cardholder may call to obtain customer assistance from you or to cancel the written approval for the recurring transaction.

DON'TS

- don't include partial payments for goods or services purchased in a single transaction.
- don't impose a finance charge in connection with the recurring transaction or preauthorized order.
- don't complete a recurring transaction after receiving a cancellation notice from the cardholder or card-issuing bank or after a request for authorization has been denied.

It is highly recommended that you obtain the 3-digit Card Validation Code on the back of the card (CVV2 for Visa and CVC2 for MasterCard), the 3-digit Card Identification (CID) on the back of the card for Discover Network and the 4-digit Card Identification (CID) on the front of the card for American Express, include the number with the first authorization request. This is not required for subsequent authorization requests.

A positive authorization response for one recurring transaction is not a guarantee that any future recurring transaction authorization request will be approved or paid.

If the recurring transaction is renewed, you must obtain from the cardholder a new written request for the continuation of such goods or services to be charged to the cardholder's account.

If you or we have terminated your right to accept cards, you must not submit authorization requests or sales data for recurring transactions that are due after the date of such termination.

For American Express transactions please also see Appendix 2 page 46.

Card checks

If you accept card checks, you must treat checks from all the card organizations that you accept equally (e.g. if you accept MasterCard and American Express, your check acceptance policy must treat checks for both of these card organizations equally). You should handle these card checks like any other personal check drawn upon a bank in the United States.

11. SALES DRAFTS

DO'S

- do prepare a sales draft for each transaction and provide a copy of the sales draft or transaction receipt to the cardholder at the time the card transaction is completed. An exception is eligible low value transactions participating in any of the 'no signature required' programs.
- do only collect transaction data provided directly to you by the cardholder.
- do include all of the following information on a single page document constituting the sales draft:
 - the cardholder's account number;
 - cardholder's signature, unless you participate in any of the 'no signature required' programs;
 - date of the transaction;
 - the total amount of the transaction, including any taxes to be collected, in the approved currency of the sale;



- description of the goods and/or services involved in the transaction—if there are too many items, combine them into one description; e.g. “clothing” to ensure that all information is contained on a single page;
 - description of your merchandise return and credit/refund policy;
 - a valid authorization code;
 - Merchant’s Doing Business As (“D/B/A”) name and location (city and state required) and Merchant Account Number; and
- if the POS device fails to read the magnetic stripe or if you are required to obtain a voice authorization, you must also use a manual imprinting machine to make a clear impression of the card on the same side of the signed sales draft. If you work in the face-to-face sales environment, you may include the Card Validation Code or Card Identification in the authorization request for US domestic key-entered transactions in lieu of taking a manual card imprint. The Card Validation Code or Card Identification with Magnetic-Stripe Failures process is applicable to all card products when the magnetic-stripe fails at the point of sale (e.g. embossed cards, unembossed cards, vertical cards and cards with customized designs).



DON'TS

- don't include the card expiration date or any more than the last four digits of the card number in the copy of the sales draft which you provide to the cardholder.
- when imprinting sales drafts, you must not alter the cardholder account number, circle or underline any information on the sales draft or alter a sales draft in any way after the transaction has been completed and signed. Stray marks and other alterations on a sales draft may result in it becoming unreadable or illegible.

For Discover Network transactions in excess of \$50 including sales taxes, tip, surcharge and/or cash over amount are not eligible for any of the 'no signature required' programs.

If you participate in the Visa Easy Payment Service (“VEPS”) (Visa’s ‘no signature required’ program), Quick Payment Service and/or Small Ticket, you are only required to provide the cardholder with the completed sales draft when requested by the cardholder.

If you are operating under certain merchant category codes (“MCC”) approved by a card organization, you are not required to:

- provide a transaction receipt, unless requested by the cardholder; and
- obtain the cardholder’s signature provided that you transmit the full track data in the authorization request and the sale amount is below the applicable program floor limit:
 - MasterCard/Discover/American Express - \$50 or less; and
 - Visa - \$25 or less, with the exception of grocery stores (MCC 5411) and discount stores (MCC 5310) for which the floor limit is \$50.



12. REFUNDS



DO'S

- do provide clear instructions to your customers regarding returns, including the following:
 - Customer Service telephone number;
 - reference number for the return;
 - expected processing time for the credit;
 - return address, preferably on a pre-formatted shipping label (if applicable).
- do document your cancellation policy and terms and conditions on the contract the cardholder signs, or on your website, as applicable.
- do create a credit draft containing the following information for every refund:
 - the account number and expiration date;
 - the cardholder's name;
 - your name, city, state and Merchant Account Number;
 - a description of the goods or services;
 - the transaction date of the credit; the total amount of the credit; and
 - for Discover Network transactions, the approved currency used and the signature of your authorized representative or employee.
- do submit all credit drafts to us within the timeframes set out in section 18 page 34;
- do submit each credit under the establishment where the credit originated;
- do provide full refunds for the exact dollar amount of the original transaction including tax, handling charges, etc., and in no circumstances provide a refund amount for more than the original card sale amount;
- do write clearly all amounts and other handwritten information - stray marks on the credit draft will render it illegible.
- if the card cannot be swiped for any reason, do imprint the credit draft with the same card used by the cardholder to make the original purchase when applicable.
- do ensure that the cardholder signs the credit draft, give the cardholder the appropriate copy, and deposit the credit draft immediately.



DON'TS

- don't circle or underline any information on the credit draft.
- don't credit an account that differs from the account used for the original transaction.
- don't include the card expiration date or any more than the last four digits of the card number in the copy of the credit draft which you provide to the cardholder.
- don't give cash, check credit refunds or other consideration for card sales, with the exception of the following type of Visa transactions only:
 - Visa Easy Payment Service Transaction (Visa's 'no signature required' program);



- a gift purchased as a Mail/Phone Order transaction; or
- Visa prepaid card transaction if the cardholder states that the Visa prepaid card has been discarded.
- don't intentionally submit a sale and an offsetting credit at a later date solely for the purpose of debiting and crediting your own or a customer's account;
- don't process a credit transaction after a chargeback has been received.

Authorization is not required for credits.

Your website must communicate your refund policy to your customers and require your customers to select a "click-to-accept" or other affirmative button to acknowledge the policy. The terms and conditions of the purchase must be displayed on the same screen view as the checkout screen that presents the total purchase amount, or within the sequence of website pages the cardholder accesses during the checkout process.

For American Express transactions please also refer to Appendix 2 page 44.

13. EXCHANGES

For an even exchange, no additional paperwork is necessary and you may simply follow your standard company policy.

For an uneven exchange, you must complete a credit draft, and follow the procedures outlined in section 11 page xx for the total amount of the goods returned. The cardholder's account will be credited for that amount. Then, complete a new sales draft for the total amount of any new goods purchased.

14. CHARGEBACKS, RETRIEVALS AND OTHER DEBITS

Chargebacks

Both the cardholder and the card-issuing bank have the right to question or dispute a transaction. If such questions or disputes are not resolved, a chargeback may occur. You are responsible for all chargebacks, our chargeback fees and related costs arising from your transactions. As a result, we will debit your settlement account or settlement funds for the amount of each chargeback.

Due to the short time frames and the supporting documentation necessary to successfully (and permanently) reverse a chargeback in your favor, we strongly recommend that:

- you adhere to the guidelines and procedures outlined in this guide;
- if you do receive a chargeback, investigate, and if you dispute the chargeback, submit the appropriate documentation within the required time frame;
- whenever possible, contact the cardholder directly to resolve the dispute (except with respect to a Discover Network cardholder with whom direct contact regarding the dispute is prohibited by Discover Network Card Organization Rules); and
- if you have any questions, call Customer Service.

You must not process a credit transaction once a chargeback is received, even with cardholder authorization, as the credits may not be recoverable and you may be financially responsible for the credit as well as the chargeback. Instead, the card-issuing bank will credit the cardholder's account.



Chargeback process

If the card-issuing bank submits a chargeback, we will send you a chargeback notification, which may also include a request for transaction documentation. Due to the short time requirements imposed by the card organizations, it is important that you respond to a chargeback notification and transaction documentation request within the time frame set out in the notification.

Upon receipt of a transaction documentation request, you must immediately retrieve the requested sales draft(s) using the following guidelines:

- make a legible copy, centered on 8-1/2 x 11-inch paper (only one (1) sales draft per page);
- write the 'case number' from the request for transaction documentation on each copy/page;
- if applicable, make copies of a hotel folio, car rental agreement, mail/phone/Internet order form, or other form of receipt;
- if a credit transaction has been processed, make a copy of the credit draft;
- letters are not acceptable substitutes for sales drafts;
- fax or mail legible copies of the sales draft(s) and credit drafts, if applicable, to the fax number or mail address provided on the request form;
- if you fax your response, please (i) set your fax machine to print your fax number and name on the documents that you send, and (ii) set the scan resolution on your fax machine to the highest setting. We can use this information to help determine where the documentation received originated from if additional research is required, and the higher resolution setting improves the clarity of characters and graphics on the documentation transmitted and helps reduce the number of illegible fulfillments and/or chargebacks.

We strongly recommend that you also include a detailed rebuttal letter along with all pertinent documents when responding to a transaction request or a chargeback notification (e.g. rental agreement, imprinted portion of the invoice or sales draft; the portion signed by the cardholder; and the area where the authorization codes, with amounts and dates, are located).

If the information you provide is both timely and, in our sole discretion, sufficient to warrant a representation of the transaction and/or reversal of the chargeback, we will do so on your behalf. However, representation and/or reversal is/are ultimately contingent upon the card-issuing bank and/or cardholder accepting the transaction under applicable card organization guidelines. Representation or reversal is not a guarantee that the chargeback has been resolved in your favor.

If we do not receive a clear, legible and complete copy of the transaction documentation within the time-frame specified on the request, you may be subject to a chargeback for "non-receipt" for which there is no recourse.

If you do not dispute the chargeback within the applicable time limits as set by the card organization rules and regulations, you will forfeit your reversal rights. Our only alternative, which is available for Visa and MasterCard only, is to attempt a "good faith collection" from the card-issuing bank on your behalf for non-fraud chargeback reason codes. This process can take up to six (6) months and must meet the card-issuing bank's criteria (e.g. at or above a set dollar amount). Good faith collection attempts are not a guarantee that any funds will be collected on your behalf. Card-issuing banks normally charge good faith collection fees, which are deducted from the transaction amount if accepted in addition to any processing fees that are charged by us.



The card-issuing bank may charge a handling fee which will be debited from your settlement account or settlement funds if a transaction documentation request results from a discrepancy between the sales draft and the transmitted record regarding any of the following:

- the name of your business;
- the city, state, or country listed for your business;
- the transaction date.

Visa: If we reverse the chargeback and represent the transaction to the card-issuing bank, the card-issuing bank, at its sole discretion, may elect to submit the matter for arbitration before Visa. Visa currently charges a \$250 filing fee and a \$250 review fee. You will be responsible for all such fees and charges whether or not a decision is made in your favor, and any other applicable fees and charges imposed by Visa. Such fees and charges will be debited from your settlement account or settlement funds, in addition to the chargeback.

MasterCard: If we reverse the chargeback and represent the transaction to the card-issuing bank, the card-issuing bank, at its sole discretion, may elect to resubmit the chargeback. In such event, at our discretion, we will debit your settlement account or settlement funds for the chargeback. However, if you feel strongly that it is an invalid chargeback, we may, on your behalf and at your request, submit the matter for arbitration before MasterCard. MasterCard currently charges a \$150 filing fee and a \$250 review fee. You will be responsible for all such fees and charges whether or not a decision is made in your favor, and any other charges imposed by MasterCard. Such fees and charges will be debited from your settlement account or settlement funds, in addition to the chargeback.

Discover Network: If Discover Network rejects our representment request and you feel strongly that the chargeback is invalid, we may, at our discretion and on your behalf and at your request, submit the matter for dispute arbitration before Discover Network. Discover Network charges fees for representment requests and an arbitration fee as published in their fee schedule.

American Express: You may request a chargeback reversal if the chargeback was applied in error, provided that (i) you have responded to the original inquiry within the specified timeframe set out in your dispute notification, and (ii) you have provided all supporting documentation to substantiate the error.

Chargeback reasons

The following section outlines the most common types of chargebacks. This list is not exhaustive. Within each group we have included recommendations on how to reduce the risk of chargebacks. These are recommendations only, and do not guarantee that you will eliminate chargebacks.

Chargebacks due to authorization

Description

Proper authorization procedures were not followed and valid authorization was not obtained.

Likely scenario

- authorization not obtained.
- authorization was declined.
- transaction processed with an expired card and authorization was not obtained.
- transaction processed with an invalid account number and authorization was not obtained.
- Card Recovery Bulletin (CRB) or Exception File was not checked (transactions below floor limit).



Recommendations to reduce risk of chargeback

- obtain valid authorization on the day of the transaction.
- if you receive the following responses:
 - decline - request another form of payment from the cardholder;
 - referral - follow the voice procedures to obtain a valid authorization and obtain an imprint of the card;
 - “Pick-up” – this means that the card-issuing bank is asking for the card to be returned – you must not accept the card for payment and, in addition, you may retain the card and send it to us so that we can arrange for its return to the card-issuing bank.
- you must not exceed any predetermined thresholds for specific POS device types as specified by each card organization.
- you must ship goods within the timeframe set out in section 18 page 34, after you have obtained authorization.

Chargebacks due to cancellation and returns

Description

Credit was not processed properly or the cardholder has canceled and/or returned items.

Likely scenario

- Cardholder received damaged or defective merchandise.
- Cardholder continued to be billed for canceled recurring transaction.
- Credit transaction was not processed.

Recommendations to reduce risk of chargeback

- issue credit to the cardholder on the same account as the purchase in a timely manner.
- do not issue credit to the cardholder in the form of cash, check or in-store/merchandise credit as we may not be able to recoup your funds if the transaction is charged back.
- for recurring transactions ensure customers are fully aware of the conditions:
 - cancel recurring transactions as soon as notification is received from the cardholder or as a chargeback, and issue the appropriate credit as needed to the cardholder in a timely manner; and
 - notify the cardholder within 10 days (domestic) and 15 days (international) in advance of each billing, to allow the cardholder time to cancel the transaction.
- provide proper disclosure of your refund policy for returned/canceled merchandise, or services to the cardholder at the time of transaction. Card present, cardholder signed the sales draft containing disclosure.
- if applicable, the words “NO EXCHANGE, NO REFUND,” etc. must be clearly printed in 1/4-inch lettering on the sales draft near or above the cardholder signature:
 - Ecommerce, provide disclosure on your website on the same page as check out. Require the cardholder to click to accept prior to completion.
 - Card Not Present, provide the cancellation policy at the time of the transaction.
- for any Travel & Entertainment (T&E) transaction, provide cancellation numbers to cardholders when the services are canceled.
- ensure delivery of the merchandise or services ordered to the cardholder.
- participate in recommended fraud mitigation tools.



Chargebacks due to fraud

Description

Transactions that the cardholder claims are unauthorized; the account number is no longer in use or is fictitious, or the merchant was identified as "high risk."

NOTE: For Visa transactions, to ensure that you preserve your chargeback rights, you must:

- complete a retrieval request and/or provide a sales slip that contains all required data elements; and
- respond to all retrieval requests with a clear legible copy of the transaction document that contains all required data elements within the specified timeframe.

Likely scenario

- multiple transactions were completed with a single card without the cardholder's permission.
- a counterfeit card was used and proper acceptance procedures were not followed.
- authorization was obtained; however, full track data was not transmitted.
- the cardholder states that they did not authorize or participate in the transaction.

Recommendations to reduce such risk of chargeback Card Present Transactions:

- obtain an authorization for all transactions.
- for recurring transactions ensure customers are fully aware of the conditions:
 - cancel recurring transactions as soon as notification is received from the cardholder or as a chargeback, and issue the appropriate credit as needed to the cardholder in a timely manner; and
 - notify the cardholder within 10 days (domestic) and 15 days (international) in advance of each billing, allowing the cardholder time to cancel the transaction.
 - American Express customers have the option to receive written notification of the recurring transaction at least (10) days prior to submitting, or any time the charge amount exceeds a maximum amount that has been set by the cardholder.
- if you are utilizing an electronic device to capture card information, swipe, dip or wave all card transactions through your electronic authorization device to capture cardholder information. When applicable, ensure the displayed cardholder number matches the number on the card.
- if you are unable to electronically capture the card or if a referral response is received, imprint the card using a valid imprinting device that will capture the embossed card and merchant information. You must write on the manually imprinted draft all pertinent information relating to the transaction (transaction date, dollar amount, authorization code and merchandise description) and obtain the cardholder signature. Do not alter the imprint on the draft in any way. You are not protected from this type of chargeback by manually entering the information into the POS device.

NOTE: Do not imprint on the back of a signed sales draft. The imprint must be on the transaction document that contains all transaction elements to prove the card was present at the time of the transaction.

- obtain the cardholder signature for all transactions; ensure the signature on the sales draft matches the signature on the back of the card.
- process all transaction one time and do not batch out transactions multiple times.
- educate staff on procedures to eliminate point of sale (POS) fraud.

Card Not Present Transactions:

- ensure delivery of the merchandise or services ordered to the cardholder.
- participate in recommended fraud mitigation tools:
 - Verified by Visa Program
 - MasterCard SecureCode
 - Address Verification Services (AVS)
 - Card Validation Code (CVV2 for Visa and CVC2 for MasterCard) and Card Identification (CID for Discover Network and American Express) verification



NOTE: While transactions utilizing these tools may still be disputed, the service may assist you with your decision to accept certain cards for payment.

- ensure you ship to the AVS confirmed address (bill to and ship to must match).
- obtain authorization for all transactions.
- ensure merchant descriptor matches the name of the business and is displayed correctly on the cardholder statement.
- ensure descriptor includes correct business address and a valid Customer Service number.
- please refer to Appendix 2 page 46 for American Express fraud mitigation tools.

Chargebacks due to cardholder disputes

Description

Goods or services not received by the cardholder, Merchandise defective or not as described.

Likely scenario

- Services were not provided or merchandise was not received by the cardholder.
- Cardholder was charged prior to merchandise being shipped or merchandise was not received by agreed upon delivery date or location.
- Cardholder received merchandise that was defective, damaged, or unsuited for the purpose sold, or did not match the description on the transaction documentation/verbal description presented at the time of purchase.
- Cardholder paid with an alternate means and their card was also billed for the same transaction.
- Cardholder canceled service or merchandise and their card was billed.
- Cardholder billed for a transaction that was not part of the original transaction document.
- Cardholder claims to have been sold counterfeit goods.
- Cardholder claims the merchant misrepresented the terms of sale.

Recommendations to reduce such risk of chargeback

- provide Services or Merchandise as agreed upon and described to the cardholder; clearly indicate the expected delivery date on the sales receipt or invoice.
- contact the cardholder in writing if the merchandise or service cannot be provided or is delayed, and offer the cardholder the option to cancel if your internal policies allow.
- if the cardholder received defective merchandise or the merchandise received was not as described; resolve the issue with the cardholder at first contact.
- if the merchandise is being picked up by the cardholder, have them sign for the merchandise after inspecting that it was received in good condition.
- do not charge the cardholder until the merchandise has been shipped, according to the agreed upon terms, and a signed Proof of Delivery from the cardholder is obtained.
- if unable to provide services or merchandise, issue a credit to the cardholder in a timely manner.
- accept only one form of payment per transaction. Ensure the cardholder is only billed once per transaction.
- do not bill cardholder for loss, theft or damages unless authorized by the cardholder.
- ensure that a description of the service or merchandise provided is clearly defined.

Chargebacks due to processing errors

Description

Error was made when transaction was processed or it was billed incorrectly.

Likely scenario

- the transaction was not deposited within the card organization specified timeframe.
- the cardholder was issued a credit draft. However, the transaction was processed as a sale.



- the transaction was to be processed in a currency other than the currency used to settle the transaction.
- the account number or transaction amount used in the transaction was incorrectly entered.
- a single transaction was processed more than once to the cardholder's account.
- the cardholder initially presented the card as payment for the transaction. However, the cardholder decided to use an alternate form of payment.
- a limited amount or self-service terminal transaction was processed for an amount over the pre-determined limit

Recommendations to reduce risk of chargeback

- process all transactions within the card organization specified timeframes.
- ensure all transactions are processed accurately and only one time
- if a transaction was processed more than once, immediately issue voids, transaction reversals or credits.
- ensure that credit transaction receipts are processed as credits and sale transaction receipts are processed as sales.
- ensure all transactions received a valid authorization approval code prior to processing the transaction. Also obtain a legible magnetic swipe or imprinted sales draft that is signed.
- do not alter transaction documentation or make any adjustments unless the cardholder has been contacted and agrees to modifications of the transaction amount.
- ensure limited amount, self-service and automated fuel dispenser terminals are set properly to conform to the pre-determined limits.

Chargebacks due to non-receipt of information

Description

Failure to respond to a retrieval request or the cardholder does not recognize the transaction.

Likely scenario

- the transaction documentation was not provided to fulfill the retrieval request.
- the retrieval request was fulfilled with an illegible sales draft or was an invalid fulfillment (incorrect sales draft or the sales draft did not contain required information that may include signature).
- the cardholder does not recognize or is unfamiliar with the transaction due to the merchant name and/or location not matching the name and/or location where the transaction took place.

Recommendations to reduce such risk of chargeback

- provide a clear and legible copy of the sales draft that contains all required data elements within the required timeframe that is specified on the retrieval request.
- ensure that the most recognizable merchant name, location and/or Customer Service phone number is provided on all transactions.
- retain copies of all transaction documentation for the required timeframe that is specified by each card organization.
- develop efficient methods to retrieve transaction documentation to maximize ability to fulfill requests.

15. SUSPECT/FRAUDULENT TRANSACTIONS

If the card being presented or the behavior of the person presenting the card appears to be suspicious or you otherwise suspect fraud, you must immediately call the Voice Authorization Center and ask to speak to a Code 10 operator. Answer all their questions and follow their instructions.



While not proof that a transaction is fraudulent, the following are some suggestions to assist you in preventing fraudulent transactions that could result in a chargeback:

Does the cardholder:

- appear nervous/agitated/hurried?
- appear to be making indiscriminate purchases (e.g. does not care how much an item costs, the size, etc.)?
- make purchases substantially greater than your usual customer (e.g. your average transaction is \$60, but this transaction is for \$360)?
- insist on taking the merchandise immediately (e.g. no matter how difficult it is to handle, is not interested in free delivery, alterations, etc.)?
- appear to be purchasing an unusual amount of expensive items or the same items?
- take an unusual amount of time to sign the sales draft, or look at the back of the card as he signs?
- talk fast or carry on a conversation to distract you from checking the signature?
- take the card from a pocket instead of a wallet?
- repeatedly come back, in a short amount of time or right before closing time, to make additional purchases?
- cause an unusual, sudden increase in the number and average sales transactions over a one-to three-day period?
- tell you he has been having some problems with his card-issuing bank and request that you call a number (that he provides) for a “special” handling or authorization?
- have a previous history of disputed charges?
- place orders to be shipped to an address other than the billing address, or use anonymous/ free email domains?
- place orders sent to zip codes or countries where you show a history of fraudulent claims?

Does the card:

- have characters the same size, height, style and all within alignment?
- appear to be re-embossed (the original numbers or letters may be detected on the back of the card)?
- have a damaged hologram?
- have a Magnetic Stripe on the back on the card?
- have an altered signature panel (e.g. appear discolored, glued or painted, or show erasure marks on the surface)?
- have “valid from” (effective) and “valid thru” (expiration) dates consistent with the sale date?

We also recommend that you are vigilant for any cardholder who behaves as follows, specifically in relation to prepaid cards:

- frequently makes purchases and then returns the goods for cash;
- uses prepaid cards to purchase other prepaid cards;
- uses large numbers of prepaid cards to make purchases.

Gift Cards, jewellery, video, stereo, computer and camera equipment, shoes and men’s clothing are typically fraud-prone because they can easily be resold. Also be suspicious of high dollar amounts and transactions with more than one fraud-prone item, e.g. two laptops, three gold chains, etc.



Part III





In this part of the guide you'll find helpful information about how long you must retain copies of records, how to return equipment and important transaction timeframes. This is also where you'll find additional guidelines for specific industries including:

- Lodging
- Travel & Entertainment
- Restaurants
- Vending machines
- Telecommunications
- Petroleum

If you'd like additional information about anything you've read in Your Card Acceptance Guide, please contact Customer Service.

16. RETENTION OF RECORDS

You must securely retain legible copies of all sales drafts and credit drafts or any other transaction records for the following periods:

MasterCard and Visa: thirteen (13) months from the transaction date. Five (5) years for healthcare sales drafts and credit drafts.

Discover Network: the longer of (i) 365 days or (ii) the resolution of any pending or threatened disputes, claims, disagreements or litigation involving the card transaction. You must also keep images or other copies of sales drafts for no less than three (3) years from the date of the Discover Network transaction.

American Express: 24 months from the date on which you submitted the sales draft or credit draft to us.

You must provide all sales drafts and credit drafts or other transaction records requested by us within the shortest time limits established by card organization rules.

17. RETURN OF EQUIPMENT

To return point of sale (POS) equipment, you must call Customer Service for the address of the location to send the device.

You must include the following information in the shipping box:

- your name, address and phone number;
- the name of the person to contact if there are any questions;
- your merchant account number;
- the lease number (if applicable); and
- the serial number of the POS device (found on the underside of the POS device).

You must return the POS device in a manner that can be tracked. Reference the lease number (if applicable) on the return packaging.



18. TIMEFRAMES

Authorizations

A positive (approved) authorization response remains valid for:

- seven (7) days for MasterCard electronic processed transactions;
- ten (10) days for Visa and Discover electronic processed transactions subject to the following exception:
 - thirty (30) days for the following Industries:
 - car rental;
 - airline and passenger railway;
 - lodging;
 - other Travel & Entertainment (T&E) categories.
- seven (7) days for American Express electronic processed transaction subject to the following exception:
 - thirty (30) days for the Travel & Entertainment (T&E) industries.

Delayed deliveries

If delivery is more than:

- seven (7) days (MasterCard, Visa and American Express transactions); or
- ten (10) days (Discover Network transactions);
- after the original transaction date and the initial authorization request, you must reauthorize the unprocessed portion of the transaction prior to delivery.

Refunds

You must submit all credit drafts to us within five (5) days of determining that a credit is due.

19. ADDITIONAL PROVISIONS FOR SPECIFIC INDUSTRIES

Merchants in the lodging industry

There are additional rules and requirements that apply to merchants in the lodging industry for practices including, but not limited to, guaranteed reservations and charges for no shows, advance deposits, overbookings, and priority checkout. If you are a lodging merchant and wish to participate in the card organization lodging services programs, please contact your sales representative or relationship manager for details and the appropriate card organization requirements.

You must provide the cardholder with written confirmation of a guaranteed reservation. The confirmation must contain:



- cardholder's name as it appears on the card, if present;
- card number, truncated where required by applicable law to you or us and card expiration date if present, unless prohibited by applicable law to you or us;
- reservation confirmation number;
- anticipated arrival date and length of stay;
- the cancellation policy in its entirety, inclusive of the date and time the cancellation privileges expire; and
- any other pertinent details related to the reserved accommodations.

If a cardholder requests a cancellation in accordance with your cancellation policy and specified time frames, you must provide the cardholder with a cancellation number and instructions to retain a record of it.

If a cardholder requests a written confirmation of the cancellation, you must provide this confirmation to the cardholder within three (3) business days of such request. For the purposes of this section, a "business day" means Monday through Friday, excluding Bank holidays.

The cancellation confirmation must contain:

- the cardholder's reference that charges were placed on the card, if applicable, or a guarantee that a "no-show" charge will not be placed on the card;
- the cardholder's name as it appears on the card, if present;
- the card number, truncated as required by applicable law to you or us;
- the card expiration date, if present, unless prohibited by applicable law to you or us;
- the reservation cancellation number;
- the date of cancellation;
- the name of your employee that processed the cancellation; and
- any other pertinent information related to the reserved accommodations.

Pre-authorization for Travel & Entertainment (T&E) and restaurant merchants

If you are a business engaged in providing travel and/or entertainment services (e.g. car rentals, hotels, motels, etc.) or a restaurant business, and engage in the practice of "pre-authorization" you must comply with the following general procedures:

- a hotel, motel, or car rental merchant may obtain an estimated authorization at the time of check-in.
- restaurants must not add an estimated tip amount to the authorization request beyond the value of the goods provided, or services rendered, plus any applicable tax.
- you must notify the cardholder of the dollar amount you intend to "Pre-Authorize".
- if the customer decides to use another form of payment (e.g. cash, check, etc.) you must promptly call the Voice authorization Response Unit to delete the authorization hold. Provide the cardholder's account number, original dollar amount and date of the transaction, and the authorization code. If a new transaction takes place, a new imprinted and signed sales draft for the exact amount and a new authorization code for that amount must be obtained.



- VEHICLE RENTAL PROVIDERS MAY NOT INCLUDE POTENTIAL VEHICLE DAMAGE OR INSURANCE DEDUCTIBLES IN ANY PREAUTHORIZATIONS.
- if you receive a decline on a transaction, you must wait twenty-four (24) hours before attempting to reauthorize. If you reauthorize prior to this time frame and receive an approval, you may be subject to a chargeback and a fine imposed by the card organizations.
- hotels, motels, and car rental merchants are allowed up to a 15% variance above the amount authorized. If the final amount charged to the cardholder exceeds the original estimate by more than 15% above the preauthorization, you must authorize any additional amounts, and all incremental authorization codes must be written in the authorization area along with the date of authorization and the amount authorized.
- pre-authorization for certain establishments, are allowed up to a 20% (instead of 15%) variance above the amount authorized. If the final amount exceeds the amount "preauthorized" by more than 20%, you must authorize the additional amount. Estimating the authorization amount to include a tip is prohibited. The authorization request must include only the amount associated with the bill presented to your customer.
- you must obtain an authorization for the initial estimated charges and then monitor the charges to ensure that the actual charges made do not exceed the estimated charges. If the actual charges exceed the amount of the initial estimated authorization (and any subsequent estimated authorizations), then you must secure a positive authorization for the additional amount. Subsequent authorizations must only be for the additional amount of total charges, and must not include any amounts already authorized.
- the estimated amount of any pre-authorization for lodging accommodations must be based on (i) the intended length of stay; (ii) the room rate; (iii) applicable taxes and service charges; and (iv) other miscellaneous charges as dictated by experience.
- if an authorization request is declined, no charges occurring after that date will be accepted for that cardholder.
- you do not need to obtain a final authorization if the total sum of charges (the final amount) does not exceed 120% of the previously authorized charges. You must record the dates, authorized amounts, and their respective authorization approval codes on the sales draft(s).

Merchants operating vending machines

For MasterCard, if you are operating vending machines under MCC 5499 (Miscellaneous Food Stores-Convenience Stores, Markets, Specialty Stores), you need not provide a receipt at the time a transaction is conducted. However, if a vending machine cannot provide a printed receipt, you must disclose and post instructions advising cardholders how a receipt may be obtained.

Telecommunication service providers

You must contact Customer Service for approval and further instructions, rules and requirements before conducting telecommunication transactions.

Telecommunication card sales occur when a telephone service provider is paid directly using a card for individual local or long-distance telephone calls, with the exception that prepaid telephone service cards are not and do not give rise to telecommunication card sales.

The petroleum industry

For Visa, MasterCard and Discover transactions, automated fuel dispensers must ensure that completion messages are submitted for such card transactions within 60 minutes of the authorization.



For Discover transactions, Merchants operating in the petroleum industry that conduct card sales at Automated Fuel Dispensers (AFDs), may submit an authorization Request for \$1 to verify the validity of the card presented. Under such circumstances, you must submit an authorization Advice Message for the actual amount of the card sale within sixty (60) minutes of completion of fuel delivery regardless of whether you previously received a Partial authorization Response or a positive authorization Response for any other amount. If you do not complete the card sale following receipt of an approved authorization Response for any amount, a request to cancel the authorization Request must be submitted within sixty (60) minutes of the completion of fuel delivery.



Appendices





APPENDIX 1

ADDITIONAL PROVISIONS FOR WEX AND VOYAGER

WEX cards

If you participate in the WEX Full Service Program, the following terms and conditions will apply:



DO'S

- do provide, at your own expense, all equipment necessary to permit the electronic acceptance of the WEX cards, including the operation and maintenance of the equipment, telecommunication link, and provision of all networking services.
- do include in any request for authorization the following information:
 - WEX cardholder account number,
 - vehicle number,
 - card expiration date,
 - driver identification number;
 - the amount of the transaction,
 - the date and time of the transaction,
 - the quantity of goods sold, unit price, and product code (the "authorization Request Data"),
 - an authorization number or other approval code from WEX for all manual WEX card sales (i.e., sales facilitated by a card imprinter).
- do ensure that the product detail of each transaction is accurate including:
 - the type of goods sold,
 - quantity of goods sold,
 - unit price/price per gallon (if applicable),
 - taxes, and
 - any coupons presented.
- do ensure that the product detail outlined equals the total amount of the sale when calculated (i.e. Product quantity x unit price must equal the product amount. The sum of all product amounts including taxes minus any coupons must equal the total transaction amount).
- do complete a WEX card sale only upon the receipt of an authorization approval message.
- do provide a copy of the receipt for a WEX card sales, upon the request of the cardholder, to the extent permitted by applicable law. The receipt must not include the full account number or driver identification number.
- do require the cardholder to sign a receipt when a WEX card sale is not completed by an island card reader.
- do take all commercially reasonable efforts to protect manual WEX card sales data from fraud or misuse.



- do securely maintain a record of all WEX card sales (including the authorization request data) for a period of one year. You must produce such records upon the reasonable request of WEX.
- do notify us of any errors contained in a settlement report within forty-five (45) days of receipt of such report. We will not accept reprocessing requests for WEX transactions older than 90 days.
- do allow WEX to audit records, upon reasonable advance notice, related to the WEX Full Service.
- do retransmit WEX card sales data when reasonably requested to do so.

DON'TS

- don't submit a WEX card sale for processing unless a WEX card is presented at the time of the sale.
- don't accept a WEX card if an expired card / decline message is received.
- don't submit a WEX card sale for processing until the goods have been delivered or services performed.
- don't accept a WEX card if it appears to be invalid or expired or there is reasonable belief that the WEX card is counterfeit or stolen.
- don't divide the price of goods and services purchased in a single WEX card sale among two or more sales receipts.
- don't permit a WEX card sale when only partial payment is made by use of the WEX card and the balance is paid with another bank card.
- don't remove fuel tax at the point of sale is not permitted. For all payment system product codes that are taxable, the transaction dollar amount and price per gallon (PPG) must contain the sum of the fuel cost and PPG inclusive of all applicable Federal, State, County, Local and other fuel taxes.

You acknowledge and agree that your sole remedies with respect to the WEX Full Acquiring services will be against us and not WEX, except to the extent that WEX knows of any fraud related to the WEX cards and fails to provide notice of such fraud or WEX commits fraud in respect to the WEX Full Acquiring Services.

Voyager cards

- you must check Fleet Cards for any printed restrictions at the point of sale.
- you must establish a fair policy for the exchange and return of merchandise.
- you must promptly submit credits to us for any returns that are to be credited to a Voyager cardholder's account.
- you must not give any cash refunds to any Voyager card holder in connection with a sale, unless required by law.

In addition to the information set out in section 8 (Sales Drafts) page xx, you must include the following information on a single page document constituting the sales draft for Voyager transactions:

- all authorization request data for Voyager card sales must include the following:
 - Voyager cardholder account number,
 - card expiration date,



- driver identification number; and
- the amount of the transaction, date and time of the transaction,
- quantity of goods sold, unit price, and product code (the “Authorization Request Data”).
- all manual Voyager card sales (i.e., sales facilitated by a card imprinter) must include:
 - the Authorization Request Data,
 - an authorization number or other approval code from Voyager
 - the type of goods sold, quantity of goods sold, unit price/price per gallon (if applicable), taxes, and
 - any coupons presented within the product.
- the product detail outlined must equal the total amount of the sale when calculated, i.e.:
 - product quantity x unit price must equal product amount.
 - the sum of all product amounts including taxes minus any coupons must equal the total transaction amount.

You must not remove fuel tax at the point of sale. For all payment system product codes that are taxable, transaction dollar amount and price per gallon (PPG) must contain the sum of the fuel cost and PPG inclusive of all applicable Federal, State, County, Local and other fuel taxes.

If there is an increase of 15% or more compared to the previous month in the number of Voyager transaction authorization calls that are not due to our or Voyager system outages, we may, at our discretion, deduct telephone charges from the settlement of your Voyager transactions. Fees will not exceed \$0.25 (25 cents) per call.

Settlement of Voyager transactions will generally occur by the fourth banking day after we process the applicable card transactions. We will reimburse you for the dollar amount of sales you submit for a given day, reduced by the amount of chargebacks, tax exemptions, discounts, credits, and the fees set out in the Application. You must notify us of any errors contained with the settlement reports within 30 calendar days of receipt of such report. Neither we nor Voyager will be required to reimburse you for sales submitted more than sixty (60) calendar days from the date of purchase.

For daily transmission of sales data, you must securely maintain true and complete records for a period of not less than thirty six (36) months from the date of the generation of the data. You may store records on electronic media, if secure. You are responsible for the expense of retaining sales data records and sales drafts.



APPENDIX 2

ADDITIONAL PROVISIONS FOR AMERICAN EXPRESS TRANSACTIONS

PART A – GENERAL PROVISIONS

Treatment of American Express cards

Except as expressly permitted by applicable law, you must not:

- solicit merchants outside the US (Puerto Rico, the US Virgin Islands and any other US territory or possession do not form part of the US for these purposes);
- indicate or imply that you prefer, directly or indirectly, any other payment products over the American Express card (“the card”);
- try to dissuade cardholders from using an American Express card;
- criticize or mischaracterize the American Express card or any American Express’ services or programs;
- try to persuade or prompt cardholders to use any other payment products or any other method of payment (e.g. payment by check);
- impose any restrictions, conditions, disadvantages or fees when the American Express card is accepted that are not imposed equally on all other payment products, except for electronic funds transfer, or cash and check;
- suggest or require cardholders to waive their right to dispute any transaction;
- engage in activities that harm the American Express business or the American Express brand (or both);
- promote any other payment products (except your own private label card that you issue for use solely at your establishments) more actively than you promote the card; or
- convert the currency of the original sale transaction to another currency when requesting authorization or submitting transactions (or both).

You may offer discounts or in-kind incentives from your regular prices for payments in cash, ACH funds transfer, check, debit card or credit/charge card, provided that (to the extent required by applicable law):

- you clearly and conspicuously disclose the terms of the discount or in-kind incentive to your customers;
- the discount or in-kind incentive is offered to all of your prospective customers; and
- the discount or in-kind incentive does not differentiate on the basis of the issuer or, except as expressly permitted by applicable law or payment network.

The offering of discounts or in-kind incentives in compliance with the terms of this section will not constitute a violation of the previous section.

Treatment of the American Express marks

Whenever payment methods are communicated to customers, or when customers ask what payments are accepted, you must indicate your acceptance of the American Express card and display the American Express marks (including any card application forms provided to you) as prominently and in the same manner as any other payment products.



You must not use the American Express marks in any way that injures or diminishes the goodwill associated with the mark, nor (without our prior written consent) indicate that American Express endorses your goods or services.

You must only use the American Express marks as permitted. You must cease using the American Express marks upon termination of your acceptance of American Express cards.

For additional guidelines on the use of the American Express marks, please contact Customer Service.

Treatment of American Express cardholder Information

Any and all cardholder information is confidential and the sole property of the card-issuing bank, American Express or its affiliates. Except as otherwise specified, you must not disclose cardholder Information, nor use nor store it, other than to facilitate transactions at your establishments in accordance with the terms on which you are authorized to accept American Express cards.

Card acceptance

You must accept the card as payment for goods and services (other than those goods and services prohibited under the Prohibited activities section below sold, or (if applicable) for charitable contributions made) at all of your establishments, except as expressly permitted by state statute.

You are jointly and severally liable for the obligations of your establishments.

Prohibited activities

You must not accept cards for any of the following:

- adult digital content sold via Internet electronic delivery;
- amounts that do not represent bona fide sales of goods or services (or, if applicable, amounts that do not represent bona fide charitable contributions made) at your establishments. For example, purchases at your establishments by your owners (or their family members) or employees contrived for cash flow purposes, or payments that you have accepted in order to advance cash to cardholders in connection with the transaction;
- amounts that do not represent bona fide, direct sales by your establishment to cardholders made in the ordinary course of your business;
- cash or cash equivalent, for example, purchases of gold, silver, platinum, and palladium bullion and/or bars (collectible coins and jewellery are not prohibited), or virtual currencies that can be exchanged for real currency (loyalty program currencies are not prohibited);
- charges that the cardholder has not specifically approved;
- costs or fees over the normal price of the goods or services (plus applicable taxes) that the cardholder has not specifically approved;
- damages, losses, penalties, or fines of any kind;
- gambling services (including online gambling), gambling chips, gambling credits, or lottery tickets,
- unlawful/illegal activities, fraudulent business transactions or when providing the goods or services is unlawful/illegal (e.g. unlawful/illegal online Internet sales of prescription medications or controlled substances; sales of any goods that infringe the rights of a rights-holder under laws applicable to American Express, you, or the cardholder);
- overdue amounts or amounts covering returned, previously dishonored or stop-payment checks (e.g. where the card is used as a payment of last resort);



- amounts that represent repayment of a cash advance including, but not limited to, payday loans, pawn loans or payday advances;
- sales made by third parties or entities conducting business in industries other than yours; or
- other items of which American Express or we notify you.

You must not use a card to verify a cardholder's age.

Authorization for Card Not Present transactions

If you process a Card Not Present transaction you must obtain the following information:

- the card number;
- the card expiration date;
- the cardholder's name as it appears on the card;
- the cardholder's billing address; and
- the delivery address if different from the billing address.

In addition, for Internet transactions you must:

- use any separate merchant numbers (Seller ID) established for your Internet orders in all of your requests for authorization and Submission of charges;
- provide us with at least one (1) month's prior written notice of any change in your Internet address; and
- comply with any additional requirements that American Express provides from time to time.

American Express has the right to chargeback for any Card Not Present transaction that the cardholder denies making or authorizing. However, American Express will not chargeback for any Card Not Present transaction based solely upon a claim by a cardholder that he or she did not receive the disputed goods if you have:

- verified the address to which the goods were shipped was the cardholder's full billing address; and
- provided proof of delivery signed by the cardholder or an authorized signer of the card indicating the delivery of the goods or services to the cardholder's full billing address.

American Express will not be liable for actual or alleged fraudulent transactions over the Internet and will have the right to chargeback for those charges.

If a disputed transaction arises involving a Card Not Present transaction that is an Internet electronic delivery transaction, American Express may exercise a chargeback for the full amount of the transaction and place you in any of its chargeback programs.

Charge records (also known as 'sales drafts')

For each transaction submitted:

- electronically - you must create an electronically reproducible charge record; and
- on paper - you must create a charge record containing all of the following required data:
 - full card number and expiration date, and if available, cardholder name;
 - the date the transaction was incurred;
 - the amount of the transaction, which must be the total price for the purchase of goods and services (plus applicable taxes and gratuities) purchased on the card;



- the authorization approval;
- a clear description of the goods and services purchased by the cardholder;
- an imprint or other descriptor of your name, address, merchant number and, if applicable, store number;
- the words “No Refunds” if you have a no refund policy, and your return and/or cancellation policies; and
- the cardholder’s signature (if a Card Present transaction), or the words “telephone order,” “mail order,” “Internet Order,” or “signature on file,” as applicable (if a Card Not Present transaction).

In the charge record (and a copy of the customer’s receipt) you must:

- include your return and/or cancellation policies; and
- mask truncated card number digits with replacement characters such as “x,” “*” or “#,” and not blank spaces or numbers.

If the cardholder wants to use more than one card for payment of a purchase, you may create a separate charge record for each card used. However, if the cardholder is using a single card for payment of a purchase, you must not divide the purchase into more than one transaction, and you must not create more than one charge record.

Refunds

To issue a refund you must:

- compare the last four digits on the charge record against the card presented (when applicable);
- issue the credit in the currency in which the original transaction was submitted to us; and
- issue the credit to the card used to make the original purchase. If the credit is for the return of a gift by someone other than the cardholder who made the original purchase, you must apply your usual refund policy.

If the cardholder indicates that the card on which the purchase was originally made is no longer active or available:

- for all cards except prepaid cards - advise the cardholder that you must issue the credit to that card; and if the cardholder has questions, advise him or her to call the Customer Service number on the back of the card in question; and
- for prepaid cards - apply your usual refund policy for returns.

In the credit draft delivered to the cardholder you must mask truncated card number digits with replacement characters such as “x,” “*” or “#,” and not blank spaces or numbers.

Your refund policy for card transactions must be at least as favorable as your refund policy for purchases made with other payment products or other payment methods.

If you issue a credit, American Express will not refund the discount or any other fees or assessments previously applied on the corresponding transaction. The discount on chargebacks will not be refunded.



Fraud mitigation tools

American Express offers fraud mitigation tools for both Card Present and Card Not Present transactions to help verify that a transaction is valid. These tools help you mitigate the risk of fraud at the point of sale, but are not a guarantee that a transaction is in fact valid or bona fide, or that you will not be subject to a chargeback. For optimal use of the tools, please visit American Express' Fraud Prevention Information at: www.americanexpress.com/fraudinfo.

Recurring transactions

For recurring transactions you must offer the cardholder the option to receive written notification for the recurring transaction(s) at least (10) ten days prior to submitting, or any time the transaction amount exceeds a maximum amount that has been set by the cardholder. You must clearly and conspicuously disclose all material terms of the option, including, if applicable, the fact that recurring billing will continue until the option is canceled by the cardholder. If the material terms of the option change after submission of the first recurring transaction, you must promptly notify the cardholder in writing of such change and obtain the cardholder's express written consent to the new terms prior to submitting another recurring transaction.

For recurring transactions you must:

- periodically verify with cardholders that their information (e.g. card number, expiration date, billing address) is still accurate. This will improve the likelihood of obtaining an approval to an authorization request;
- retain evidence of consent to receive updated card account information from the card-issuing bank for twenty-four (24) months from the date you submit the last recurring transaction.
- ensure that your process for cancellation of recurring transactions is simple and expeditious; and
- within twenty-four (24) hours of incurring the first recurring billing transaction, provide the cardholder written confirmation (e.g. email or facsimile) of such transaction, including all material terms of the option and details of your cancellation/refund policy.

If your recurring transaction amounts vary, you must offer the cardholder the right to receive written notification of the amount and date of each recurring transaction:

- at least ten (10) days before submitting each transaction; or
- whenever the amount of the transaction exceeds a maximum recurring transaction amount specified by the cardholder.

Keyed transactions

There are instances when you will need to key-enter an in-person transaction. This occurs most often when the POS system cannot read the card. If the card cannot be read electronically, you must:

- verify that the card is not visibly altered or mutilated;
- verify that the customer is the cardholder, except for where the cardholder name is not captured on the charge record or for prepaid cards that do not show a name on their face, in which case this is not necessary;
- key-enter the data;
- obtain an authorization approval;



- unless you and the transaction qualify for the No Signature Program, obtain signature and verify that the signature is identical to the name on the card, except for where the cardholder name is not captured on the charge record or for prepaid cards that do not show a name on their face, in which case this is not necessary;
- compare the signature (when obtained) on the charge record with the signature on the card;
- verify the card's expiration date;
- match the card number and the expiration date on the card to the same information on the charge record; and
- validate the card's presence by taking an imprint of the card (the imprint is for your records)

Prepaid cards

American Express prepaid cards can be identified because the American Express "Blue Box" logo appears either on the face or back of the card.

Prepaid cards are valid through the date on the card, and most prepaid cards can be used for both in-store and online purchases.

A prepaid card must be tendered for an amount that is no greater than the funds available on the card. Instruct cardholders that, before making a purchase, they must check their remaining funds by calling the twenty-four (24)-hour, toll-free number on the back of the card. Because prepaid cards are pre-funded, if you receive a decline when seeking authorization, ask the cardholder to call the toll-free number on the back of the card to confirm that the purchase price does not exceed the available funds on the prepaid card. If the prepaid card does not have enough funds to cover the purchase price, process a split tender transaction or request an alternative form of payment.

To accept a prepaid card:

- swipe the prepaid card at the point of sale just like any other card; and
- create a transaction record as you would for any other card.

If your return policy for prepaid cards is different from your standard return policy, you must:

- clearly disclose your return policy for prepaid cards to the cardholder at the time of purchase; and
- ensure that your return policy for prepaid cards is printed on all transaction receipts and charge records that you provide to cardholders.

For more information about processing prepaid cards:

- call the Customer Service number on the back of the card in question; and/or
- see American Express Card Organization Rules regarding "additional authorization requirements."

Contact Chip Card transactions

When presented with a chip card to be inserted into a POS device, you must:

- verify that the card is not visibly altered or mutilated;
- verify that the customer is the cardholder, except for where the cardholder name is not captured on the charge record or for prepaid cards that do not show a name on their face, in which case this is not necessary;
- capture chip card data by inserting the card into the POS device;



- obtain an authorization approval;
- verify the card's expiration date;
- match the card number and the expiration date on the card to the same information on the charge record; and
- ensure the name that prints on the charge record matches the name on the front of the card.

In terms of capturing chip card data, the POS system will advise cardholders to enter their PIN (a Chip and PIN transaction) or sign for the transaction (a Chip and signature transaction):

Chip and PIN transactions: Cardholders must enter their PIN into the POS system using the keypad. If the transaction cannot be completed due to a technical problem, the POS system will show an error message, in which case you must follow the procedures for a swiped transaction, "magnetic stripe card charges".

Chip and signature transactions: Unless you and the transaction qualify for the No Signature Program, you must obtain the cardholder's signature on the charge record and compare the signature on the charge record to the name and signature on the card, except for where the cardholder name is not captured on the charge record or for prepaid cards that do not show a name on their face, in which case this is not necessary.

No Signature Program

You may participate in the No Signature Program under which you are not required to request a signature from cardholders on the transaction record provided that:

- your business is classified in an industry that accepts in-person charges, with the exception of the following categories:
 - Merchants who do not conduct in-person charges (i.e., Internet, mail order or telephone order).
 - prohibited merchants or prohibited transactions (or both) as defined in American Express Card Organization Rules regarding "risk evaluation." Please refer to the Prohibited activities section above.
 - high risk Merchants (e.g. Internet electronic services or nightclubs/lounges) as defined in American Express Card Organization Rules regarding "high risk merchants."
 - Merchants placed in our Fraud Full Recourse Program. See American Express Card Organization Rules regarding "chargeback programs."
- in relation to the transaction:
 - the transaction amount must meet the threshold established in American Express' country specific policy.
 - the transaction must include the appropriate indicator to reflect that the card and the Cardholder were present at the point of sale.
 - the transaction must include a valid approval.

Under the American Express No Signature Program, chargebacks will not be exercised for such charges based solely on your failure to obtain the cardholder's signature at the point of sale.

If a disproportionate number of disputed charges under the No Signature Program occurs, you must cooperate to reduce the number of disputed charges. If such efforts fail, you may be placed in American Express chargeback programs, or your participation in the No Signature Program may be modified or terminated.



Keyed No Imprint

To participate in the Keyed No Imprint Program under which you may submit in-person transactions without taking an imprint of the card you must:

- key-enter the transaction;
- include in the transaction the appropriate indicator to reflect that the card and the cardholder were present at the point of sale;
- include in the transaction a valid approval; and
- confirm the 4-digit Card Identification (CID) on the front of the card as a positive match.

Under the Keyed No Imprint Program, chargebacks will not be permitted based solely on your failure to obtain an imprint of the card.

If a disproportionate number of disputed transactions under the Keyed No Imprint Program occurs, you must cooperate to reduce the number of disputed transactions. If such efforts fail, you may be placed in any of American Express' chargeback programs or your participation in the Keyed No Imprint Program may be modified or terminated.

Mobile contactless charges

If a cardholder uses a mobile phone at the point of sale for an American Express mobile contactless transaction you must:

- capture the magnetic stripe or chip card data by waving the contactless-enabled mobile phone in close proximity to the contactless reader;
- obtain an authorization approval;
- obtain signature (excluding charges at CATs), unless the transaction qualifies for the American Express No Signature Program; and
- compare the signature (when obtained) on the charge record with the signature on the companion physical card or a valid form of formal identification (e.g. driver's license).

Travelers cheques

Travelers cheques are available in various denominations and currencies. The denominations in US dollars range from \$20 to \$1000.

You must exercise caution when presented with a travelers cheque in a denomination of \$500 or greater. The higher-denominated travelers cheques are rarely sold, and so more likely to be counterfeit.

To accept a travelers cheque, watch your customer countersign in the lower left corner of the travelers cheque, and compare the countersignature to the signature in the upper left corner of the travelers cheque.

- if the signature and countersignature are a reasonable match (they look alike, but may not be identical), you may accept the cheque and there is no need to obtain any identification.
- if you suspect that the countersignature may be false, or you did not watch the customer countersign, ask your customer to turn the cheque over and sign again across the left-hand side (in the same manner one typically endorses a check); then take the cheque and fold up the bottom right-hand corner so that you can compare the original signature with the new one.
- if the signatures are not the same, or you have any questions regarding the validity of the cheque, call Customer Service.



- if you suspect that the travelers cheque may be fraudulent, verify that the cheque is authentic by:
 - performing the smudge test. Turn the cheque over (non-signature side). Wipe a moistened finger across the denomination.
 - on the right side of the cheque, the ink should not smudge.
 - on the left side of the cheque, the ink should smudge.
 - obtaining online Authorization at www.americanexpress.com/verifyamextc.

You are not required to obtain authorization before accepting a travelers cheque.

High CV Merchants

You acknowledge that you will be converted from the American Express US Enhanced Acquisition Program to a direct card acceptance relationship with American Express if and when you become a 'High CV Merchant' in accordance with the American Express Card Organization Rules. As part of this acknowledgment you agree that upon conversion: (i) you will be bound by American Express' then-current agreement for card acceptance; and (ii) American Express will set pricing and other fees payable by you for card acceptance.

A 'High CV Merchant' is a merchant with either (i) greater than \$1,000,000 in charge volume in a rolling twelve (12) month period or (ii) greater than \$100,000 in charge volume in any three (3) consecutive months. For clarification, if a merchant has multiple establishments, the charge volume from all establishments shall be summed to together when determining whether the merchant has exceeded the thresholds above.

Marketing opt-outs

You agree that when providing your contact information to us that you may receive messages from American Express, including important information about American Express products, services, and resources available to your business. These messages may be sent to the phone numbers, email addresses or fax numbers that you provide. If you provide a wireless phone number, you agree that you may be contacted at that number and the communications sent may include autodialed short message service (SMS or "text") messages or automated or pre-recorded calls. If you provide a fax number, you agree that you may be sent fax communications. American Express may otherwise use and share your information for business purposes and as permitted by applicable law. American Express uses reasonable administrative, technical and physical security measures to protect your information consistent with the sensitivity of the information.

You may opt out of newsletters or messages about products, services and resources for different forms of communications by contacting us, via inbound telephone, email, facsimile, website and any other means identified by us, or by exercising the opt-out options that may be described or offered in emails, SMS messages, faxes or other communications. If you opt out, you may still receive messages from American Express regarding services and programs designed to enhance the value of the American Express Network.



PART B: PROTECTING AMERICAN EXPRESS CARD MEMBER INFORMATION

These merchant data security requirements apply to all of your equipment, systems, and networks on which encryption keys, cardholder data and/or sensitive authentication data are stored, processed, or transmitted.

Standards for protection of cardholder data and sensitive authentication data

You must, and you must ensure that all of your employees, agents, representatives, subcontractors, processors, service providers, providers of point-of-sale equipment or systems or payment processing solutions, and any other party to whom you may provide card member information access, will:

- store American Express cardholder data only to facilitate transactions for your acceptance of American Express cards;
- comply with the current version of the Payment Card Industry Data Security Standard (“PCI DSS”), which is available at www.pcisecuritystandards.org, no later than the effective date for implementing that version; and
- use, when deploying new or replacement PIN entry devices or payment applications (or both), only those that are PCI-Approved.

You must protect all charge records and credit records retained in accordance with these data security provisions. You must use these records only for purposes of your acceptance of American Express cards and you must safeguard the records accordingly.

Data incidents

If you discover a data incident, you must:

- you must notify us immediately and in no case later than twenty-four (24) hours after such discover;
- conduct a thorough forensic investigation of each data incident; this must be conducted by a PCI forensic investigator (PFI) if the data incident involves 10,000 or more unique card numbers (or otherwise at our request);
- promptly provide to us all compromised card numbers and the forensic investigation report of the data incident;
- work with us to rectify any issues arising from the data incident, including consulting with us about your communications to card members affected by the data incident and providing (and obtaining any waivers necessary to provide) to us all relevant information to verify your ability to prevent future data incidents; and
- at our request, provide validation by a qualified security assessor (QSA) that the deficiencies have been remediated.

Forensic investigation reports must:

- include forensic reviews, reports on compliance, and all other information related to the data incident;
- identify the cause of the data incident;
- confirm whether or not you were in compliance with the PCI DSS at the time of the data incident: and
- verify your ability to prevent future data incidents by providing a plan for remediating all PCI DSS deficiencies.



American Express has the right to disclose information about any data incident to card members, issuers, other participants on the American Express network, and the general public as required by applicable law, by judicial, administrative, or regulatory order, decree, subpoena, request, or other process; in order to mitigate the risk of fraud or other harm; or otherwise to the extent appropriate to operate the American Express network.

Periodic validation of your systems

You must take steps to validate under PCI DSS annually and quarterly the status of your equipment, systems and/or networks (and their components) on which cardholder data and/or sensitive authentication data are stored, processed or transmitted.

Step 1 – Enroll in a compliance program

You must submit applicable periodic validation documentation to us. Please contact us for more information regarding data security compliance requirements.

Step 2 – Determine merchant level and validation requirements

Most merchant levels are based on the volume of transactions submitted by establishments. You will fall into one of the merchant levels specified in the following table:

Merchant level	Definition	Validation documentation	Requirement
1	2.5 million transactions or more per year; or any merchant that American Express otherwise deems a level 1 merchant	Annual on-site security assessment report and quarterly network scan	Mandatory
2	50,000 to 2.5 million transactions per year	Annual self-assessment questionnaire (SAQ) and quarterly network scan	Mandatory
3	Less than 50,000 transactions per year	Annual SAQ and quarterly network scan	Strongly recommended
3*	Less than 50,000 transactions per year and designated a level 3 merchant by American Express	Annual SAQ and quarterly network scan	Mandatory

– As designated by American Express.



American Express may require certain level 3 merchants to enroll in American Express' compliance program. Such merchants must enroll no later than ninety (90) days following receipt of such notice from us. All other level 3 merchants need not submit validation documentation, but must comply with all other provisions of these data security provisions.

The validation documentation which you must send to us is as follows:

Annual onsite security assessment	Annual self-assessment questionnaire	Quarterly network scans
<p>This is a detailed onsite examination of your equipment, systems, and networks (and their components) where cardholder data or sensitive authentication data (or both) are stored, processed, or transmitted.</p> <p>You must:</p> <ul style="list-style-type: none"> ensure that the annual onsite security assessment is performed by (i) a QSA, or (ii) you and certified by your chief executive officer, chief financial officer, chief information security officer or principal; submit the AOC section of the SAQ annually to us, and include copies of the full SAQ upon request; and ensure that the AOC certifies compliance with all requirements of the PCI DSS. 	<p>This is a process using the PCI DSS self-assessment questionnaire (SAQ) that allows self-examination of your equipment, systems, and networks (and their components) where cardholder data or sensitive authentication data (or both) are stored, processed, or transmitted.</p> <p>You must:</p> <ul style="list-style-type: none"> ensure that the SAQ is performed by you and certified by your chief executive officer, chief financial officer, chief information security officer or principal; submit the AOC section of the SAQ annually to us, and include copies of the full SAQ upon request; and ensure that the AOC of the SAQ certifies compliance with all requirements of the PCI DSS. 	<p>The quarterly network scan is a process that remotely tests your Internet-connected computer networks and web servers for potential weaknesses and vulnerabilities.</p> <p>You must:</p> <ul style="list-style-type: none"> ensure that the quarterly network scan is performed by an approved scanning vendor (ASV); complete and submit the ASV scan report attestation of scan compliance (AOSC) or executive summary of findings of the scan (and copies of the full scan, on request) quarterly to us; ensure that the AOSC or executive summary certifies that (i) the results satisfy the PCI DSS scanning procedures, (ii) no high risk issues are identified, and (iii) the scan is passing or compliant.

Step 3 – Send the validation documentation to Participant

Compliance and validation are completed at your expense. By submitting validation documentation to us, you represent and warrant to us that you are authorized to disclose the information contained in it and are providing the validation documentation without violating any other party's rights.

Merchants not compliant with PCI DSS

If you are not compliant with the PCI DSS, then you must:

- complete and submit an AOC including "Part 4. Action Plan for Non-Compliant Status" to us;
- designate a remediation date, not to exceed twelve (12) months following the date of the AOC, for achieving compliance; and
- provide us with periodic updates of your progress toward remediation under the "Action Plan for Non-Compliant Status."



Non-validation fees and termination of right to accept cards

We have the right to impose non-validation fees on you and terminate your right to accept cards if you do not fulfill these requirements or fails to provide the mandatory validation documentation to us by the applicable deadline.

We will notify you separately of the applicable deadline for each annual and quarterly reporting period. If we do not receive your mandatory validation documentation, then we have the right to terminate your right to accept cards and to impose non-validation fees on you.

Periodic validation of level EMV merchants

Your merchant level may be classified as EMV if you submit 50,000 (or more) American Express card transactions per year, of which at least seventy-five percent (75%) are made by the card member with the physical card present at a point of sale system compliant with EMV specifications and capable of processing contact and contactless transactions on a chip-enabled device.

If you are classified as merchant level EMV, you may submit the annual EMV attestation (AEA) instead of other validation documentation, in which case you must submit the AEA annually to us. Even if you fall into merchant level 1 or 2, if you are classified as merchant level EMV, you only need to submit the AEA, and not the other merchant level 1 and 2 validation documentation.

The AEA involves a process using PCI DSS requirements that allows self-examination of your equipment, systems, and networks (and their components) where cardholder data or sensitive authentication data (or both) are stored, processed or transmitted.

The AEA must:

- be performed by you;
- be certified by your chief executive officer, chief financial officer, chief information security officer, or principal; and
- certify that you meet the requirements for merchant level EMV.

PART C: ADDITIONAL PROVISIONS APPLICABLE TO MERCHANTS IN CERTAIN INDUSTRIES

The following provisions also apply to merchants who are categorised as being in the industries stated below:

Auto dealer industry

The following requirements will apply to charges for the down payment or the entire purchase price of new and used motor vehicles.

You may accept the card for down payment of a motor vehicle, subject to the following provisions:

- you must not submit a charge for the down payment price of a used motor vehicle unless and until you have a written agreement/bill of sale signed by the cardholder setting forth the terms of the sale, including down payment price, and your cancellation policy.
- In addition to our other chargeback rights, American Express also has chargeback rights for any portion of the charge for the down payment price of a used motor vehicle that is disputed by the cardholder, if such disputed charge cannot be resolved in your favor based upon unambiguous language contained in the written agreement/bill of sale.

If a cardholder exercises his or her right to rescind the written agreement/bill of sale during any rescission period set out in the cardholder's agreement with you or at law, you must submit a credit to us promptly.

If American Express has classified you as an auto dealer of used motor vehicles exclusively, the down payment must not exceed 50% of the full purchase price of the motor vehicle.



If the cardholder denies making or authorizing the charge, American Express will have chargeback rights for such charge in addition to our other chargeback rights

You may also accept the card for the entire purchase price of a new or used motor vehicle, subject to the following provisions:

- you are classified as an auto dealer of new or new and used motor vehicles (i.e. Your dealership sells new motor vehicles exclusively or both new and used motor vehicles).
- the amount of the charge does not exceed the total price of the motor vehicle after deduction of applicable discounts, taxes, rebates, cash down payments, and trade-in values.
- you must not submit a charge for the entire purchase price of a new or used motor vehicle unless and until you have a written agreement/bill of sale signed by the cardholder setting forth the terms of the sale, including purchase price, delivery date and your cancellation policy.

In addition to other chargeback rights, American Express also has chargeback rights for any portion of the charge for the entire purchase price of a new or used motor vehicle which is disputed by the cardholder, if such disputed charge cannot be resolved in your favor based upon unambiguous language contained in the written agreement/bill of sale.

If the cardholder denies making or authorizing the charge and you have not transferred title or physical possession of the motor vehicle to the cardholder, American Express will have chargeback rights for such charge in addition to its other chargeback rights.

Business-to-business (B2B)/ wholesale distribution industries

If you are classified in the business-to-business (B2B) or wholesale distribution industries, and American Express determines that you are not in the telecommunications industry, then notwithstanding the prohibition in the section entitled "Prohibited Uses of the Card", you may accept the card for overdue amounts to the extent that acceptance of overdue amounts is a common practice in your industry and does not constitute an attempt to obtain payment from the cardholder whose prior methods of payment have, in American Express' reasonable judgment, been difficult to collect or uncollectible. An indicator of such difficulty, for example, may be the fact that you have sent an overdue customer account to collections.

To minimize your risk of a chargeback with B2B charges, always:

Obtain a signature for all in-person charges. For Card Not Present charges, obtain Proof of Delivery, and Maintain clear and accurate records of orders and returns.

Notwithstanding the restriction in the section entitled "Submission Requirements - Electronic", you must not submit any charge until the goods have been shipped or services have been provided to the cardholder. To the extent that you have clearly disclosed your intentions to the cardholder and the cardholder agrees, then you may submit the following types of charges to us before you ship the goods to the cardholder:

- charges representing deposits on custom and special orders (so long as you comply with applicable law) or goods not in inventory at the time the order is placed; and
- charges representing advance, partial, or full payment for goods that the cardholder asks you to ship at a later date.

Insurance industry

If any of your goods or services are sold or billed by independent agencies, then you must provide to American Express a list of such independent agencies and notify Customer Service of any subsequent changes in the list. American Express may use this list to conduct mailings that encourage such independent agencies to accept the card.



American Express may mention your name in such mailings, and you must provide us with a letter of endorsement or assistance as American Express may require.

You must use your best efforts to encourage independent agencies to accept the card. American Express acknowledges that you have no control over such independent agencies. From time to time, American Express may establish joint marketing campaigns that promote card acceptance specifically at your establishments or, generally, at insurance companies. You may be requested to submit cardholder Information so that American Express can perform back-end analyses to determine the success of such joint marketing campaigns.

American Express undertakes no responsibility on your behalf for the collection or timely remittance of premiums. American Express will not be subject to any liability, under any circumstances, for any claim arising from, or related to, any insurance policy issued by you or your agencies. You must indemnify, defend, and hold harmless American Express and our Affiliates, successors, assigns, and card-issuing banks, from and against all damages, liabilities, losses, costs, and expenses, including legal fees, to cardholders (or former cardholders) arising or alleged to have arisen from the termination by you or your agencies of your right to accept American Express cards or other action regarding their insurance coverage; breach, negligent or wrongful act or omission; failure to perform in accordance with the terms on which you are authorized to accept American Express cards; or failure in the provision of your goods or services.

If the card is accepted as payment for fixed rate cash value life insurance policies or fixed rate annuities in accordance with the terms under which you are authorized to accept American Express cards, you represent and warrant to us that the fixed rate cash value life insurance policies and fixed rate annuities for which the card will be accepted for premium payments are not securities requiring registration under the Securities Act of 1933, and, in addition to your other indemnification obligations to American Express, you must further indemnify, defend, and hold harmless American Express, us and our affiliates, successors, assigns and card-issuing banks from and against all damages, liabilities, losses, costs, and expenses, including legal fees, arising or alleged to have arisen from your breach of such representation and warranty.

Oil and petroleum industry

General

American Express may place you in the Fraud Full Recourse Program if you accept charges originating at a Customer Activated Terminal (CAT) gas pump. American Express will not exercise chargeback up to a certain dollar amount for charges that qualify under the Oil Fraud Protection Program.

If you are classified in the oil and petroleum industry, you must:

- Obtain a unique Merchant Number for your CAT gas pump sales. If you conduct any other business at your establishment (e.g. convenience store sales, car washing services), you must obtain a unique Merchant Number for those lines of business.
- submit dealer location data along with each authorization request and each Submission file. Dealer location data consists of your business':
 - dealer number (store number)
 - name
 - street address
 - city
 - postal code



Recommendations

American Express has implemented several policies and fraud prevention tools to assist in combating fraud at the gasoline pump.

American Express recommends that you:

- set a pre-authorization request of \$100 at your CAT gas pumps.
- for higher charges such as diesel, adjust the pre-authorization amount to accommodate the higher charges.
- set your CAT gas pumps to shut off when they reach the pre-authorization amount.
- request a separate authorization for purchases that exceed the original pre-authorization amount.

Oil fraud protection program

The Oil Fraud Protection Program addresses counterfeit fraud chargebacks at CAT fuel pumps. Under this program American Express will not exercise chargeback for a charge less than \$100 provided that the following criteria are met:

- the authorization request: (i) meets the data requirements for customer activated terminals, and (ii) includes the merchant category code (MCC) 5542 for automated fuel dispensers;
- the card-issuing bank determines that the card used to initiate the charge was counterfeit; and
- you qualified for chargeback protection under the program at the time of the charge.

For an establishment to qualify under the Oil Fraud Protection Program, it (i) must authorize and submit transactions under the unique Merchant Number (Seller ID) assigned to the establishment, and (ii) must have, in a given month, a counterfeit fraud to charge volume ratio below 1%. An establishment whose counterfeit fraud to charge volume ratio rises to or exceeds 1% in a given month will not qualify under the Oil Fraud Protection Program until the ratio falls below 1% for three (3) consecutive months. Notwithstanding the foregoing, the Oil Fraud Protection Program does not apply to Merchants that submit one Merchant Number (Seller ID) consolidated charges from multiple establishments (i.e., central submitters) or to the establishments that those Merchants submit on behalf of.

American Express offers a variety of fraud prevention tools that may enable Merchants to reduce fraud in order to qualify and retain eligibility for the program.

Restaurant and bar industry

If the final restaurant or bar charge is no greater than the amount for which you obtained authorization plus 20% of that amount, no further authorization is necessary.

If the final restaurant or bar charge is greater than the amount for which you obtained authorization by more than 20%, you must obtain authorization for any additional amount of the charge that is greater than the original authorization. When submitting the charge, only include the initial approval.

Telecommunications industry

If American Express classifies you in the telecommunications industry, notwithstanding anything to the contrary in the terms under which you are authorized to accept American Express cards, American Express may place you in one or more of the following chargeback programs:

- partial Immediate chargeback Program for an amount of \$50 or less; or
- Fraud Full Recourse Program



American Express may establish audit procedures determined in American Express' discretion to ensure that no charges except for recurring billing charges are submitted under the Merchant Number designated for recurring billing charges.

The list of Affiliates that you must provide to us under the must include any Agency in the geographic area where you offer any telecommunications services.

Government, utilities and education industries

This section applies to Merchants classified in the government, utilities, or certain education industries (i.e. higher education, private school - kindergarten to grade 12).

Customers must feel free to use all forms of payment that you accept without being penalized for choosing a particular form of payment. To promote customer choice, you are generally prohibited from imposing any restrictions, conditions, or disadvantages when the card is accepted that are not imposed equally on all Other Payment Products.

Merchants in these specific industries may assess convenience fees on charges, provided that they comply with the other requirements of this section, as follows:

- you must not impose a higher convenience fee on charges than it imposes on Other Payment Products, except for Automated Clearing House funds transfers, cash, and checks. American Express views discrimination against cardholders as a breach of the terms under which you are authorized to accept American Express cards.
- Merchants classified as government entities, including government utilities, and privately owned utilities may assess convenience fees on all charges.
- Merchants classified as educational institutions may assess convenience fees only on charges for tuition, room and board, school lunch payments or other mandatory fees.
- you must clearly disclose the amount of convenience fees to the customer and give the customer the opportunity to cancel the charge if the customer does not want to pay the convenience fee.

Any explanation, verbal or written, describing why the convenience fee is being assessed, or how it is calculated, must characterize the convenience fee as an assessment to cover your administrative costs and not as an assessment to cover your cost of accepting the card.

You must obtain separate authorizations and Approval codes for each of the principal charges and the convenience fee. Furthermore, the descriptor on the convenience fee must clearly state that it is a convenience fee (e.g. Official Payments – City of X (principal payment) and Official Payments Convenience Fee (convenience fee)).

Your third party service provider can only assess a convenience fee when it accepts the card for the foregoing charges in compliance with the requirements of this section.

Internet/online pharmacy industry

If it is determined that you are an Internet/online pharmacy merchant that accepts the card for sales of prescription medications (as defined by applicable law) in the Card Not Present environment:

- you must be certified by the Verified Internet Pharmacy Practice Sites program of the National Association of Boards of Pharmacy (www.nabp.net); or
- you or your authorized representative must attest that you comply with the licensing and inspection requirements of (i) US federal law and the state in which you are located, and (ii) each state to which you dispense pharmaceuticals.



Upon request, you must promptly provide documentation to demonstrate that you meet such requirements. Failure to provide this documentation promptly may result in suspension or disenfranchisement of card acceptance privileges. Specific procedures exist for transaction processing by Internet/online Merchants.

Online and/or mail order tobacco and e-cigarette retail industry

You must provide the website address of the online store from which you sell your tobacco products. If your website facilitates tobacco sales, you will be required on request to provide an executed and notarized Affidavit of Compliance with Laws - Online/Mail Order Tobacco.

If you fail to complete the Affidavit, card acceptance privileges may be suspended. American Express may monitor your website.

APPENDIX 3

SPECIAL PROVISIONS FOR DISCOVER NETWORK

DISCOVER NETWORK PROTOCOL FOR INTERNET TRANSACTIONS

Each Internet Discover Network card transaction accepted by you and submitted to us shall comply with Discover Network standards, including, without limitation, Discover Network standards governing the formatting, transmission and encryption of data, referred to as the "designated protocol".

You shall accept only those Internet Discover Network card transactions that are encrypted in accordance with the designated protocol. As of the date of these procedures, the designated protocol for the encryption of data is Secure Socket Layer (SSL).

We may, at our discretion, withhold Settlement until security standards can be verified. However, the designated protocol, including any specifications with respect to data encryption, may change at any time upon thirty (30) days advance written notice. You shall not accept any Internet Discover Network card transaction unless the transaction is sent by means of a browser that supports the designated protocol.

AUTHORIZATIONS

Card Not Present Transactions

For Discover Network Card Not Present transactions, you must also verify the name and billing address of the Discover Network cardholder using the Address Verification System (AVS). If you do not receive a positive match, you must not process the transaction.

Discover Network procedure for request for cancellation of authorization

If a Discover Network card sale is canceled or the amount of the transaction changes following your receipt of authorization for the sale, you must call your Authorization Center directly and request a cancellation of the authorization. An authorization may be canceled at any time within ten (10) days of your receipt of the authorization, but must be canceled before the sales data relating to the transaction is submitted to us, after which the authorization cannot be changed. For an authorization cancellation, you must provide us with the following information, in this order:

- the Discover Network Merchant Number used in the authorization;
- the card number;
- the original amount of the authorization being canceled;
- the new amount of the total transaction (if any);



- the original authorization code for the authorization being canceled;
- the expiration date of the card; and
- a brief reason for the authorization cancellation.

Discover Network Cash Over Transactions

Cash over transactions are only available for Discover Network.

You may issue cash over in connection with a Discover Network card sale, provided that you comply with the terms on which you are authorized to accept cards, including the following requirements:

- you must deliver to us a single authorization request for the aggregate total of the goods/ services purchase amount and the cash over amount of the card sale. You may not submit separate authorization requests for the purchase amount and the cash over amount;
- the sales draft must include both the purchase amount and the cash over amount, and you may not use separate sales drafts for the purchase amount and cash over amount;
- cash over may only be offered with a Card Present card sale that includes a purchase of goods or services by the cardholder. You must not issue cash over as a stand-alone transaction. If you offer cash over, you may require the total amount of a card sale with a credit product, including cash over, to meet a minimum transaction amount of up to \$10. You must not assess or charge fees of any type or amount, including any surcharges, on cash over transactions. You must not include in cash over transactions any of the fees or charges applicable to cash advances;
- cash over may not be dispensed in connection with credits, cash advances, or any card sale for which you are unable to electronically capture Track Data using the POS device; and
- the maximum amount of cash that you may issue as cash over is \$100.

Cash over may not be available in certain markets. Contact us for further information.