American Express
Merchant Operating Guide
Canada
October 2017
### Change Bars
Change bars are vertical lines in the left margin that identify revised, added, or removed text. All changes in the *Merchant Operating Guide* are indicated with a change bar as shown here:

### Summary of Changes Table
Important updates are listed in the following table and are also indicated in the *Merchant Operating Guide* with a change bar.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section/Subsection</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2, &quot;Doing Business with American Express&quot;</td>
<td>Subsection 2.1.1, &quot;Merchant Category Codes&quot;</td>
<td>Added clarification on industry classification and assignment of MCCs.</td>
</tr>
<tr>
<td>Chapter 4, &quot;Transaction Processing&quot;</td>
<td>Subsection 4.3.1.1, &quot;Magnetic Stripe Card Charges&quot;</td>
<td>Added language to reference Section 4.3.3, &quot;Actions for In-Person Charges&quot;.</td>
</tr>
<tr>
<td></td>
<td>Subsection 4.3.1.3, &quot;Contactless Chip Card Charge&quot;</td>
<td>Updated language on accepting Contactless payments.</td>
</tr>
<tr>
<td></td>
<td>Section 4.5, &quot;Processing a Card Not Present Charge&quot;</td>
<td>Added clarification on Transactions that involve goods picked up at a physical store.</td>
</tr>
<tr>
<td></td>
<td>Section 4.17, &quot;Recurring Billing Charges&quot;</td>
<td>Revised requirement for obtaining Cardmember approval for Recurring Billing Charges.</td>
</tr>
<tr>
<td>Chapter 5, &quot;Authorizations&quot;</td>
<td>Section 5.4, &quot;Possible Authorization Responses&quot;</td>
<td>Added tip box to clarify that Voice Authorizations carry a higher risk of fraud.</td>
</tr>
<tr>
<td>Chapter 8, &quot;Protecting Cardmember Information&quot;</td>
<td>Section 8.1, &quot;Data Security Requirements&quot;</td>
<td>Updated language using PCI definitions of protected data.</td>
</tr>
</tbody>
</table>
| | Section 8.2, "Definitions" | Added definition for:  
- Security Technology Enhancement Program (STEP)  
Updated definitions for:  
- Notification Date  
- Validation Documentation |
<p>| | Section 8.6, &quot;Periodic Validation of Merchant Systems&quot; | Added STEP-eligible Merchants to the Merchant Level table. |
| Chapter 9, &quot;Fraud Prevention&quot; | Section 9.5, &quot;Recognizing Suspicious Activity&quot; | Added clarification to Suspicious Activity and added language to tip box. |
| Chapter 10, &quot;Risk Management&quot; | Section 10.2, &quot;Prohibited Merchants&quot; | Updated list of prohibited merchant industries and categories to align with Network policy. |</p>
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section/Subsection</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 11, &quot;Chargebacks and Inquiries&quot;</td>
<td>Section 11.1, &quot;Introduction&quot;</td>
<td>Revised introductory text on when a dispute may be initiated.</td>
</tr>
<tr>
<td></td>
<td>Subsection 11.2.1</td>
<td>Added illustration on the disputed charge process.</td>
</tr>
<tr>
<td>Chapter 12, &quot;Specific Industries&quot;</td>
<td>Section 12.6, &quot;Government/Utilities/Education&quot;</td>
<td>Added language to clarify pricing terms for convenience fees.</td>
</tr>
<tr>
<td></td>
<td>Section 12.10, &quot;Rental Establishments&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 12.11, &quot;Restaurants&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subsection 12.12.2.1, &quot;Vehicle Rentals — Special Authorization Procedures&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subsection 12.12.3, &quot;Assured Reservations&quot;</td>
<td>The Assured Reservation Program has been expanded beyond the lodging industry to include the trailer park/campground, vehicle, bicycle, boat, equipment, motor home, and motorcycle rentals industries.</td>
</tr>
<tr>
<td>Appendix B, &quot;Glossary&quot;</td>
<td></td>
<td>Added definition:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Attestation of Compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Attestation of Scan Compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Contactless</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Expresspay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Merchant Category Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Notification Date</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Validation Documentation</td>
</tr>
</tbody>
</table>
# Table of Contents

1 **Introduction** ........................................ 1  
1.1 About American Express ................................ 2  
1.2 About the Merchant Operating Guide .................... 2  
1.3 Organization of the Merchant Operating Guide ............. 3  
1.4 Changes in the Merchant Operating Guide ................... 3  

2 **Doing Business with American Express** ................. 4  
2.1 Compliance with the Technical Specifications ............... 5  
2.2 Establishment Closing .................................. 5  
2.3 Verification and Disclosure of Information .................. 6  
2.4 Merchant Information: Marketing Communication Opt-Outs . 6  
2.5 List of Merchants ....................................... 6  

3 **Card Acceptance** ...................................... 7  
3.1 Card Acceptance ....................................... 8  
3.2 Treatment of the American Express Brand ................... 8  
3.3 Prohibited Uses of the Card ................................ 9  
3.4 Prohibited Merchants .................................... 10  
3.5 Treatment of American Express Cardmember Information .... 10  

4 **Transaction Processing** ................................ 11  
4.1 Introduction ........................................ 12  
4.2 Completing a Transaction at the Point of Sale ............. 12  
4.3 Processing an In-Person Charge .......................... 13  
4.4 Customer Activated Terminals ............................. 19  
4.5 Processing a Card Not Present Charge ..................... 19  
4.6 Charge Records ........................................ 20  
4.7 Processing a Credit ..................................... 21  
4.8 Credit Records .......................................... 22  
4.9 Return and Cancellation Policies .......................... 23  
4.10 Processing Transactions for Specific Industries ............ 23  
4.11 Reserved ............................................... 23  
4.12 Advance Payment Charges ................................ 24  
4.13 Aggregated Charges .................................... 25  
4.14 Delayed Delivery Charges ................................ 25  
4.15 Keyed No Imprint Program ............................... 26  
4.16 No Signature/No PIN Program ............................ 27  
4.17 Recurring Billing Charges ............................... 28  
4.18 Processing Prepaid Cards ................................ 29  
4.19 Processing Travelers/Gift Cheques ......................... 30
# Table of Contents

5 **Authorizations** .................................................. 32
  5.1 Introduction .................................................. 33
  5.2 Transaction Cycle .............................................. 33
  5.3 The Purpose of Authorization ................................. 33
  5.4 Possible Authorization Responses ............................. 33
  5.5 Obtaining an Electronic Authorization ....................... 34
  5.6 Obtaining a Voice Authorization .............................. 34
  5.7 Card Identification (CID) Number ............................ 35
  5.8 Authorization Reversal ......................................... 35
  5.9 Authorization Time Limit ...................................... 35
  5.10 Floor Limit .................................................. 36
  5.11 Pre-Authorization ............................................. 36
  5.12 Additional Authorization Requirements ...................... 36

6 **Submissions** ................................................... 37
  6.1 Introduction .................................................. 38
  6.2 Transaction Cycle .............................................. 38
  6.3 Purpose of Submission ......................................... 38
  6.4 Submission Requirements – Electronic .......................... 38
  6.5 Submission Requirements – Paper ............................. 39
  6.6 How to Submit ................................................ 40

7 **Settlement** ...................................................... 41
  7.1 Introduction .................................................. 42
  7.2 Payment Errors or Omissions ................................... 42
  7.3 Collecting from Cardmembers .................................. 42

8 **Protecting Cardmember Information** ......................... 43
  8.1 Data Security Requirements ................................... 44
  8.2 Definitions .................................................. 44
  8.3 Standards for Protection of Cardmember Information ....... 47
  8.4 Data Incident Management Obligations ....................... 48
  8.5 Reserved .................................................... 48
  8.6 Periodic Validation of Merchant Systems ..................... 48
  8.7 Reserved .................................................... 52
  8.8 Disclaimer .................................................. 52

9 **Fraud Prevention** ............................................... 53
  9.1 Introduction .................................................. 54
  9.2 Strategies for Deterring Fraud ................................ 54
  9.3 Card Acceptance Policies ..................................... 55
  9.4 Card Security Features ....................................... 56
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5 Recognizing Suspicious Activity</td>
<td>58</td>
</tr>
<tr>
<td>9.6 Prepaid Card Security Features</td>
<td>59</td>
</tr>
<tr>
<td>9.7 Recognizing Suspicious Activity for Prepaid Cards</td>
<td>59</td>
</tr>
<tr>
<td>9.8 Travelers Cheque and Gift Cheque Security Features</td>
<td>59</td>
</tr>
<tr>
<td>9.9 Fraud Mitigation Tools</td>
<td>61</td>
</tr>
<tr>
<td>10 Risk Management</td>
<td>64</td>
</tr>
<tr>
<td>10.1 Introduction</td>
<td>65</td>
</tr>
<tr>
<td>10.2 Prohibited Merchants</td>
<td>65</td>
</tr>
<tr>
<td>10.3 Monitoring</td>
<td>67</td>
</tr>
<tr>
<td>10.4 Fraudulent, Deceptive, or Unfair Business Practices, Illegal Activities, or Prohibited Uses of the Card</td>
<td>69</td>
</tr>
<tr>
<td>11 Chargebacks and Inquiries</td>
<td>70</td>
</tr>
<tr>
<td>11.1 Introduction</td>
<td>71</td>
</tr>
<tr>
<td>11.2 Disputed Charge Process</td>
<td>71</td>
</tr>
<tr>
<td>11.3 Tips for Avoiding Chargebacks</td>
<td>72</td>
</tr>
<tr>
<td>12 Specific Industries</td>
<td>73</td>
</tr>
<tr>
<td>12.1 Introduction</td>
<td>74</td>
</tr>
<tr>
<td>12.2 Auto Dealers</td>
<td>74</td>
</tr>
<tr>
<td>12.3 Business-to-Business (B2B) Wholesale Distribution</td>
<td>75</td>
</tr>
<tr>
<td>12.4 Charitable Donations</td>
<td>76</td>
</tr>
<tr>
<td>12.5 E-Commerce Businesses</td>
<td>76</td>
</tr>
<tr>
<td>12.6 Government/Utilities/Education</td>
<td>76</td>
</tr>
<tr>
<td>12.7 Insurance</td>
<td>77</td>
</tr>
<tr>
<td>12.8 Oil/Petroleum</td>
<td>77</td>
</tr>
<tr>
<td>12.9 Parking</td>
<td>78</td>
</tr>
<tr>
<td>12.10 Rental Establishments</td>
<td>78</td>
</tr>
<tr>
<td>12.11 Restaurants</td>
<td>79</td>
</tr>
<tr>
<td>12.12 Travel Industries</td>
<td>79</td>
</tr>
<tr>
<td>13 Dispute Resolution</td>
<td>87</td>
</tr>
<tr>
<td>13.1 Arbitration Agreement (as to Claims involving American Express)</td>
<td>88</td>
</tr>
<tr>
<td>Appendix A</td>
<td></td>
</tr>
<tr>
<td>Acknowledgement of Responsibility</td>
<td>90</td>
</tr>
<tr>
<td>Appendix B</td>
<td></td>
</tr>
<tr>
<td>Glossary</td>
<td>92</td>
</tr>
</tbody>
</table>
Contents

1.1 About American Express
1.2 About the Merchant Operating Guide
1.3 Organization of the Merchant Operating Guide
1.4 Changes in the Merchant Operating Guide
1.1 About American Express

American Express was established more than 150 years ago and has undergone remarkable changes over the years. One characteristic has remained constant, however: American Express is guided by a value system that is steadfastly focused on doing business in more than 130 countries around the globe with trust and integrity, delivering quality products and services to American Express' valued customers.

The American Express Network operates worldwide, including in Territories where Applicable Law, or other considerations, may require that certain of our Affiliates or licensees act as Acquirers. The Network also supports millions of Merchants globally and processes billions of Transactions daily, forging relationships between Cardmembers and Merchants. American Express helps build the businesses of millions of Merchants, from neighbourhood shops to multinational corporations.

As a world-recognized brand leader, American Express takes its commitment to Merchants seriously. This guide is designed to provide information about American Express and how accepting the American Express® Card can benefit Merchants.

1.1.1 Intended Audience for this Guide

This Merchant Operating Guide is intended for use by Canadian Merchants that have entered into a legally binding Agreement with a Merchant Services Provider based in Canada to accept the American Express® Card. While not an exhaustive list, qualifying Merchants:

- are physically located in Canada and maintain a bank account at a Canadian financial institution;
- have an estimated annual American Express charge volume of less than CAD $500,000; and,
- transact in Canadian currency (CAD) only and receive payment from its Merchant Services Provider in Canadian dollars into a Canadian bank account.

This Merchant Operating Guide governs your acceptance of the American Express Card in Canada. If you are a US-based Merchant operating under an Agreement with a US-based Merchant Services Provider, click this link to download the American Express Merchant Operating Guide for the policies and procedures governing your acceptance of the American Express Card in the US.

Amex Bank of Canada is a licensed user of the American Express Network and provides access to qualified Merchant Services Providers that have entered into a Program Agreement and comply with the American Express® Technical Specifications.

1.2 About the Merchant Operating Guide

This Merchant Operating Guide sets forth the policies and procedures governing your acceptance of the American Express® Card in Canada. It is a part of, and is hereby incorporated by reference into, the Merchant Agreement with your Merchant Services Provider ("the Agreement"). You agree to be bound by and accept all provisions in the Merchant Operating Guide (as changed from time to time) as if fully set out in the Agreement and as a condition of your agreement to accept the Card.
You should consult with your Merchant Services Provider for further information about any policy or procedure contained in the Merchant Operating Guide.

1.3 Organization of the Merchant Operating Guide

The Merchant Operating Guide is designed to follow the flow of the Transaction cycle – from Card acceptance, to Authorization, to Submission, to Settlement, to Disputed Charges, to Chargebacks.

1.4 Changes in the Merchant Operating Guide

American Express reserves the right to make changes to the Merchant Operating Guide in scheduled changes and at any time in unscheduled changes. You agree to accept all changes (and further to abide by the changed provisions of the Merchant Operating Guide) as a condition of your agreement to accept the Card, except where Applicable Law takes precedence.

The Merchant Operating Guide is published in electronic format on a scheduled basis, twice each year, in April and October. You may obtain the latest version of the American Express Merchant Operating Guide by visiting www.americanexpress.ca/merchantguide, or by contacting your Merchant Services Provider.

Provisions changed in unscheduled releases generally take effect ninety (90) days after notice to Merchants and Merchant Services Providers (unless another effective date is specified in the notice).

Upon notification of an unscheduled change, you shall be responsible for obtaining and referring to the then-current version of the Merchant Operating Guide.
Contents

2.1 Compliance with the Technical Specifications
2.2 Establishment Closing
2.3 Verification and Disclosure of Information
2.4 Merchant Information: Marketing Communication Opt-Outs
2.5 List of Merchants
2.1 Compliance with the Technical Specifications

You must ensure that you and any third parties you enlist to facilitate Transaction processing comply with the American Express Technical Specifications (valid and accurate data must be provided for all data elements in accordance with the American Express Technical Specifications).

Contact your Merchant Services Provider for further information about complying with these specifications.

2.1.1 Merchant Category Codes

You must use the Merchant Category Code (MCC) that most closely represents your industry classification. If you have multiple, clearly distinct businesses, then those businesses should be segmented across the appropriate MCCs and Merchant Numbers. If you have multiple businesses, but a distinction between them is not clear or cannot reasonably be determined, then you should use the MCC which most closely represents your business’s primary industry classification.

You must make sure your MCCs are accurate and provide the appropriate MCC in all Authorizations and Submissions. Work with your Merchant Services Provider if you have questions related to your MCC assignment.

2.2 Establishment Closing

If you close any of your Establishments, you must follow these guidelines:

- Follow your Merchant Services Provider guidelines for notification of Establishment closing.
- Policies must be conveyed to the Cardmember prior to completion of the Charge and printed on the copy of a receipt or Charge Record the Cardmember signs. See Section 4.9, “Return and Cancellation Policies” for additional information.
- If not providing refunds or exchanges, post notices indicating that all sales are final (e.g., at the front doors, by the cash registers, on the Charge Record and on websites and catalogues).
- Return and cancellation policies must be clearly disclosed at the time of sale.
- For Advance Payment Charges or Delayed Delivery Charges, you must either deliver the goods or services for which you have already charged the Cardmember or issue Credit for any portion of the Charge for which you have not delivered the goods or services.
2.3 Verification and Disclosure of Information

You acknowledge that when you provide information to your Merchant Services Provider that such information may be disclosed and shared with your Merchant Services Provider’s agents, subcontractors, Affiliates, and other parties, including American Express, industry organizations, and reporting agencies, for any purpose permitted by Applicable Law.

You further acknowledge that, by entering into the Agreement with your Merchant Services Provider, you provide permission to obtain or disclose information in connection with the Agreement, release and waive any right or Claim arising out of or related to such disclosure, including defamation Claims, even if the information that is disclosed is incorrect or incomplete. You hereby specifically consent to the reporting, and waive and hold American Express and your Merchant Services Provider harmless from all Claims and liabilities you may have as a result of such reporting.

2.4 Merchant Information: Marketing Communication Opt-Outs

You agree that, upon providing contact information to your Merchant Services Provider, American Express may send you commercial marketing messages, including information on products, services, and resources available to your business. These messages may be sent to the mailing address, phone numbers, email addresses, or fax numbers you provide. If you provide a wireless phone number, you agree that American Express may contact you at that number and the communication American Express sends may include autodailed short message service (SMS or “text”) messages or automated or prerecorded calls. If you provide a fax number, you agree that American Express may send you 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 Merchant information consistent with the sensitivity of the information.

You may opt out of receiving American Express commercial marketing communications about products and services by contacting your Merchant Services Provider directly via inbound telephone, email, website, or any other means identified by your Merchant Services Provider, or by exercising any opt-out option that American Express may describe or offer in emails, SMS messages, faxes, or other communications. If you have opted-out, you may continue to receive important transactional or relationship communications from American Express. In addition, you may continue to receive marketing communications from American Express while American Express updates its records to reflect your opt-out choice.

2.5 List of Merchants

For the purpose of communicating your acceptance of the Card, American Express may include your name, address (including website addresses or URLs), customer service telephone numbers, and/or industry classification in lists of Merchants that accept the Card. The information reflected on such lists is based on that which you have provided to your Merchant Services Provider, or that is otherwise publicly available. American Express may publish or publicly disclose that information from time to time.
Contents

3.1 Card Acceptance
3.2 Treatment of the American Express Brand
3.3 Prohibited Uses of the Card
3.4 Prohibited Merchants
3.5 Treatment of American Express Cardmember Information
3.1 Card Acceptance

You must accept the Card as payment for goods and services sold (other than those goods and services prohibited under Section 3.3, ”Prohibited Uses of the Card”), or (if applicable) for charitable contributions made, at all of your Establishments, except as expressly permitted by Applicable Law. You are jointly and severally liable for the obligations of your Establishments under the Agreement.

By accepting the Card at your Establishment, you are providing your customers with convenience and flexibility in the choice of payment methods offered.

3.1.1 Japan Credit Bureau

American Express has an established relationship with Japan Credit Bureau (JCB), one of the largest card issuers in the world, whereby we act as JCB’s merchant acquirer in Canada and generally accept and process JCB cards in the same manner and at the same Discount Rate as American Express Cards. The definition of American Express Card or Card includes JCB cards and references to our Marks include the marks of JCB. Merchants in Canada are able to accept JCB cards on the same Merchant Number and on the same POS device on which they accept the American Express Card.

We may disclose information concerning Transactions on JCB cards to JCB and its affiliates to process those Transactions, and as appropriate to implement JCB card acceptance on the Network.

Complimentary American Express and JCB decals and signage are available for Merchants in Canada. See www.americanexpress.ca/signage for more information.

3.2 Treatment of the American Express Brand

Except as expressly permitted by Applicable Law, you must not:

- indicate or imply that you prefer, directly or indirectly, any Other Payment Products over the Card,
- try to dissuade Cardmembers from using the Card,
- criticize or mischaracterize the Card or any of American Express’ services or programs,
- try to persuade or prompt Cardmembers to use any Other Payment Products or any other method of payment (e.g., payment by cheque),
- impose any restrictions, conditions, disadvantages, or fees when the Card is accepted that are not imposed equally on all Other Payment Products, except for electronic funds transfer, cash or cheque,
- suggest or require Cardmembers to waive their right to dispute any Transaction,
- engage in activities that harm 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).

The prohibitions stated in the previous section apply unless allowable under Applicable Law or industry codes of conduct to which American Express subscribes.

Specifically, you may offer discounts from your regular posted prices to prospective buyers for other methods of payments such as cash or by electronic funds transfer, cheque, or credit and debit products issued on other payment networks, provided that you clearly and conspicuously disclose the terms of the discount offer to all prospective buyers at the point of purchase or checkout.

3.2.1 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 Card and display American Express Marks (including any Card application forms provided) 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 prior written consent from your Merchant Services Provider) indicate that American Express endorses your goods or services.

You shall only use the American Express Marks as permitted by the Agreement and shall cease using American Express’ Marks upon termination of the Agreement.

Contact your Merchant Services Provider for additional guidelines on the use of the American Express Marks. To order complimentary point-of-purchase promotional material and decals, you may also visit the American Express Signage Web Store at www.americanexpress.ca/signage.

3.3 Prohibited Uses of the Card

You must not accept the Card 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 owners (or their family members) or employees contrived for cash flow purposes, or payments that you have accepted in order to advance cash to Cardmembers in connection with the Transaction,

❖ amounts that do not represent bona fide, direct sales by your Establishment to Cardmembers 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 jewelry are not prohibited), or virtual currencies that can be exchanged for real currency (loyalty program currencies are not prohibited),

❖ Charges that the Cardmember has not specifically approved,

❖ costs or fees over the normal price of the goods or services (plus applicable taxes) that the Cardmember has not specifically approved,
This document contains sensitive, confidential and trade secret information, and must not be disclosed to third parties without the express prior written consent of Amex Bank of Canada.
4.1 Introduction
4.2 Completing a Transaction at the Point of Sale
4.3 Processing an In-Person Charge
4.4 Customer Activated Terminals
4.5 Processing a Card Not Present Charge
4.6 Charge Records
4.7 Processing a Credit
4.8 Credit Records
4.9 Return and Cancellation Policies
4.10 Processing Transactions for Specific Industries
4.11 Reserved
4.12 Advance Payment Charges
4.13 Aggregated Charges
4.14 Delayed Delivery Charges
4.15 Keyed No Imprint Program
4.16 No Signature/No PIN Program
4.17 Recurring Billing Charges
4.18 Processing Prepaid Cards
4.19 Processing Travelers/Gift Cheques
4.1 Introduction

In today’s marketplace, point of sale Transactions encompass a wide variety of customer options, including:
- in-store Transactions
- internet/e-commerce Transactions
- Application-initiated Transactions
- phone/mail order Transactions
- Customer Activated Terminal (CAT) Transactions

This section of the *Merchant Operating Guide* addresses Transaction processing and offers specific procedures and guidelines for dealing with various Transaction types. It covers Card Present, Card Not Present, the acceptance of Prepaid Cards, and more. In all situations, you should consult with your Merchant Services Provider’s instructions for Transaction processing for additional information and guidance.

4.2 Completing a Transaction at the Point of Sale

All valid Transactions begin with a Cardmember’s purchase at the point of sale. Whether the physical Card is used to facilitate a Card Present Charge, or the Cardmember provides his or her Cardmember Information over the phone, via mail order, or the internet, the Transaction must not be completed without the Card and/or information provided by the Cardmember.

To accept the Card for Charges at your Establishments, at the point of sale, you must:
- clearly and conspicuously, disclose all material terms of sale prior to obtaining an Authorization, and
- clearly and conspicuously inform Cardmembers at all points of interaction (e.g., sales conducted in person, over the internet, mobile or via mail or telephone order) what Entity is making the sales offer, so that the Cardmember can clearly distinguish you from any other party involved in the interaction (e.g., a vendor of goods or provider of services you may engage, or another Merchant seeking to conduct business with the Cardmember).

The Transaction Data you collect to facilitate the Charge must be, or have been, provided directly to you by the Cardmember.

You must not accept or have accepted Transaction Data from, nor shall you provide or have provided Transaction Data to, any third parties other than your Covered Parties. If you fail to comply with this requirement, you may be charged non-compliance fees and/or have your Card acceptance privileges at your Establishments suspended or disentitled.
4.3 Processing an In-Person Charge

In-Person Charges refer to Charges in which the Card and Cardmember are present at the point of sale. An example of this is when a Cardmember presents a Card to the Merchant at a retail store.

For all In-Person Charges, the Card must be presented. There are several ways in which an In-Person Charge can be conducted. The steps taken vary according to how the following two types of In-Person Charges are conducted:

- electronic Charges
- key-entered Charges

4.3.1 Electronic Charges

Electronic Point of Sale (POS) Systems automatically capture required information from the Card so it can be used to request Authorization for the Charge. Electronic charges can be conducted in a variety of ways depending on the type of Card presented.

- Magnetic Stripe Cards – contain Cardmember and Card account information on the stripe on the back of the Card, or in a contactless Chip embedded in the Card.
- Chip Cards – contain a Chip on which data is stored (including Cardmember and Card account information), which the POS System can read in order to guide the processing of the Transaction.
- Mobile Devices – An Issuer approved and American Express recognized electronic device (including but not limited to, a mobile telephone, tablet, or wearable device) that is enabled to initiate a Digital Wallet Payment Transaction.

Some Magnetic Stripe, Chip Cards, and Mobile Devices may be read over the contactless interface of the POS System. The Charge Record is then created from the information captured during the electronic Charge.

You must work with your Merchant Services Provider if you have questions related to your POS capabilities.

4.3.1.1 Magnetic Stripe Card Charges

When presented with a Card at the point of sale, you must:

1. Verify that the Card is not visibly altered or mutilated,
2. Verify that the customer is the Cardmember* (Cards are not transferable),
3. Capture Magnetic Stripe data by swiping the Card (unless the Charge was already initiated by waving the contactless Chip Card in close proximity to the POS System) as described in Subsection 4.3.1.3, “Contactless Chip Card Charge” and Subsection 4.3.1.2, “Contact Chip Card Charges”,
4. Obtain an Authorization Approval,
5. Obtain signature (excluding Charges at CATs) and verify that the signature is identical to the name on the Card.* Obtaining a signature may not be required if your Establishment and the Charge qualify for the No Signature/No PIN Program (see Section 4.16, “No Signature/No PIN Program” for additional information),
6. Compare the signature (when obtained) on the Charge Record with the signature on the Card,

7. Verify the Card's Expiration Date,

8. Match the Card Number and the Expiration Date on the Card to the same information on the Charge Record, and

9. Ensure the name that prints on the Charge Record matches the name on the front of the Card.*

* Except when the Cardmember name is not captured on the Charge Record or for Prepaid Cards that do not show a name on their face. If you encounter an In-Person Transaction that raises concern, refer to Subsection 4.3.3, "Actions for In-Person Charges" and proceed accordingly.

4.3.1.2 Contact Chip Card Charges

When presented with a Chip Card to be inserted into a Chip Card reader, you must:

1. Verify that the Card is not visibly altered or mutilated (see Chapter 9, "Fraud Prevention" for additional information),

2. Verify that the customer is the Cardmember* (Cards are not transferable),

3. Capture Chip Card Data by inserting the Card into the Chip Card reader,

The POS System will advise Cardmembers to enter their PIN (a Chip and PIN Charge) or sign for the Charge (a Chip and signature Charge):

- Chip and PIN Charges: Cardmembers will enter their PIN into the POS System using the keypad. If the Chip and PIN Charge is unable to be completed due to a technical problem, the POS System will show an error message. Follow the procedures for a swiped Charge in Subsection 4.3.1.1, "Magnetic Stripe Card Charges". Failure to validate the PIN, when required, can render you liable for Chargebacks if the Cardmember disputes the Charge. Validating a PIN may not be required if your Establishment and the Charge qualify for the No Signature/No PIN Program (see Section 4.16, "No Signature/No PIN Program" for additional information).

- Chip and signature Charge: Obtain the Cardmember’s signature on the Charge Record and compare the signature on the Charge Record to the name and signature on the Card. Obtaining a signature may not be required if your Establishment and the Charge qualify for the No Signature/No PIN Program (see Section 4.16, "No Signature/No PIN Program" for additional information).

4. If your POS Systems have not been upgraded to accept and process Chip and PIN Cards, and a Chip Card is presented, American Express may exercise Chargeback for counterfeit, lost, stolen, or non-received fraud. Contact your Merchant Services Provider for additional information regarding your POS System’s capabilities.
If your POS Systems have been so upgraded and a Chip Card is presented:

- American Express may exercise Chargeback for lost, stolen, and non-received fraud if a Chip and PIN Card is presented and the Charge is facilitated as a Chip and Signature Charge.
- American Express will not exercise Chargeback for counterfeit, lost, stolen, or non-received fraud if, due to a technical problem with the terminal, you are unable to complete the Charge as a Chip Card Charge.

If a Cardmember presents a Chip Card and the Transaction is manually keyed, the Transaction may be subject to counterfeit, lost/stolen and non-received fraud Chargebacks in the event of a dispute. Refer to your Merchant Services Provider’s information on Disputes and Chargebacks for further information.

### 4.3.1.3 Contactless Chip Card Charge

Some Chip Card Charges involve transmission of payment information when the Card is waved in close proximity to a contactless reader. Merchants that choose to accept Contactless payments must comply with the current American Express contactless POS System requirements. Work with your Merchant Services Provider if you have questions related to Contactless Chip Card acceptance.

When presented with a Card to be read via a contactless reader, you must:

1. Capture Magnetic Stripe or Chip Card Data using the contactless reader, and

For contactless Charges that are $100 or less, a signature is not required. [Section 4.16, "No Signature/No PIN Program"] does not apply to these Charges. For contactless Charges that are $100 or less, your Merchant Services Provider will not exercise a counterfeit, lost, stolen, or non-received fraud Chargeback provided that Magnetic Strip or Chip Card Data was captured and an authorization approval was obtained.

For Charges above $100, or if any of the following exclusions apply, follow the relevant Card acceptance procedures outlined in either [Subsection 4.3.1.1, "Magnetic Stripe Card Charges"], [Subsection 4.3.1.2, "Contact Chip Card Charges"], or [Subsection 4.3.1.4, "Digital Wallet Payments"].

Exclusions:

- Prohibited Merchants or prohibited Transactions (or both) as defined in [Chapter 10, "Risk Management"]. See [Section 3.3, "Prohibited Uses of the Card"].
- High Risk Merchants as defined in [Section 10.3.1, "High Risk Merchants"].
- Merchants placed in American Express' Fraud Full Recourse Program.
4.3.1.4 Digital Wallet Payments

Digital wallets within a Mobile Device facilitate Transactions as follows:

- For a Digital Wallet Contactless-initiated Transaction, the Mobile Device completes a Card Present Charge by waving the device in close proximity to a contactless-enabled POS System.
- For a Digital Wallet Magnetic Secure Transmission Transaction, the Mobile Device completes a Card Present Charge by waving the device in close proximity to the magnetic swipe-enabled POS System.
- For a Digital Wallet Application-initiated Transaction, the Mobile Device completes a Card Not Present Charge (typically made online) using a software application within the Mobile Device and not the contactless payment application.

When presented with a Mobile Device for a Card Present Charge, you should:

1. Capture Magnetic Stripe or Chip Card data by having the Cardmember wave the Mobile Device in close proximity to the contactless reader or magnetic swipe-enabled POS System.

   **Note:** If you choose to accept contactless payments, you should consult with your Merchant Services Provider to ensure compliance with the current American Express contactless POS System requirements.


3. Obtain a signature or have the Cardmember complete a Consumer Device Cardholder Verification Method (CDCVM) on contactless initiated Transactions. For Magnetic Secure Transmission Transactions, you must continue to obtain a signature (excluding Charges at CATs and Charges that qualify for the No Signature/No PIN Program – see Section 4.16, "No Signature/No PIN Program" for additional information).

4. Continue to include an indicator in the Authorization that the Transaction is a contactless Transaction, if applicable.

5. If a Mobile Device initiated Transaction cannot be processed for any reason, you should request that the Cardmember provide the companion physical Card and complete the Transaction by following the relevant Card acceptance procedures outlined in:

   - Subsection 4.3.1.1, "Magnetic Stripe Card Charges", or
   - Subsection 4.3.1.2, "Contact Chip Card Charges".

For Application-initiated Transactions, you should follow Card Not Present Charge policy as described in Section 4.5, "Processing a Card Not Present Charge".

For a Transaction to be recognized as Digital Wallet Application-initiated Transaction, you should:

1. Consult with your Merchant Services Provider to arrange for certification for Digital Wallet Application-initiated Transactions.
2. Include appropriate indicators in the Authorization and Submission that the Transaction is a Digital Wallet Application-initiated Transaction (see Section 2.1, "Compliance with the Technical Specifications").

Mobile Devices do not have the same security features as a traditional plastic Card. For instance, the screens on the Mobile Device may not display all the digits of the Card Number and expiration date, or the Cardmember name. Likewise, there may not be a CID visible on the handset screen.
4.3.2 Key-Entered Charges

There are instances when you may need to key-enter an In-Person Charge. This occurs most often when the POS System cannot read the Card.

If the Card cannot be read electronically, and you wish to key-enter the Transaction, then you must:

1. Verify that the Card is not visibly altered or mutilated,
2. Verify that the customer is the Cardmember* (Cards are not transferable),
3. Key-enter the data,
4. Obtain an Authorization Approval,
5. Obtain a signature and verify that the signature is identical to the name on the Card.* Obtaining a signature may not be required if your Establishment and the Charge qualify for the No Signature/No PIN Program (see Section 4.16, "No Signature/No PIN Program" for additional information),
6. Compare the signature (when obtained) on the Charge Record with the signature on the Card,
7. Verify the Card’s Expiration Date,
8. Match the Card Number and the Expiration Date on the Card to the same information on the Charge Record, and
9. Validate the Card’s presence by taking an imprint of the Card (the imprint is for your records). Failure to validate the Card’s presence by taking an imprint of the Card can render you liable for Chargebacks if the Cardmember disputes the Charge.

* Except when the Cardmember name is not captured on the Charge Record or for Prepaid Cards that do not show a name on their face.

When keying Charges, ensure:
- the Card Number is keyed correctly, and
- the Expiration Date is entered in a YY/MM format.

You may also validate the Card’s presence by ensuring the Charge meets the criteria of the Keyed No Imprint Program (See Section 4.15, "Keyed No Imprint Program"). Key-entered Charges are subject to a fee.

You may still be subject to other fraud Chargebacks, including counterfeit, lost, stolen, and non-received for manually key-entered Transactions. Key-entered Charges that occur when a Chip Card is presented are subject to Chargeback for counterfeit, lost, stolen, and non-received fraud.

Contact your Merchant Services Provider for additional guidance or to obtain information on fees assessed on Key-entered Charges.

In-Person Charges that must be key-entered because the Magnetic Stripe cannot be read are more likely to be fraudulent. See Chapter 9, "Fraud Prevention" to learn how to inspect the Card and for procedures to follow when you suspect fraud. Transactions that are manually key-entered when a Chip Card is presented may be subject to counterfeit, lost/stolen and non-received Chargebacks in the event of a fraud dispute. To minimize your risk of Chargebacks, avoid manually key-entered Transactions whenever possible.
4.3.3 Actions for In-Person Charges

The following table describes the course of action required during an In-Person Transaction cycle:

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Card is obviously altered or counterfeit.</td>
<td>Do not accept the Card.</td>
</tr>
<tr>
<td>The Cardmember is attempting to use the Card outside of its Valid Dates.</td>
<td>Do not accept the Card. Advise the Cardmember to contact the customer service number on the back of the Card.</td>
</tr>
<tr>
<td><strong>Note:</strong> Cards are valid through the last day of the month on the front of the Card.</td>
<td><strong>Note:</strong> Cards are valid through the last day of the month on the front of the Card.</td>
</tr>
<tr>
<td>It appears that someone other than the Cardmember is attempting to use the Card.</td>
<td>Do not accept the Card. Indicate that the Cards are non-transferable and that only the Cardmember is permitted to use the Card.</td>
</tr>
<tr>
<td>The signature does not match the name on the Card.</td>
<td>Contact your Merchant Services Provider with a Code 10.</td>
</tr>
<tr>
<td>You are unable to obtain Authorization electronically.</td>
<td>Contact your Merchant Services Provider to obtain an Authorization.</td>
</tr>
<tr>
<td>The Authorization is Declined.</td>
<td>Do not accept the Card and follow your internal policies for handling various Authorization responses. See Section 5.4, <em>Possible Authorization Responses</em>.</td>
</tr>
<tr>
<td>The customer presents an unsigned Card.</td>
<td>An unsigned Card is invalid. Show customer that the Card is not signed. Ask the customer to sign the Card and also request photo identification (ID) such as a valid driver’s license or passport to compare the signatures.</td>
</tr>
<tr>
<td>The customer’s signature on the Charge Record does not appear to match the customer’s signature on the Card.</td>
<td>Contact your Merchant Services Provider with a Code 10, or if you prefer, simply decline to accept the Card.</td>
</tr>
<tr>
<td>The Card Numbers and Valid Dates on the Card do not match the Charge Record.</td>
<td>Contact your Merchant Services Provider with a Code 10, or if you prefer, simply decline to accept the Card.</td>
</tr>
<tr>
<td>The name on the Charge Record does not match the name on the Card (except in the case of a Prepaid Card which may not show a name on its face).</td>
<td>Contact your Merchant Services Provider with a Code 10, or if you prefer, simply decline to accept the Card.</td>
</tr>
<tr>
<td>The appearance of the Card, or the actions of the customer appear suspicious.</td>
<td>Contact your Merchant Services Provider with a Code 10, or if you prefer, simply decline to accept the Card.</td>
</tr>
</tbody>
</table>
4.4 Customer Activated Terminals

Charges for purchases at Customer Activated Terminals (CATs) must meet the requirements for Charge Records as detailed in Section 4.6, "Charge Records" as well as comply with the Technical Specifications.

You must include:
- Full Magnetic Stripe data stream or Chip Card Data in all Authorization requests, and
- a CAT indicator on all Authorization requests and Submissions.

American Express will not be liable for actual or alleged fraudulent Transactions occurring through CATs and American Express will have the right to Chargeback for those Charges. Contact your Merchant Services Provider for additional information on CAT Transactions.

4.5 Processing a Card Not Present Charge

Mail orders, telephone orders, and Internet Orders increase your business opportunities, but such Card Not Present Charges do not provide you the opportunity to inspect the physical Card. For these Card Not Present Charges, fraud might be difficult for you to detect.

You must:
- obtain information about the Cardmember as described below;
- obtain an authorization Approval; and
- submit the Charge to your Merchant Services Provider.

For Card Not Present Charges, you must create a Charge Record as described in Section 4.6, "Charge Records". The information you must obtain in order to proceed with the Transaction includes:
- Card Number or Token, and
- Card or Token Expiration Date.

In addition, it is recommended that you ask for:
- name as it appears on the Card,
- Cardmember's billing address, and
- ship-to address, if different from the billing address.
American Express has the right to Chargeback for any Card Not Present Charge that the Cardmember denies making or authorizing. American Express will not Chargeback for such Charges based solely upon a Cardmember claim that he or she did not receive the disputed goods if you have:

- verified the address to which the goods were shipped was the Cardmember’s full billing address, and
- provided Proof of Delivery signed by the Cardmember or an authorized signer of the Card indicating the delivery of the goods or services to the Cardmember’s full billing address.

American Express will not be liable for actual or alleged fraudulent Transactions over the internet and American Express will have the right to Chargeback for those Charges.

For Internet Orders, you must:

- use any separate Merchant Numbers established by your Merchant Services Provider for Internet Orders in all your requests for Authorization and Submission of Charges, and
- provide your Merchant Services Provider written notice of any change in your internet address, in accordance with your Merchant Services Provider’s instructions.

Additionally, if a Disputed Charge arises involving a Card Not Present Charge that is an Internet Electronic Delivery Charge, American Express may exercise Chargeback for the full amount of the Charge.

When providing Proof of Delivery, a signature from the Cardmember or an authorized signer of the Card is not required.

Contact your Merchant Services Provider for additional information and guidance on processing Card Not Present Charges.

4.6 Charge Records

You must create a Charge Record for every Charge. For each Charge submitted electronically, you must create an electronically reproducible Charge Record, and the Charge must comply with the Technical Specifications. See Section 2.1, “Compliance with the Technical Specifications”.

The Charge Record (and a copy of the customer’s receipt) must disclose your return and/or cancellation policies. See Section 4.9, “Return and Cancellation Policies” for additional information.

If the Cardmember wants to use different Cards for payment of a purchase, you may create a separate Charge Record for each Card used. However, if the Cardmember is using a single Card for payment of a purchase, you must not divide the purchase into more than one Charge, nor create more than one Charge Record.

For all Charge Records, you must:

1. Submit the Charge to your Merchant Services Provider for payment.
2. Retain the original Charge Record (as applicable) and all documents evidencing the Charge, or reproducible records thereof, for twenty-four (24) months. See Chapter 8, “Protecting Cardmember Information” for additional information.
3. Provide a copy of the Charge Record to the Cardmember.

Ensure that your Proof of Delivery includes a courier receipt with the following information at minimum:

- date merchandise was delivered,
- full name of recipient, and
- full shipping address (e.g., suite or apartment number, city, state/province, zip/postal code, country).

If you ship goods to an alternate address, we recommend that you keep a record of this. Then you can show a record of previous undisputed Transactions which were shipped to this address.
You may be able to create more than one Charge Record if the purchase qualifies for a Delayed Delivery Charge. See Section 4.14, “Delayed Delivery Charges”.

Pursuant to Applicable Law, truncate the Card Number and do not print the Card’s Expiration Date on the copies of Charge Records delivered to Cardmembers. Truncated Card Number digits must be masked with replacement characters such as “x,” “*,” or “#,” and not blank spaces or numbers. Here is an example of a Charge Record with a truncated Card Number.

### 4.7 Processing a Credit

A Credit may occur when a Merchant processes a refund for purchases or payments made on the Card.

Follow these steps to issue a Credit:

1. Create a Credit Record.
2. Compare the last four digits on the Charge Record against the Card presented (when applicable).
3. Have the Cardmember sign the Credit Record (when applicable).
4. Provide a copy of the Credit Record to the Cardmember.

You must submit Credits to your Merchant Services Provider within seven (7) days of determining that a Credit is due and create a Credit Record that complies with your Merchant Services Provider’s requirements (see Section 4.8, “Credit Records” for additional information). You must not issue a Credit when there is no corresponding Charge, nor issue a Credit in exchange for cash or other consideration from a Cardmember.

You must submit all Credits under the Establishment where the Credit originated.

A Credit must be issued in the currency in which the original Charge was submitted to your Merchant Services Provider. You must issue Credits to the Card used to make the original purchase; however, if the Credit is for the return of a gift by someone other than the Cardmember who made the original purchase, apply your usual refund policy.

If the Cardmember indicates that the Card on which the purchase was originally made is no longer active or available, do the following:

- For all Cards except Prepaid Cards, advise the Cardmember that you must issue the Credit to that Card. If the Cardmember has questions, advise him or her to call the customer service number on the back of the Card in question.
- If the inactive or unavailable Card is a Prepaid Card, apply your usual refund policy for returns.
4.8 Credit Records

You must create a Credit Record for any Credit that you issue. For each Credit submitted electronically, you must create an electronically reproducible Credit Record, and the Credit must comply with the *Technical Specifications*. See Section 2.1, "Compliance with the Technical Specifications".

If you submit Credits on paper, you must create a Credit Record containing all of the following required data:

- full Card Number and Expiration Date (pursuant to Applicable Law), and if available, Cardmember name,
- the date the Credit was issued,
- the amount of the Credit, and
- your Establishment name and address and, if applicable, store number.

For all Credit Records, you must:

1. Submit the Credit through your Merchant Services Provider.
2. Retain the original Credit Records (as applicable) and all documents evidencing the Transaction, or reproducible records thereof, for twenty-four (24) months from the date you submitted the corresponding Credit.
3. Provide a copy of the Credit Record to the Cardmember.

The retention time frame for Credit Records is twenty-four (24) months from the date you submitted the corresponding Credit to your Merchant Services Provider.

Pursuant to Applicable Law, you must truncate the Card Number and must not print the Card’s Expiration Date on copies of Credit Records delivered to the Cardmember.

Contact your Merchant Services Provider for additional information and guidance on submission of Credit Records.
4.9 Return and Cancellation Policies

Your return and cancellation policies must be fair and clearly disclosed at the time of sale in compliance with Applicable Law. Your policies must be conveyed to the Cardmember prior to completion of the Charge and printed on a copy of a receipt, Charge Record, or otherwise provided to a Cardmember in writing.

You must not give cash refunds to Cardmembers for goods or services they purchase on the Card, unless required by Applicable Law. Your refund policy for purchases on the Card must be at least as favourable as your refund policy for purchases made with Other Payment Products or other payment methods.

**Return Policy recommendations:**

- Provide clear return instructions for your customers, including the following information:
  - customer service telephone number,
  - reference number for the return,
  - expected processing time for the Credit, and
  - return address, preferably on a pre-formatted shipping label (if applicable).

**Cancellation Policy recommendations:**

- Document cancellation policy and terms and conditions on the contract the Cardmember signs, or on your website, as applicable. Provide Cardmember with a cancellation number that can be tracked in your records.

4.9.1 Return Policy for Prepaid Products

This section applies to Merchants who accept the Card for the purchase of any prepaid product (Prepaid Cards, non-American Express branded stored value or gift cards, or both). If your return policy for the purchase of prepaid products is different from your standard return policy, notwithstanding the requirements listed in Section 4.9, "Return and Cancellation Policies", you must ensure that such prepaid product-specific return policy is clearly disclosed to the Cardmember at the time of purchase and also coded to print on all receipts and copies of Charge Records.

4.10 Processing Transactions for Specific Industries

Most policies and procedures in the Merchant Operating Guide are applicable to all Merchants, regardless of industry. Some Merchants classified in specific industries, however, are subject to additional policies and procedures. These policies and procedures are contained in Chapter 12, "Specific Industries".
4.12 Advance Payment Charges

You must follow these procedures if you offer Cardmembers the option or require them to make Advance Payment Charges for the following types of goods and/or services:

- 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
- Travel-related services (e.g., tours, guided expeditions)

For an Advance Payment Charge, you must:

- State your full cancellation and refund policies, clearly disclose your intent and obtain written consent from the Cardmember to bill the Card for an Advance Payment Charge before you request an Authorization. The Cardmember’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.
- Obtain an Authorization Approval.
- Complete a Charge Record. If the Advance Payment Charge is a Card Not Present Charge, you must also:
  - ensure that the Charge Record contains the words “Advance Payment” (see Section 4.6, “Charge Records”), and
  - within twenty-four (24) hours of the Charge being incurred, provide the Cardmember 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 and details of your cancellation/refund policy.

If goods and/or services cannot be delivered (e.g., because custom-ordered merchandise cannot be fulfilled), and if alternate arrangements cannot be made, you must immediately issue a Credit for the full amount of the Advance Payment Charge which cannot be fulfilled.

In addition to other Chargeback rights, American Express may exercise Chargeback for any Disputed Advance Payment Charge or portion thereof if, in American Express’ sole discretion, the dispute cannot be resolved in your favour based upon unambiguous terms contained in the terms of sale to which you obtained the Cardmember’s written consent.
4.13 Aggregated Charges

If you are classified in an internet industry, you may process Aggregated Charges provided the following criteria are met:

- Clearly disclose your intent and obtain written consent from the Cardmember that their purchases or refunds (or both) on the Card may be aggregated and combined with other purchases or refunds (or both) before you request an Authorization.
- Each individual purchase or refund (or both) that comprises the Aggregated Charge must be incurred under the same Merchant Number and on the same Card.
- Obtain a pre-Authorization of no more than $15. See Section 5.9, "Authorization Time Limit" for additional information.
- Create a Charge Record for the full amount of the Aggregated Charge. For more information on Charge Records, see Section 4.6, "Charge Records".
- The amount of the Aggregated Charge must not exceed $15 or the amount for which you obtained pre-Authorization.
- Submit each Charge Record in accordance with Section 6.4, "Submission Requirements – Electronic". For the purposes of Section 6.4, "Submission Requirements – Electronic", a Charge will be deemed "incurred" on the date of the first purchase or refund (or both) that comprises the Aggregated Charge.
- Provide the Cardmember with an email containing:
  - the date, amount, and description of each individual purchase or refund (or both) that comprises the Aggregated Charge, and
  - the date and the amount of the Aggregated Charge.

To minimize your risk of a Disputed Charge with Aggregated Charges, always:

- confirm to the Cardmember the Aggregated Charge amount and individual purchase details (and/or refund as applicable) at check-out, and
- in the email confirmation, advise where the Cardmember can find additional information about their purchases (and/or refunds as applicable).

4.14 Delayed Delivery Charges

To accept the Card for Delayed Delivery Charges, you must:

- Clearly disclose your intent and obtain written consent from the Cardmember to perform a Delayed Delivery Charge before you request an Authorization,
- Obtain a separate Authorization Approval for each of the two Delayed Delivery Charges on their respective Charge dates,
- Clearly indicate on each Delayed Delivery Charge Record that the Charge is either for the deposit or for the balance of the Delayed Delivery Charge,
- Submit the Delayed Delivery Charge Record for the balance of the purchase only after the goods have been shipped, provided or services rendered.
Submit each Delayed Delivery Charge Record in accordance with Section 6.4, “Submission Requirements – Electronic”. For the purposes of Section 6.4, “Submission Requirements – Electronic”, the Charge will be deemed “incurred”:
- for the deposit – on the date the Cardmember agreed to pay the deposit for the purchase.
- for the balance – on the date the goods are shipped, provided or services are rendered.

Submit and Authorize each Delayed Delivery Charge under the same Merchant Number, and

Treat deposits on the Card no differently than you would treat deposits on all Other Payment Products.

4.15 Keyed No Imprint Program

All Cards qualify for the Keyed No Imprint Program. The Keyed No Imprint Program allows you to submit In-Person Charges without taking an imprint of the Card if you meet the following Charge criteria:
- the Charge must be key-entered,
- the Charge submission must include the appropriate indicator to reflect that the Card and the Cardmember were present at the point of sale,
- the Charge submission must include a valid Approval, and
- the Card Identification (CID) Number must be confirmed as a positive match.

Under the Keyed No Imprint Program, American Express will not exercise Chargeback for such Charges based solely on the Establishment’s failure to obtain an imprint of the Card.

If American Express receives disproportionate amounts or numbers of Disputed Charges under the Keyed No Imprint Program, you must work with your Merchant Services Provider to reduce the number of Disputed Charges. If such efforts fail, American Express may place you in a Chargeback program, revoke participation in the Keyed No Imprint Program, or require cancellation or disentitlement of Card acceptance.

To minimize your risk of a Disputed Charge with Delayed Delivery Charges, always:
- clearly disclose all sales and refund policies (see Section 4.9, “Return and Cancellation Policies”), and
- retain a copy of the Cardmember’s written consent in a format that easily allows you to respond to an Inquiry.

To learn more about how to send the CID Number through your POS System, contact your Merchant Services Provider.
4.16 No Signature/No PIN Program

You may participate in American Express’ No Signature/No PIN Program. The No Signature/No PIN Program allows Merchants not to request a signature or a PIN from Cardmembers on the Charge Record.

To qualify for the No Signature/No PIN Program, both the Establishment and each Charge must meet the following criteria:

**Merchant criteria:**

If you are classified in an industry that accepts In-Person Charges, then you may participate in the No Signature/No PIN Program 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 Chapter 10, "Risk Management". See also Section 3.3, "Prohibited Uses of the Card".
- High Risk Merchants (e.g., internet electronic services or nightclubs/lounges) as defined in Section 10.3.1, "High Risk Merchants".
- Merchants placed in American Express’ Fraud Full Recourse Program.

**Charge criteria:**

- The amount or Charge must meet the established threshold.
- The Charge submission must include the appropriate indicator to reflect that the Card and the Cardmember were present at the point of sale.
- The Charge submission must include a valid Approval.

Under the No Signature/No PIN Program, American Express will not exercise Chargeback for such Charges based solely on your Establishment’s failure to obtain the Cardmember’s signature or PIN at the point of sale.

If disproportionate amounts or number of Disputed Charges are received under the No Signature/No PIN Program, you must work to reduce the amount or number of Disputed Charges. If such efforts fail, American Express may place you in a Chargeback program and your Merchant Services Provider and/or American Express may modify participation in the No Signature/No PIN Program or revoke or terminate your participation in the No Signature/No PIN Program.

The established threshold for charges to qualify under the No Signature/No PIN Program is $50.00 or less.
4.17 Recurring Billing Charges

Recurring Billing is an option offered to Cardmembers to make recurring Charges automatically on their Card. The Recurring Billing Charges are for a product or service the Cardmember agrees to pay periodically and automatically (e.g., membership fees to health clubs, magazine subscriptions, and insurance premiums).

If you offer Cardmembers the option to make Recurring Billing Charges, you must:

- obtain the Cardmember’s express consent for you to bill the Card before submitting the first Recurring Billing Charge, and
- notify the Cardmember that he or she can cancel such consent at any time and provide contact details for cancelling recurring billing.

In addition to other Chargeback rights, American Express may exercise Chargeback for any Charge which does not meet the requirements listed in this section. American Express may also exercise Chargeback, prior to sending you an Inquiry, if you process Recurring Billing Charges after having previously been notified that the Cardmember has cancelled their consent for Recurring Billing Charges.

The method you use to secure such consent must contain a disclosure that you may receive updated Card account information from the Issuer.

Before submitting a Recurring Billing Charge, you must obtain Authorization and complete a Charge Record (see Section 4.6, "Charge Records"), except with the words “signature on file,” if applicable, on the signature line and the appropriate electronic descriptor on the Charge Record. For complete Authorization requirements, see Chapter 5, "Authorizations".

If the Agreement terminates for any reason, then you must notify all Cardmembers for whom you have submitted Recurring Billing Charges that you no longer accept the Card.

You must fulfill Cardmembers’ requests that you discontinue the Recurring Billing Charges immediately and provide cancellation numbers to Cardmembers as proof of the cancellation.

The cancellation of a Card constitutes immediate cancellation of that Cardmember’s consent for Recurring Billing Charges. You will not be notified of such cancellation, nor will your Merchant Services Provider or American Express have any liability to you arising from such cancellation.

If a Card is cancelled, or if a Cardmember cancel consent to Recurring Billing Charges, you are responsible for arranging another form of payment (as applicable) with the Cardmember.

You must retain evidence of consent to receive updated Card account information from the Issuer for twenty-four (24) months from the date you submit the last Recurring Billing Charge.

If you offer Cardmembers the option to make Recurring Billing Charges, you must:

- ensure that your process for cancellation of Recurring Billing is simple and expeditious,
- clearly and conspicuously disclose all material terms of the option, including, if applicable, an initial notice of recurring billing, and the fact that Recurring Billing will continue until the option is cancelled by the Cardmember,
- within twenty-four (24) hours of incurring the first Recurring Billing Charge, provide the Cardmember written confirmation (e.g., email or facsimile) of such Charge, including all material terms of the option and details of your cancellation/refund policy, and

To minimize your risk of Chargeback with Recurring Billing Charges, always:

- ensure updates are applied in a timely manner when notified of Cardmember cancellation or Card Number update, and
- obtain express consent from the Cardmember to continue billing after the end date of the contract.
where the material terms of the option change after submission of the first Recurring Billing Charge, promptly notify the Cardmember in writing of such change and obtain the Cardmember’s express written consent to the new terms prior to submitting another Recurring Billing Charge.

4.18 Processing Prepaid Cards

Prepaid Cards are available for a variety of uses: gifting, travel, incentive, etc. All American Express Prepaid Cards show the American Express “Blue Box” logo either on the face or back of the Prepaid Card. Prepaid Cards may or may not be embossed. Most Prepaid Cards can be used for both in-store and online purchases.

Prepaid Cards are valid through the date on the Card. Swipe or insert the Card at the point of sale just like any other Card. A Prepaid Card must be tendered for an amount that is no greater than the funds available on the Card.

Instruct Cardmembers that, before making a purchase, they may check their remaining funds by:

- calling the twenty-four (24) hour, toll-free number on the back of the Card,
- checking online, or
- using the mobile app offered by their Issuer (where available).

Because Prepaid Cards are pre-funded, if you receive a Decline when seeking Authorization, ask the customer to go online, use their mobile app, or 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. See Section 5.12, “Additional Authorization Requirements”.

You must create a Charge Record for a Prepaid Card as you would any other Card. For information about processing Prepaid Cards, call the customer service number on the back of the Card in question.
4.19 Processing Travelers/Gift Cheques

American Express Travelers Cheques, Cheques for Two, and Gift Cheques are easy to accept provided that the cheque is an authentic American Express Travelers Cheque. See Subsection 4.19.1, "Acceptance Procedures".

Businesses can accept these cheques for payment. You can deposit Travelers Cheques, Cheques for Two and Gift Cheques directly into your Bank Account as they never expire.

Travelers Cheques

American Express Travelers Cheques are a widely used and recognized travel currency. If they are ever lost or stolen, they can be replaced quickly and easily, almost anywhere in the world, usually within twenty-four (24) hours.

Travelers Cheques come in various denominations and currencies. Travelers Cheques come in denominations ranging from $20 to $1000. Be cautious when presented with an American Express Travelers Cheque in a denomination of $500 or greater. These higher-denominated Travelers Cheques are rarely sold, and therefore are more likely to be counterfeit. For information on how to perform a "smudge test," which is designed to test the authenticity of the Travelers Cheque, see Section 9.8, "Travelers Cheque and Gift Cheque Security Features".

Gift Cheques

American Express Gift Cheques function like Travelers Cheques, and are available in $10, $25, $50, and $100 denominations only. Any Gift Cheque presented that is greater than $100 is counterfeit. If you receive a Gift Cheque greater than $100, do the following:

- Contact Travelers Cheque/Gift Cheque Customer Service at 1-866-296-5198.
- Do not accept it.
- Write the word "VOID" across the front of the counterfeit Cheque.

For further information, see Chapter 9, "Fraud Prevention".

4.19.1 Acceptance Procedures

Accepting American Express Travelers and Gift Cheques is easy:

- Watch your customer countersign in the lower left corner of the cheque, and compare the countersignature to the signature in the upper left corner for American Express Travelers Cheques and Gift Cheques. For Cheques for Two, the customer’s countersignature must match either one of the two signatures on top.

- Validate Security Features – Validating these features will help reduce the acceptance of counterfeit cheques. See Section 9.8, "Travelers Cheque and Gift Cheque Security Features".
 Obtain authorization – American Express recommends obtaining an authorization to reduce the chances of accepting fraudulent cheques. American Express offers a variety of authorization tools. See authorization methods in the following table to determine your course of action:

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>The signature and countersignature are a reasonable match (they look alike, but may not be identical)</td>
<td>Accept the cheque. There is no need to obtain any identification.</td>
</tr>
<tr>
<td>You suspect that the countersignature may be false, or you did not watch the customer countersign</td>
<td>Ask the customer to turn the cheque over and sign again across the left-hand side (in the same manner one typically endorses a cheque). Then take the cheque and fold up the bottom right-hand corner so that you can compare the original signature with the new one.</td>
</tr>
<tr>
<td>The signatures are not the same, or if there is a question regarding the validity of the cheque</td>
<td>Call the Travelers Cheque/Gift Cheque Customer Service at 1-866-296-5198.</td>
</tr>
<tr>
<td>You suspect that the Travelers cheque being presented is fraudulent</td>
<td>Use any of the following methods to verify that the cheque you are accepting is authentic:</td>
</tr>
<tr>
<td></td>
<td>☑ Perform a smudge test (see Chapter 9, &quot;Fraud Prevention&quot; for details).</td>
</tr>
</tbody>
</table>
Contents

5.1 Introduction
5.2 Transaction Cycle
5.3 The Purpose of Authorization
5.4 Possible Authorization Responses
5.5 Obtaining an Electronic Authorization
5.6 Obtaining a Voice Authorization
5.7 Card Identification (CID) Number
5.8 Authorization Reversal
5.9 Authorization Time Limit
5.10 Floor Limit
5.11 Pre-Authorization
5.12 Additional Authorization Requirements
5.1 Introduction

The payment card industry devotes significant amounts of time and resources to developing Authorization systems and decision models in an effort to mitigate the financial losses. Every Transaction begins and ends with the Cardmember. Between the time the Cardmember presents the Card for payment and receives the goods or services, however, a great deal of data is exchanged, analysed, and processed. A process that literally takes seconds at the point of sale is actually a highly complex approach to analysing each Transaction.

5.2 Transaction Cycle

The Authorization process begins when you provide an Authorization request to your Merchant Services Provider. After requesting Authorization, you receive an Authorization response, which you use, in part, to determine whether to proceed with the Charge.

5.3 The Purpose of Authorization

The purpose of an Authorization is to provide you with information that will help you determine whether or not to proceed with a Charge.

For every Charge, you are required to obtain an Authorization Approval for the full amount of the Charge except for Merchants that are classified in the restaurant, lodging, and vehicle rental industries (see Chapter 12, "Specific Industries").

An Authorization Approval does not guarantee that (i) the person making the Charge is the Cardmember, (ii) the Charge is in fact valid or bona fide, (iii) you will be paid for the Charge, or (iv) you will not be subject to a Chargeback.

5.4 Possible Authorization Responses

Responses to your requests for Authorization are generated by Issuers and transmitted to you. The following are among the most commonly generated responses to your request for Authorization. The exact wording may vary so check with your Merchant Services Provider to determine what Authorization responses will display on your equipment.

<table>
<thead>
<tr>
<th>Authorization Response</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>The Charge is approved.</td>
</tr>
<tr>
<td>Partially Approved</td>
<td>The Charge is approved. The Approval is for an amount less than the value originally requested. The Charge must only be submitted for the approved amount. Collect the remaining funds due from the Cardmember via another form of payment. See Section 5.12, &quot;Additional Authorization Requirements&quot; for more information about split tender.</td>
</tr>
<tr>
<td>Declined or Card Not Accepted</td>
<td>The Charge is not approved. Do not submit the Charge. If you nevertheless choose to submit the Charge, you will be subject to a Chargeback. Inform the Cardmember promptly that the Card has been Declined. If the Cardmember has questions or concerns, advise the Cardmember to call the customer service telephone number on the back of the Card. Never discuss the reason for the Decline.</td>
</tr>
</tbody>
</table>

Electronic Authorizations should be used whenever possible as Voice Authorizations (e.g. referrals such as a "please call" message) pose a higher risk of fraud.
### 5.5 Obtaining an Electronic Authorization

Generally, Establishments must obtain an electronic Authorization. You must ensure that all Authorization requests comply with the *Technical Specifications* (see Section 2.1, "Compliance with the Technical Specifications"). If the Authorization request does not comply with the *Technical Specifications*, the submission may be rejected or you may be subject to a Chargeback. Contact your Merchant Services Provider for information about your obligations to comply with the *Technical Specifications*.

If the Card is unreadable and you have to key-enter the Charge to obtain an Authorization, then you must follow the requirements for key-entered Charges. See Subsection 4.3.2, "Key-Entered Charges" for additional information.

If you use an electronic POS System to obtain Authorization, the Approval must be printed automatically on the Charge Record.

Occasionally, obtaining an electronic Authorization may not be possible (e.g., due to POS System problems, System Outages, or other disruptions of an electronic Charge). In these instances, you must obtain a Voice Authorization (see Section 5.6, "Obtaining a Voice Authorization").

### 5.6 Obtaining a Voice Authorization

When Authorization is required, if your electronic POS System is unable to reach American Express’ Authorization system, or you do not have an electronic POS System, you must seek Authorization using the following steps:

1. Call your Merchant Services Provider’s Authorization department.
2. The following minimum information will be requested:
   - Card Number
   - Merchant Number
   - Charge amount

   **Note:** In some situations, you may be asked for additional information such as Expiration Date or CID Number.

3. A response will be provided. If the request for Authorization is approved, capture the Approval for submission.
4. If you are submitting electronically, you must enter the Approval into your POS System. For instructions on how to complete this type of Charge, refer to your Merchant Services Provider’s operating instructions or contact them directly.

5.7 Card Identification (CID) Number

The Card Identification (CID) Number provides an extra level of Cardmember validation and is part of the Authorization process. The CID Number is printed on the Card.

If, during the Authorization, a response is received that indicates the CID Number given by the person attempting the Charge does not match the CID Number that is printed on the Card, re-prompt the customer at least one more time for the CID Number. If it fails to match again, follow your internal policies.

Note: CID Numbers must not be stored for any purpose. They are available for real time Charges only. See Chapter 8, "Protecting Cardmember Information". See Chapter 9, "Fraud Prevention" for more information on CID Numbers and CID Verification.

5.8 Authorization Reversal

It is a good practice to reverse an Authorization for an Approved Charge if you do not intend to send a submission to your Merchant Services Provider within the Authorization time limits. See Section 5.9, "Authorization Time Limit". You may reverse an Authorization for a corresponding Charge by:

- initiating an Authorization reversal message, or
- Contacting your Merchant Services Provider for instructions on how to reverse an Authorization.

After a Charge Record has been submitted, however, the Authorization cannot be cancelled or changed. For example, if you make an error in a Charge but have already submitted the Charge Record, you cannot systematically request a change in the Charge. You must instead, follow the procedures for Processing a Credit, as defined in Section 4.7, "Processing a Credit".

5.9 Authorization Time Limit

Authorization Approvals are valid for seven (7) days after the Authorization date, except for certain Charges from Merchants that are classified in the lodging and vehicle rental industries. You must obtain a new Approval if you submit the Charge to your Merchant Services Provider more than seven (7) days after the original Authorization date.

For Charges of goods or services that are shipped or provided more than seven (7) days after an order is placed, you must obtain an Approval for the Charge at the time the order is placed and again at the time you ship or provide the goods or services to the Cardmember.
The new Approval must be included in the Charge Record. If either of the Authorization requests is Declined, do not provide the goods or services or submit the Charge. If you do, you will be subject to a Chargeback.

5.10 Floor Limit

You must obtain an Authorization on all purchases, regardless of the amount, as a zero-dollar Floor Limit applies for all charges.

5.11 Pre-Authorization

A pre-Authorization is an Authorization request that you submit in advance of providing the goods or services, allowing you then to submit the Approved Charge (e.g., fuel pump CATs).

5.12 Additional Authorization Requirements

There are instances, which are outlined in the following table, when additional Authorization requirements apply.

Merchants classified in certain industries are also subject to additional specific Authorization requirements. See Chapter 12, "Specific Industries".

<table>
<thead>
<tr>
<th>Topic</th>
<th>Additional Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurring Billing</td>
<td>You must flag all requests for Authorization with a Recurring Billing indicator. To improve the likelihood of obtaining an Approval to an Authorization request, it is recommended that you periodically verify with Cardmembers that all their information (e.g., Card Number, Expiration Date, and billing address) is still accurate. See Section 4.17, &quot;Recurring Billing Charges&quot;.</td>
</tr>
<tr>
<td>American Express Gift Cheques and American Express Travelers Cheques</td>
<td>You are not required to obtain Authorization prior to accepting Gift and Travelers Cheques. You must, however, follow the appropriate procedures outlined in Section 4.19, &quot;Processing Travelers/Gift Cheques&quot;. Questions concerning the validity of Gift or Travelers Cheques can be addressed by calling the Travelers Cheque/Gift Cheque Customer Service at 1-866-296-5198.</td>
</tr>
<tr>
<td>Split Tender</td>
<td>During a Split Tender Transaction, the Cardmember uses multiple forms of payment for a single purchase (e.g., Prepaid Cards, cash, Card). You may follow your policy on combining payment on Prepaid Cards with any Other Payment Products or methods of payment. If the other payment method is a Card then you are required to follow all provisions of the Agreement. Check with your Merchant Services Provider to determine if your POS System is set up for Split Tender functionality.</td>
</tr>
</tbody>
</table>
6

Contents

6.1 Introduction
6.2 Transaction Cycle
6.3 Purpose of Submission
6.4 Submission Requirements – Electronic
6.5 Submission Requirements – Paper
6.6 How to Submit
6.1 Introduction

Merchants are familiar with commitments that keep their business running smoothly. One such commitment is to submit Transactions conducted at your Establishments to your Merchant Services Provider for payment.

Since payment cannot occur until the Transactions are submitted, you are encouraged to submit Transactions daily, or more frequently, to your Merchant Services Provider, even though you have up to seven (7) days to do so.

See Section 4.3, “Processing an In-Person Charge” and Section 4.7, “Processing a Credit” for additional information.

6.2 Transaction Cycle

Collect Transactions during the business day and submit them according to the instructions provided by your Merchant Services Provider.

6.3 Purpose of Submission

Refer to your Merchant Services Provider’s instructions on submission requirements.

6.4 Submission Requirements – Electronic

You must submit Transactions electronically except under extraordinary circumstances.

When you transmit Charge Data and Transmission Data electronically, you must still complete and retain Charge Records and Credit Records.

You must submit Charges and Credits only in Canadian Dollars.

6.4.1 Charge Submissions

You must submit all Charges to your Merchant Services Provider within seven (7) days of the date they are incurred. Charges are deemed “incurred” on the date the Cardmember indicates to you that they will pay for the goods or services purchased with the Card. Charges must not be submitted to your Merchant Services Provider until after the goods are shipped, provided, or the services are rendered. You must submit all Charges under the Establishment where the Charge originated.

For Aggregated Charges, the Charge must be submitted within seven (7) days of the date of the last purchase (and/or refund as applicable) that comprises the Aggregated Charge. See Section 4.13, “Aggregated Charges” for additional information.

Delayed Delivery Charges and Advance Payment Charges may be submitted before the goods are shipped, provided, or the services are rendered. See Section 4.14, “Delayed Delivery Charges” and Section 4.12, “Advance Payment Charges” for additional information.

6.4.2 Credit Submissions

You must submit all Credits to Merchant Services Provider within seven (7) days of determining that a Credit is due. You must submit each Credit under the Establishment where the Credit originated.
6.5 Submission Requirements – Paper

If you are presented with an unembossed Prepaid Card, you must hand-write the required information to process a Charge Record. See Section 4.6, “Charge Records”.

If you cannot obtain an electronic Authorization, you must obtain a Voice Authorization (see Section 5.6, “Obtaining a Voice Authorization” for more information).

Retain a copy of the Charge Record with the Cardmember’s signature for your records (see Section 4.6, “Charge Records”.

If, under extraordinary circumstances, you submit Transactions on paper, you must do so in accordance with instructions provided by your Merchant Services Provider.

Examples of circumstances that may prevent Merchants from submitting electronically are:
- special events (e.g., conferences, outdoor marketplaces, concerts)
- Merchants that do not conduct business from fixed locations
- remote locations, or Merchants who experience System Outages

If you submit Charges on paper, you must create a Charge Record containing all of the following required data:
- Full Card Number and Expiration Date (pursuant to Applicable Law), and if available, Cardmember name.
- The date the Charge was incurred.
- The amount of the Charge, which must be the total price for the purchase of goods and services (plus applicable taxes and gratuities) purchased on the Card.
- A clear description of the goods or services purchased by the Cardmember.
- 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. See Section 4.9, “Return and Cancellation Policies” for additional information.
- If a Card Present Charge, the Cardmember’s signature.
- If a Card Not Present Charge, the words “telephone order,” “mail order,” “Internet Order,” or “signature on file,” as applicable.

Charge Records submitted on paper must comply with the applicable requirements in Section 4.6, “Charge Records”.

Charges must be submitted in accordance with the applicable requirements described in Section 6.4, “Submission Requirements – Electronic”.

Refer to your Merchant Services Provider’s instructions when submitting Transactions on paper.
6.6 How to Submit

Many POS Systems are equipped with a “batch out” key or similar functionality. Contact your Merchant Services Provider for information on the best way to submit a batch.

In many cases, your POS System automatically processes the Transactions in Batches at the end of the day. On busy days, your Transaction volume may be greater than your POS System’s storage capability.

Consult information provided by your Merchant Services Provider to determine POS storage capacity and whether it’s necessary to submit multiple Batches (e.g., submit a Batch at midday and again in the evening).

Contact your Merchant Services Provider for additional information regarding submission requirements.
Contents

7.1 Introduction
7.2 Payment Errors or Omissions
7.3 Collecting from Cardmembers
7.1 Introduction

All settlement activity is the responsibility of your Merchant Services Provider and any questions or concerns should be directed to them for resolution.

7.2 Payment Errors or Omissions

Immediately notify your Merchant Services Provider of any error or omission in respect to your transactions or other fees or payments for Charges, Credits, or Chargebacks.

7.3 Collecting from Cardmembers

You must not bill or collect from any Cardmember for any purchase or payment made on the Card unless:

- Chargeback was exercised for such Charge,
- You have fully paid your Merchant Services Provider for such Charge, and
- You otherwise have the right to do so.
Contents

8.1 Data Security Requirements
8.2 Definitions
8.3 Standards for Protection of Cardmember Information
8.4 Data Incident Management Obligations
8.5 Reserved
8.6 Periodic Validation of Merchant Systems
8.7 Reserved
8.8 Disclaimer
8.1 Data Security Requirements

As a leader in consumer protection, American Express has a long-standing commitment to protect Cardholder Data and Sensitive Authentication Data, ensuring that it is kept secure. Compromised data negatively impacts consumers, Merchants, and Issuers. Even one incident can severely damage a company’s reputation and impair its ability to effectively conduct business. Addressing this threat by implementing security operating policies can help improve customer trust, increase profitability, and enhance a company’s reputation.

American Express knows that you share American Express’ concern and requires, as part of your responsibilities, that you comply with the data security requirements in the Agreement with your Merchant Services Provider and the American Express Data Security Requirements (DSR), which we may amend from time to time and which is available electronically at www.americanexpress.ca/dsr.

These requirements apply to all your equipment, systems, and networks (and their components) on which encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted.

8.2 Definitions

For the purposes of this Chapter 8, “Protecting Cardmember Information”, the following definitions apply:

**Approved Scanning Vendors (ASVs)** – Entities that have been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to certain Payment Card Industry Data Security Standard (PCI DSS) requirements by performing vulnerability scans of internet facing environments. See Section 8.6, “Periodic Validation of Merchant Systems”.

**Attestation of Compliance (AOC)** – A declaration of the status of your compliance with the PCI DSS, in the form provided by the Payment Card Industry Security Standards Council, LLC.

**Attestation of Scan Compliance (AOSC)** – A declaration of the status of your compliance with the PCI DSS based on a network scan, in the form provided by the Payment Card Industry Security Standards Council, LLC.

**Cardholder Data** – Has the meaning given in the then-current Glossary of Terms for the PCI DSS.

**Compromised Card Number** – An American Express Card account number related to a Data Incident.

**Covered Parties** – Any or all of your employees, agents, representatives, subcontractors, Processors, Service Providers, providers of your point-of-sale equipment or systems or payment processing solutions, Entities associated to your American Express merchant account, and any other party to whom you may provide Cardmember Information access in accordance with the Agreement.
**Data Incident** – An incident involving unauthorized access or use of encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) that are stored, processed, or transmitted on equipment, systems, and/or networks (or the components thereof) of yours or the use of which you mandate.

**Data Incident Event Window** – The period that begins up to 365 days prior to the Notification Date and ends 30 days after the Notification Date.

**EMV Specifications** – The specifications issued by EMVCo, LLC, which are available at [www.emvco.com](http://www.emvco.com).

**Encryption Key** – All keys used in the processing, generation, loading and/or protection of Account Data. This includes, but is not limited to, the following:
- Key Encrypting Keys: Zone Master Keys (ZMKs) and Zone PIN Keys (ZPKs)
- Master Keys used in secure cryptographic devices: Local Master Keys (LMKs)
- Card Security Code Keys (CSCKs)
- PIN Keys: Base Derivation Keys (BDKs), PIN Encryption Keys (PEKs), and ZPKs

**Merchant Level** – The designation assigned to Merchants related to their PCI DSS compliance validation obligations, as described in [Section 8.6, “Periodic Validation of Merchant Systems”](#).

**Notification Date** – The date that American Express provides Issuers with final notification of a Data Incident. Such date is contingent upon American Express’ receipt of the final forensic report or internal analysis and shall be determined in American Express’ sole discretion.

**Payment Application** – Has the meaning given to it in the then-current Glossary of Terms for Payment Card Industry Payment Application Data Security Standard, which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**PCI-Approved** – A PIN Entry Device or a Payment Application (or both) that appears at the time of deployment on the list of approved companies and providers maintained by the PCI Security Standards Council, LLC, which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**PCI Forensic Investigator (PFI)** – An Entity that has been approved by the Payment Card Industry Security Standards Council, LLC to perform forensic investigations of a breach or compromise of payment card data.


**PIN Entry Device** – Has the meaning given to it in the then-current Glossary of Terms for the Payment Card Industry PIN Transaction Security Requirements, Point of Interaction Modular Security Requirements, which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Point of Sale (POS) System** – An information processing system or equipment, including a terminal, personal computer, electronic cash register, contactless reader, or payment engine or process, used by a Merchant, to obtain Authorizations or to collect Transaction data, or both.
Qualified Security Assessors (QSAs) – Entities that have been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to the PCI DSS. See Section 8.6, "Periodic Validation of Merchant Systems".

Security Technology Enhancement Program (STEP) – American Express’ program in which Merchants are encouraged to deploy technologies that improve data security. To qualify for STEP, Merchants must not have had a Data Incident in the twelve (12) months prior to submitting the Annual Attestation of Compliance and conducted at least 75% of all Transactions using Point-to-Point Encryption or face to face Transactions using EMV Chip Enabled Devices.

Self-Assessment Questionnaire (SAQ) – A self-assessment tool created by the Payment Card Industry Security Standards Council, LLC, intended to evaluate and attest to compliance with the PCI DSS.

Sensitive Authentication Data – Has the meaning given in the then-current Glossary of Terms for the PCI DSS.

Validation Documentation – The AOC rendered in connection with an Annual Onsite Security Assessment or SAQ, the AOSC and executive summaries of findings rendered in connection with Quarterly Network Scans, or the annual STEP Attestation.
8.3 Standards for Protection of Cardmember Information

You must, and you must cause your Covered Parties, to:

- store Cardholder Data only to facilitate American Express Card Transactions in accordance with, and as required by, the Agreement.
- comply with the current version of the PCI DSS no later than the effective date for implementing that version.
- use, when deploying new or replacement PIN Entry Devices or Payment Applications (or both), in attended locations, only those that are PCI-Approved.

You must protect all Charge Records and Credit Records retained pursuant to the Agreement in accordance with these data security provisions; you must use these records only for purposes of the Agreement and safeguard them accordingly. You are financially and otherwise liable to your Merchant Services Provider for ensuring your Covered Parties’ compliance with this Chapter 8, “Protecting Cardmember Information” (other than for demonstrating your Covered Parties’ compliance with this policy under Section 8.6, “Periodic Validation of Merchant Systems” except as otherwise provided in this section).
8.4 Data Incident Management Obligations

You must notify your Merchant Services Provider immediately after discovery of a Data Incident.

You must conduct a thorough forensic investigation of each Data Incident. For Data Incidents involving 10,000 or more unique Card Numbers (or otherwise at American Express’ request), a PCI Forensic Investigator (PFI) must conduct this investigation. The unedited report must be provided to your Merchant Services Provider in accordance with their time frame for providing such information.

You must promptly provide to your Merchant Services Provider all Compromised Card Numbers and the forensic investigation report of the Data Incident. American Express reserves the right to conduct its own internal analysis to identify Card Numbers involved in the Data Incident. You must work with your Merchant Services Provider to rectify any issues arising from the Data Incident, including consulting with your Merchant Services Provider about your communications to Cardmembers affected by the Data Incident and providing (and obtaining any waivers necessary to provide) to your Merchant Services Provider all relevant information to verify your ability to prevent future Data Incidents in a manner consistent with the Agreement.

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. Upon your Merchant Services Provider’s request, you shall provide validation by a QSA that the deficiencies have been remediated.

Notwithstanding any contrary confidentiality obligation in the Agreement, American Express has the right to disclose information about any Data Incident to Cardmembers, 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.

8.5 Reserved

8.6 Periodic Validation of Merchant Systems

8.6.1 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 encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed or transmitted.

Step 1 - Enroll in American Express’ Compliance Program under this Policy

Level 1 Merchants, Level 2 Merchants, those Level 3 Merchants whom American Express has designated (as described below), and STEP-eligible Merchants, as described below, must submit applicable periodic Validation Documentation to their Merchant Services Providers. Please contact your Merchant Services Provider for more information regarding its data security compliance requirements.
American Express may require certain Level 3 merchants to enroll in American Express’ compliance program under this policy by sending them written notice. The designated Level 3 Merchant must enroll no later than ninety (90) days following receipt of the notice.

Step 2 - Determine Your Merchant Level and Validation Requirements

Most Merchant Levels are based on the volume of Transactions submitted by all of your Establishments. You will fall into one of the Merchant Levels specified in the following table.

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Definition</th>
<th>Validation Documentation</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.5 million Transactions or more per year; or any Merchant that American Express otherwise deems a Level 1 Merchant</td>
<td>annual on-site security assessment report and quarterly network scan</td>
<td>Mandatory</td>
</tr>
<tr>
<td>2</td>
<td>50,000 to 2.5 million Transactions per year</td>
<td>annual Self Assessment Questionnaire (SAQ) and quarterly network scan</td>
<td>Mandatory</td>
</tr>
<tr>
<td>3 – Designated</td>
<td>Less than 50,000 Transactions per year and designated by American Express as being required to submit validation documents</td>
<td>annual SAQ and quarterly network scan</td>
<td>Mandatory</td>
</tr>
<tr>
<td>3 – All Other</td>
<td>Less than 50,000 Transactions per year but not classified as Level 3 Designated</td>
<td>annual SAQ and quarterly network scan</td>
<td>Strongly recommended*</td>
</tr>
<tr>
<td>STEP**</td>
<td>All eligible Merchants</td>
<td>Annual STEP Attestation</td>
<td>Mandatory for Merchants desiring STEP eligibility</td>
</tr>
</tbody>
</table>

* For the avoidance of doubt, Level 3 Merchants (other than Designated Level 3 Merchants) need not submit Validation Documentation, but nevertheless must comply with, and are subject to liability under all other provisions of these Data Security Requirements.

** STEP is not available for Merchants that have had a Data Incident in the 12 months prior to submitting the Annual Attestation of Compliance or do not otherwise meet the STEP eligibility requirements.

American Express, or your Merchant Services Provider, may verify the results of your PCI Validation process up to and including engaging, at American Express' expense, a Qualified Security Assessor (QSA) of its own choosing.
Step 3 - Determine your Merchant Level and the Validation Documentation that you must send to your Merchant Services Provider.

<table>
<thead>
<tr>
<th>Validation Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Onsite Security Assessment</td>
</tr>
</tbody>
</table>
| The annual onsite security assessment is a detailed onsite examination of your equipment, systems, and networks (and their components) where encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted. It must be performed by:
  - a QSA, or
  - you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal.
  The annual onsite security assessment must be submitted annually to your Merchant Services Provider on the applicable AOC. To fulfil validation obligations under this policy, the AOC must certify compliance with all requirements of the PCI DSS and, upon request, include copies of the full report on compliance. |
| Annual Self Assessment Questionnaire (SAQ) |
| The annual self assessment is a process using the PCI DSS SAQ that allows self-examination of your equipment, systems, and networks (and their components) where encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted. It must be performed by you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal. The AOC section of the SAQ must be submitted annually to your Merchant Services Provider. To fulfil validation obligations under this policy, the AOC section of the SAQ must certify your compliance with all requirements of the PCI DSS and include full copies of the full report on compliance. |
| Quarterly Network Scans |
| The quarterly network scan is a process that remotely tests your internet-connected computer networks and web servers for potential weaknesses and vulnerabilities. It must be performed by an ASV. You must complete and submit the ASV Scan Report AOSC or executive summary of findings of the scan (and copies of the full scan, on request) quarterly to your Merchant Services Provider. To fulfil validation obligations under this policy, the AOSC or executive summary must certify that the results satisfy the PCI DSS scanning procedures, that no high risk issues are identified, and that the scan is passing or compliant. |
Step 4 - Send the Validation Documentation to Your Merchant Services Provider

Level 1, Level 2, and designated Level 3 Merchants must submit the Validation Documentation marked "mandatory" in the table in Step 2.

- Level 1 Merchants' Validation Documentation must include the AOC from the annual onsite security assessment report and AOSC or executive summaries of findings of quarterly network scans.
- Level 2 Merchants' and designated Level 3 Merchants' Validation Documentation must include the AOC from the SAQ and the AOSC or the executive summaries of findings of the Quarterly Network Scans, as described in the table above.
- Level 3 Merchants (other than designated Level 3 Merchants) are not required to submit Validation Documentation (but must comply with, and are subject to liability under, all other provisions of this policy).
- STEP-eligible Merchants may submit the STEP Annual Attestation in place of other Validation Documentation.

You must submit your Validation Documentation to your Merchant Services Provider as instructed by them. If you have general questions about the program or the process of submitting Validation Documentation, please contact your Merchant Services Provider.

Compliance and validation are completed at your expense. By submitting Validation Documentation to your Merchant Services Provider, you represent and warrant that you are authorized to disclose the information contained therein to your Merchant Services Provider and to American Express, and are providing the Validation Documentation without violating any other party's rights.

8.6.2 Merchants Not Compliant with PCI DSS

If you are not compliant with the PCI DSS, then you must complete an AOC including "Part 4. Action Plan for Non-Compliant Status" and designate a remediation date, not to exceed twelve (12) months following the date of the AOC, for achieving compliance. You must submit this AOC with "Action Plan for Non-Compliant Status" to your Merchant Services Provider. You shall provide your Merchant Services Provider with periodic updates of your progress toward remediation under the "Action Plan for Non-Compliant Status". For the avoidance of all doubt, Merchants that are not compliant with PCI DSS are not eligible for STEP.

8.6.3 Non-Validation Fees and Termination of Agreement

American Express and your Merchant Services Provider have the right to impose non-validation fees on you and terminate the Agreement if you do not fulfil these requirements or fail to provide the mandatory Validation Documentation by the applicable deadline.

Your Merchant Services Provider will notify you separately of the applicable deadline for each annual and quarterly reporting period.

If your Merchant Services Provider does not receive your mandatory Validation Documentation, then your Merchant Services Provider may have the right to terminate the Agreement in accordance with its terms as well as impose non-validation fees on you.

Visit pcisecuritystandards.org for:
- QSAs and ASVs
- SAQs
- The AOC and AOSC
8.6.4 Periodic Validation of STEP-eligible Merchants

Merchants that are compliant with PCI DSS may also qualify for American Express’ STEP if they deploy certain additional security technologies throughout their Card processing environments.

STEP applies only if the Merchant has not experienced a Data Incident in the previous twelve (12) months and if 75% of all merchant Card transactions are performed using:

- EMV – on an active Chip-Enabled Device having a valid and current EMVCo (www.emvco.com) approval/certification and capable of processing AEIPS compliant Chip Card Transactions, or
- Point-to-Point Encryption (P2PE) – communicated to the Merchant’s processor using a PCI-SSC-approved or QSA-approved Point-to-Point Encryption system.

If you are classified as a STEP-eligible Merchant, you may submit a declaration of the status of your compliance with the PCI DSS, in the form which is available through your Merchant Services Provider (Annual STEP Attestation) instead of other Validation Documentation. It must be performed by you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal. You must complete the process by submitting the STEP Attestation annually to your Merchant Services Provider (See Section 8.6, “Periodic Validation of Merchant Systems”, Step 3).

8.7 Reserved

8.8 Disclaimer

AMERICAN EXPRESS HEREBY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND LIABILITIES WITH RESPECT TO THESE DATA SECURITY REQUIREMENTS, THE PCI DSS, THE EMV SPECIFICATIONS, AND THE DESIGNATION AND PERFORMANCE OF QSAs, ASVs, OR PFIs (OR ANY OF THEM), WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Issuers are not third-party beneficiaries under these Data Security Requirements.
Contents

9.1 Introduction
9.2 Strategies for Deterring Fraud
9.3 Card Acceptance Policies
9.4 Card Security Features
9.5 Recognizing Suspicious Activity
9.6 Prepaid Card Security Features
9.7 Recognizing Suspicious Activity for Prepaid Cards
9.8 Travelers Cheque and Gift Cheque Security Features
9.9 Fraud Mitigation Tools
9.1 Introduction

You work hard to protect the interests of your business and Cardmembers. Unfortunately, fraudulent Card use can undermine your best efforts. Millions of dollars are lost each year because of such fraud.

American Express offers a full suite of tools and programs that can help to mitigate the chances of fraud on American Express Cards and reduce this cost to your business.

Some Merchants may not be eligible to participate in the full suite of fraud tools and fraud liability shift programs offered. Additionally, American Express may, in our sole discretion, immediately suspend or terminate a Merchant from using any fraud tool or participation in any fraud liability shift program and American Express may suspend or terminate any fraud tool or fraud liability shift program at any time.

This section of the Merchant Operating Guide offers fraud mitigation tips for both Card Present and Card Not Present Transactions. Contact your Merchant Services Provider for information related to fraud mitigation tools and resources that may be available for your use.

9.2 Strategies for Deterring Fraud

Implementing multiple layers of fraud protection to help secure your business is recommended. These layers may include a combination of your point of sale procedures and controls as well as implementation of fraud mitigation tools.

Layers of Protection

Your first layer for mitigating fraud is to follow the Card acceptance policies and procedures, as outlined in Chapter 4, “Transaction Processing”. Other fraud mitigation strategies that you choose to implement may include any combination of:

- recognition of suspicious behaviours or circumstances that may signal fraudulent activity
- implementation of fraud mitigation tools that take advantage of American Express’ risk controls to identify fraudulent activity
- additional risk models or controls that you can develop internally or obtain externally from third parties

American Express is committed to working with you and your Merchant Services Provider to deploy tools that can help reduce the likelihood that fraudulent Charges will be Approved. The implementation and use of the strategies and tools detailed in this section, however, does not guarantee that (i) the person making the Charge is the Cardmember, (ii) the Charge is in fact valid or bona fide, (iii) you will be paid for the Charge, or (iv) you will not be subject to a Chargeback.
9.3 Card Acceptance Policies

A critical component in your overall fraud mitigation strategy is to follow your Merchant Services Provider’s operating instructions including American Express Card acceptance procedures, as defined in Chapter 4, “Transaction Processing”. These procedures can also serve as your first line of defence against potential fraud. The additional layers of fraud mitigation mentioned previously can supplement this line of defence.
9.4 Card Security Features

In many cases, the physical appearance of the Card will offer the most obvious clues of fraudulent activity.

American Express Card security features are designed to help you assess whether a Card is authentic or has been altered. Ensure that all of your personnel are familiar with American Express’ Card’s security features so they can identify potentially compromised Cards.

The following picture is just one example of an American Express Card as a number of different Cards are offered. These are some things you must look for:

1. Pre-printed CID Numbers usually appear above the Card Number, on either the right or the left edge of the Card.
2. All American Express Card Numbers start with “37” or “34.” The Card Number appears embossed on the front of the Card. Embossing must be clear, and uniform in sizing and spacing. Some Cards also have the Card Number printed on the back of the Card in the signature panel. These numbers, plus the last four digits printed on the Charge Record, must all match.
3. Do not accept a Card outside the Valid Dates.
4. Only the person whose name appears on an American Express Card is entitled to use it. Cards are not transferable.
5. Some Cards contain a holographic image on the front or back of the plastic to determine authenticity. Not all American Express Cards have a holographic image.
6. Some Cards have a Chip on which data is stored and used to conduct a Charge.
7. The signature on the back of the Card must match the Cardmember’s signature on the Charge Record, and must be the same name that appears on the front of the Card. The signature panel must not be taped over, mutilated, erased, or painted over. Some Cards also have a three-digit Card Security Code (CSC) number printed on the signature panel.

Note: The security features for Prepaid Cards and Travelers Cheques are listed in Section 9.6, “Prepaid Card Security Features,” and Section 9.8, “Travelers Cheque and Gift Cheque Security Features.”
9.4.1 Compromised Card Security Features

In this example of an altered Card, the signature panel has been painted white under the signature. In addition, the Card Number has been erased from the back panel.

Do not accept a Card if:

**Altered Magnetic Stripe**
- The Magnetic Stripe has been altered or destroyed.
- The Card Number on the front of the Card does not match the number printed on the back (when present), or the last four digits printed on the Charge Record (or both).

**Altered Front of the Card**
- The Card Number or Cardmember name on the front of the Card appears out of line, crooked, or unevenly spaced.
- The ink on the raised Card Number or Cardmember name is smudged or messy.
- The Card Number or Cardmember name is not printed in the same typeface as the American Express typeface.

**Altered Back of the Card**
- The Card Number printed on the back of the Card (when present) is different from the Card Number on the front.
- The Card Number on the back of the Card (when present) has been chipped off or covered up.
- The signature panel has been painted-out, erased, or written over.

**Altered Appearance of the Card**
- There are "halos" of previous embossing or printing underneath the current Card Number and Cardmember name.
- A portion of the surface looks dull compared with the rest of the Card. Valid American Express Cards have a high-gloss finish.
- The Card has a bumpy surface or is bent around the edges.
- You suspect any Card security features have been compromised.
- The Card appears physically altered in any way.

If you suspect Card misuse, follow internal store policies, and, if directed to do so, call your Merchant Services Provider and state that you have a Code 10. **Never put yourself or your employees in unsafe situations, nor physically detain or harm the holder of the Card.**
Often, you can look closely at Cards to determine if they’re altered or counterfeit. As another layer in your internal fraud prevention program, educate yourself and all your personnel on how to identify a potentially altered Card.

### 9.5 Recognizing Suspicious Activity

Diligently scrutinizing behaviours and circumstances can help prevent you from being victimized by fraud. As a prudent Merchant, you must always be aware of circumstances that may indicate a fraudulent scheme or suspicious behaviours that may flag a fraudulent customer.

**Suspicious Behaviour**

A suspicious situation may arise, causing you to question the authenticity of the Card, or the legitimacy of the person presenting it. Any single behaviour may not be risky. However, when customers exhibit more than one of the following behaviours, your risk factor may increase:

- Larger-than-normal Transaction dollar amounts,
- Orders containing many of the same items,
- Orders shipped to an address other than a billing address,
- Orders using anonymous/free email domains,
- Orders sent to postal codes or countries where you show a history of fraudulent claims,
- Orders of a "hot" product (i.e., highly desirable goods for resale),
- Customer is a first-time shopper,
- Customer is purchasing large quantities of high-priced goods without regard to colour, size, product feature, or price,
- Customer comes in just before closing time and purchases a large quantity of goods,
- Customer wants to rush or overnight the order,
- Customer has a previous history of Disputed Charges,
- Customer is rude or abusive toward you; wanting to rush or distract you,
- Customer frequents your Establishment to make small purchases with cash, then returns to make additional purchases of expensive items with a Card.

If you suspect Card misuse, follow your internal store policies, and immediately call your Merchant Services Provider with a Code 10. **Never put yourself or your employees in unsafe situations, nor physically detain or harm the holder of the Card.**
9.6  Prepaid Card Security Features

You are responsible for following all American Express’ Prepaid Card acceptance procedures in Section 4.18, "Processing Prepaid Cards". Although there are a number of unique Prepaid Cards, all Prepaid Cards share similar features, except that:

- Prepaid Cards may or may not be embossed, and
- The following features may appear on the front or back of the Card (or a combination of both):

1. The American Express logo generally appears in the bottom right corner.
2. The words PREPAID or INCENTIVE will generally be shown above the American Express logo.
3. Cards pre-loaded with funds may show the dollar amount or the total points (reloadable Cards generally will not show a number).
4. The CID Number will appear usually above the Card Number or above the logo.
5. The Card Number appears on the Card.
6. The Valid Date or Expiration Date appears on the Card.
7. The recipient’s name or company name may appear on the Card; otherwise a generic “Recipient” or “Traveler” may appear, or this area might be blank.

9.7  Recognizing Suspicious Activity for Prepaid Cards

American Express recommends that you follow the procedures in the preceding Section 9.5, “Recognizing Suspicious Activity” in addition to being vigilant for the following suspicious behaviours related specifically to Prepaid Cards:

- Customer frequently makes purchases and then returns goods for cash. (To avoid being the victim of this scheme, you should follow your internal store procedures when you cannot issue a Credit on the Card used to make the original purchase.)
- Customer uses Prepaid Cards to purchase other Prepaid Cards.
- Customer uses large numbers of Prepaid Cards to make purchases.

9.8  Travelers Cheque and Gift Cheque Security Features

Even though American Express’ Travelers Cheques and Gift Cheques offer more convenience and security, counterfeit products circulate worldwide. You must verify all cheque products presented at your Establishment and contact the Travelers Cheque/Gift Cheque Customer Service with questions or suspicions.
One of the easiest and most effective tests to determine authenticity is the smudge test:

1. Turn the cheque over (non-signature side).
2. Locate the denomination on the right side of the cheque. Wipe a moistened finger across the denomination. The ink should not smudge.
3. Wipe a moistened finger across the denomination on the left side of the cheque. The ink should smudge.

The following shows an example of a smudge test:

For Travelers and Gift Cheque acceptance procedures, see Section 4.19, “Processing Travelers/Gift Cheques”. American Express also recommends that you follow the procedures in the preceding Section 9.5, “Recognizing Suspicious Activity” to assist you in the mitigation of fraud.

As another layer of protection, there are a number of security features inherent in American Express’ Travelers Cheque and Gift Cheque products. Following are a few security features to help you recognize an authentic Cheque.

- Centurion Portrait
- Watermark
- Security Threads
- Holographic Foils
9.9 Fraud Mitigation Tools

Fraud mitigation tools are available for both Card Present and Card Not Present Transactions to help verify that a Charge is valid. These tools help you mitigate the risk of fraud at the point of sale, but are not a guarantee that (i) the person making the Charge is the Cardmember, (ii) the Charge is in fact valid or bona fide, (iii) you will be paid for the Charge, or (iv) you will not be subject to a Chargeback.

For optimal use of the tools, it is critical that:

- you comply with the applicable sections of the Technical Specifications (see Section 2.1, "Compliance with the Technical Specifications"), and
- you provide high quality data in the Authorization request.

American Express offers strategies and tools for preventing fraud. For more information about what you and your business can do, review the tools listed below and contact your Merchant Services Provider to determine what tools are supported.
## 9.9.1 Card Not Present Fraud Tools

<table>
<thead>
<tr>
<th>Description</th>
<th>Automated Name and Address Verification</th>
<th>Email Verification</th>
<th>Billing Phone Number Verification</th>
<th>Enhanced Authorization</th>
<th>Charge Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helps to ensure that the person placing the order actually has the Card in his or her possession and is not using a stolen Card Number.</td>
<td>Helps issuer evaluate Cardmember identity by comparing information provided by the Cardmember at the point of sale with Cardmember billing information not available on the Card.</td>
<td>Email Address Verification helps evaluate Cardmember identity by comparing information provided by the customer during the check-out process with Cardmember information not available on the Card.</td>
<td>Billing Phone Number Verification helps evaluate Cardmember identity by comparing information provided by the customer during the check-out process with Cardmember information not available on the Card.</td>
<td>Helps mitigate fraud before a Transaction is authorized by analyzing key data elements submitted with Authorization requests.</td>
<td>Enables you to obtain additional verification on orders you suspect may be fraudulent.</td>
</tr>
<tr>
<td>Contact your Merchant Services Provider</td>
<td>Contact your Merchant Services Provider</td>
<td>Contact your Merchant Services Provider</td>
<td>Contact your Merchant Services Provider</td>
<td>Contact your Merchant Services Provider</td>
<td>Contact your Merchant Services Provider</td>
</tr>
</tbody>
</table>

**American Express Merchant Operating Guide - Canada**

Fraud Prevention

This document contains sensitive, confidential and trade secret information, and must not be disclosed to third parties without the express prior written consent of Amex Bank of Canada.

October 2017 62
## 9.9.2 Card Present Fraud Tools

<table>
<thead>
<tr>
<th>Description</th>
<th>Purpose</th>
<th>How To Implement</th>
</tr>
</thead>
<tbody>
<tr>
<td>You request the four-digit CID number printed on the Card from the Cardmember and send it with the Authorization request to the Issuer.</td>
<td>Helps to ensure that the person making the purchase is not using an altered or duplicated Card.</td>
<td>Contact your Merchant Services Provider</td>
</tr>
<tr>
<td>Issuer compares the CID number provided with that on file for the Card and, based on the comparison, returns a match code to you.</td>
<td>Can signal tampering and alteration of the Card’s Magnetic Stripe.</td>
<td>Contact your Merchant Services Provider</td>
</tr>
<tr>
<td>POS terminal captures data encoded in the Track 1 of the Magnetic Stripe and sends it to the Issuer with the Authorization request.</td>
<td>Provides enhanced protection against fraud from lost, stolen, and counterfeit Cards.</td>
<td>Contact your Merchant Services Provider</td>
</tr>
<tr>
<td>Issuer compares information in track to information on file and sends approval decision.</td>
<td>Helps detect high risk patterns of a particular POS device.</td>
<td>Contact your Merchant Services Provider</td>
</tr>
<tr>
<td>Chip technology uses an embedded microchip to encrypt card information, making it more difficult for unauthorized users to copy or access the data. Data can only be accessed when the Card is inserted into a chip-enabled terminal.</td>
<td>A special phrase you use to indicate to your Merchant Services Provider that you have suspicions concerning the Cardmember, the Card, the CID, and/or the circumstances of the sale.</td>
<td>If you suspect Card misuse, follow your internal store policies, and, if directed to do so, call your Merchant Services Provider with a Code 10 Authorization Request. Only pick up a Card if directed to do so by your Merchant Services Provider or the Issuer. Never put yourself or your employees in unsafe situations.</td>
</tr>
</tbody>
</table>
Contents

10.1 Introduction
10.2 Prohibited Merchants
10.3 Monitoring
10.4 Fraudulent, Deceptive, or Unfair Business Practices, Illegal Activities, or Prohibited Uses of the Card
10.1 Introduction

As a Merchant, you understand the hard work and dedication it takes to keep a business running. At American Express, we also work hard to maintain our business and uphold our reputation as a world-class global payments and network company. Part of our regimen is to evaluate Merchants to ensure compliance with our policies and procedures, in addition to assessing any potential risk to our business.

10.2 Prohibited Merchants

Some Merchants are not eligible (or may become ineligible) to accept the Card. American Express may terminate Card acceptance (including immediate termination without prior notice to you) if it is determined that you meet any of the following criteria:

- Your participation as a Merchant on the American Express Network or acceptance of Cards (or both) may cause American Express not to be in compliance with Applicable Laws, regulations, or rules.
- You do not have a verifiable physical address and can only be reached by telephone.
- You are involved (or knowingly participate or have participated) in a fraudulent or illegal activity.
- You are identified as a sponsor of international terrorism as warranting special measures due to money laundering concerns, or as non-cooperative with international anti-money laundering principles or procedures.
- You are listed on the List of Names made subject to the Regulations Establishing a List of Entities pursuant to subsection 83.05(1) of the Criminal Code of Canada or the United Nations Suppression of Terrorism Regulations, OSFI, or any other such list or regulation that may exist now or in the future.
- You fall into one of the following categories and/or accept Transactions for the prohibited activities displayed in the following table.

<table>
<thead>
<tr>
<th>Business Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult Entertainment</td>
<td>Internet adult digital content sites.</td>
</tr>
<tr>
<td>Cash Advances</td>
<td>Establishments that accept the Card in connection with repayment of cash advances, including, but not limited to payday loans, pawn loans, or payday advances.</td>
</tr>
<tr>
<td>Check Cashing/Guarantee</td>
<td>Cardmember cashes a check using the Card as a check guarantee.</td>
</tr>
<tr>
<td>Child Pornography</td>
<td>Any written or visual depiction of a minor engaged in obscene or sexually explicit conduct.</td>
</tr>
<tr>
<td>Condo (Real Estate) Down Payments</td>
<td>Payments to other debt-related real estate products.</td>
</tr>
<tr>
<td>Credit Restoration Services</td>
<td>A service that promises to remove negative factors from a consumer’s credit report by disputing it with the credit bureau and correcting errors like outdated or incorrect claims.</td>
</tr>
<tr>
<td>Business Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Debt Collection</td>
<td>Collection agencies, payday lenders, factoring companies, liquidators, bailiffs, bail bondsmen, and bankruptcy lawyers. <em>Exceptions: bail bondsmen fees (i.e., Merchant must not accept Cards to pay for a bail bond but Merchant may accept the Card to pay the fee to the bail bondsman).</em></td>
</tr>
<tr>
<td>Door-to-door Sales</td>
<td>Unsolicited vendors with immediate payment expected.</td>
</tr>
<tr>
<td>Escort Services and Non-Licensed Massage Parlours</td>
<td>Payment of potentially sexual related services.</td>
</tr>
<tr>
<td>Financial Services</td>
<td>Banks, credit unions, savings and loans associations, equities (defined as an instrument that signifies an ownership position, or equity, in a corporation, and represents a claim on its proportionate share in the corporation’s assets and profits, e.g., stocks, bonds, and securities), unit trusts, mutual funds, foreign exchange, Bureau de Change, and payday lenders.</td>
</tr>
<tr>
<td>Foreign Exchange Bureaus</td>
<td>Any establishment that allows the purchase of foreign exchange currency using an American Express Card product.</td>
</tr>
<tr>
<td>Future Services</td>
<td>Investments made on futures maturity of goods and/or services with an intention of gaining return on investment (e.g., stock market, wine future, horse breeding, timber investment, precious metals).</td>
</tr>
<tr>
<td>Gambling</td>
<td>Casino Gaming Chips, Off-Track Betting and Wagers at Race Tracks, Gambling Services, Internet Gambling Sites. <em>Exceptions: Accommodations, restaurant, bar or gift shop facilities within a casino complex.</em></td>
</tr>
<tr>
<td>Lottery Sales</td>
<td>Sales of lottery tickets.</td>
</tr>
<tr>
<td>Marijuana Dispensaries</td>
<td>Sellers of marijuana, whether sold for recreational or medicinal purposes.</td>
</tr>
<tr>
<td>Mortgage Payments</td>
<td>Payments to other debt related real estate products.</td>
</tr>
</tbody>
</table>
| Multi-level Pyramid Sales            | Multi-level marketing system using one or more of the following practices:  
  - Participants pay for the right to receive compensation for recruiting new participants.  
  - Participants are required to buy a specific quantity of products, other than at cost, for the purpose of advertising before participants are allowed to join the plan or advance within the plan.  
  - Participants are sold unreasonable quantities of the product or products (also known as inventory loading).  
  - Participants are not allowed to return products on reasonable commercial terms.                                                                                                                                   |
## Risk Management

### Mixed Business

If any segment of your Charge volume is submitted from the aforementioned business types, you must not accept the Card for those Transactions. If you accept the Card for these Transactions, American Express will exercise Chargeback. You may also be placed in one of American Express’ Chargeback programs or cancelled (or disentitled) for Card acceptance (or both).

### 10.3 Monitoring

After you become a Merchant on the Network, American Express monitors to identify potential risks. American Express uses internal and third-party information when monitoring and looks for, among other things:

- disproportionate Disputed Charges and Chargebacks,
- Merchants that meet the High Risk Merchant criteria set forth in Subsection 10.3.1, “High Risk Merchants”,
- schemes to defraud American Express,
- legal, compliance, or other credit and fraud risks, and

<table>
<thead>
<tr>
<th>Business Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payday Lenders</td>
<td>Payday lenders are companies that provide short-term loans at high rates of interest to consumers to help them meet short-term expenses (e.g., repayment of cash advances, including payday loans and payday advances).</td>
</tr>
<tr>
<td>Prostitution</td>
<td>Payment for sexual services.</td>
</tr>
<tr>
<td>Timeshares</td>
<td>Selling partial ownership of a property for use as a holiday home, whereby a Cardmember can buy the rights to use the property for the same fixed period annually.</td>
</tr>
<tr>
<td>Travel Tour Operators</td>
<td>Travel Tour Operators without membership to a Travel Industry Bonding Agency or not an authorized ticket agent (e.g. ARC/IATA/ABTA).</td>
</tr>
<tr>
<td>Unlawful Sale of Prescription Drugs</td>
<td>Online sale of prescription drugs to U.S. consumers by a pharmacy that is not:</td>
</tr>
</tbody>
</table>
|                                        | - Certified by VIPPS® (Verified Internet Pharmacy Practice Sites); or
|                                        | - Licensed by the Board of Pharmacy in the state in which it is located.                                                               |
| Unlawful Sale of Tobacco and Smokeless Tobacco | Online sale of tobacco and smokeless tobacco products to U.S. consumers by a retailer that is not:                                      |
|                                        | - Certified to pay state taxes; and/or                                               |
|                                        | - Preventing sale of tobacco products to underage consumers.                          |
| Unregulated Charities                  | Merchant that does not have a tax exemption or local council registration number.                                                          |
| Virtual Currency                       | Card acceptance to purchase virtual currency that can be exchanged for real currency (e.g., Bitcoin).                                     |
data submitted in compliance with the Technical Specifications.

American Express will monitor you for actions or behaviours (or both) which may put American Express, Issuers, or Cardmembers at risk. Based on the results of American Express’ monitoring, American Express reserves the right to take action to mitigate its risk, including one or more of the following (in American Express’ sole judgement):

- requesting information about your finances and operations,
- instituting Card acceptance restrictions,
- exercising Chargeback, rejecting Charges, charging fees, or assessments,
- requesting corrective action, or
- terminating any Card acceptance privileges or suspending those privileges until the risk has subsided.

### 10.3.1 High Risk Merchants

High Risk Merchants are those types of businesses that American Express determines put American Express at risk and/or whose business has excessive occurrences of fraud.

If American Express determines, in American Express’ sole discretion, that you meet the criteria for one or more of the High Risk Merchant categories, American Express may place you in a Chargeback program and/or terminate Card acceptance.

American Express considers you to be "high risk" if you meet at least one criterion in the following table:*

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High risk industry</td>
<td>Your type of business has had historically high occurrences of fraud and Disputed Charges with American Express or as compared to other similarly situated Merchants (or both). Examples of high risk industries include: internet electronic delivery and aggregators.</td>
</tr>
<tr>
<td>Performance</td>
<td>You have recent high occurrences of fraud that present an excessive risk to American Express. You have had high occurrences of fraud and/or high fraud amounts for a number of consecutive months.</td>
</tr>
<tr>
<td>Cancelled derogatory</td>
<td>Your Agreement was cancelled due to unsatisfactory activity.</td>
</tr>
<tr>
<td>Fictitious</td>
<td>You accept Cards fraudulently.</td>
</tr>
<tr>
<td>Prohibited</td>
<td>You are not eligible to accept the Card on the American Express Network. For prohibited criteria see Section 10.2, “Prohibited Merchants”.</td>
</tr>
</tbody>
</table>

* This list is not exhaustive and American Express may, in its sole discretion, consider other criteria as high risk and modify this list accordingly.
10.4 Fraudulent, Deceptive, or Unfair Business Practices, Illegal Activities, or Prohibited Uses of the Card

If your Merchant Services Provider determines, or is notified by American Express that there is reason to believe, that you engage or have engaged (or knowingly participate or knowingly have participated) in any of the activities listed in the following table; in any scheme that defrauds American Express, Issuers, and/or Cardmembers; or in business practices that American Express deems fraudulent, deceptive, and/or unfair, corrective action may be taken on you, which may include but is not limited to:

- placement in a Chargeback program,
- exercising Chargeback or rejecting Charges, or
- termination of the Agreement (including immediate termination without prior notice to you) or disentitlement of Card acceptance.

<table>
<thead>
<tr>
<th>Factoring</th>
<th>Factoring occurs when Transactions do not represent bona fide sales of goods or services at your Establishments (e.g., purchases at your Establishments by your owners (or their family members) or employees contrived for cash flow purposes).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collusion</td>
<td>Collusion refers to activities whereby your employee collaborates with another party to conduct fraudulent Transactions. It is your responsibility to set appropriate controls to mitigate such activity as well as to have monitoring systems to identify such activity.</td>
</tr>
<tr>
<td>Marketing fraud</td>
<td>Marketing fraud occurs when mail, telephone, or Internet Order solicitations are used for fraudulent or deceptive purposes (e.g., to obtain valid Cardmember Information for fraudulent Transactions, or to charge unauthorized sales to a valid Card account).</td>
</tr>
<tr>
<td>Identity theft</td>
<td>Identity theft is the assumption of another person’s identity to gain access to their finances through fraudulent Merchant setup or fraudulent Transactions.</td>
</tr>
<tr>
<td>Illegal activities, fraudulent (other than marketing), unfair or deceptive business practices, or prohibited uses of the Card</td>
<td>If American Express determines, or has reason to believe, in American Express’ sole discretion, that you engage or have engaged (or knowingly participate or knowingly have participated) in fraudulent, deceptive, or unfair business practices, or accepted the Card to facilitate, directly or indirectly, illegal activity of any kind, and without waiving American Express’ other rights and remedies, American Express has the right to terminate Card acceptance. If American Express finds that the Transaction involved a prohibited use of the Card (see Section 3.3, &quot;Prohibited Uses of the Card&quot;), American Express may apply the corrective actions listed above.</td>
</tr>
</tbody>
</table>

* This list is not exhaustive and does not reflect all circumstances under which American Express may act to protect the interest of American Express.
Contents

11.1 Introduction
11.2 Disputed Charge Process
11.3 Tips for Avoiding Chargebacks
11.1 Introduction

11.1.1 A dispute happens when a Cardmember questions some aspect of an item on their billing statement — such as they don’t recognize the Charge; they don’t agree with the amount; they were charged twice; the goods or services were not received; and many more.

11.1.2 You must not suggest or require Cardmembers to waive their right to dispute any Transaction.

11.2 Disputed Charge Process

11.2.1 If a Cardmember disputes a Charge, American Express opens a case. With respect to a Disputed Charge:

- You may receive an Inquiry from your Merchant Services Provider prior to a Chargeback being exercised, or
- Prior to receiving an Inquiry, you may receive a Chargeback if it is determined that sufficient information is available to resolve the Disputed Charge in favour of the Cardmember.

---

**Diagram:**

- **INQUIRY:** American Express sends an Inquiry notice to Merchant Services Provider.
- **A CARDMEMBER DISPUTES A CHARGE:** Merchant Services Provider sends an Inquiry notice to Merchant.
- **SUBMIT DOCUMENTS:**
  - **CASE RESOLVED:** The case may be resolved in your favour if you provide the appropriate supporting documents and information within the time frame specified by your Merchant Services Provider.
  - **CHARGEBACK:** A Chargeback will be processed if your reply is insufficient; you do not reply on time; or you authorize us.
  - **REVERSAL:** A Reversal may be processed if you provide the appropriate supporting documents within the time frame specified by your Merchant Services Provider.
  - **CHARGEBACK STANDS:** The Chargeback stands if your reply is insufficient; or you do not reply on time.
- **UPFRONT CHARGEBACK:** American Express sends a Chargeback notice to Merchant Services Provider.
11.2.2 American Express has Chargeback rights:
- whenever Cardmembers bring Disputed Charges, as described in this section, or have rights under Applicable Law or contract to withhold payments,
- in cases of actual or alleged fraud relating to Charges,
- if you do not comply with the Agreement (including omitting any Transaction Data from Charge Submissions), even if your Merchant Services Provider and/or American Express had notice when you were paid by your Merchant Services Provider for a Charge that you did not so comply and even if you obtained Authorization for the Charge in question, or
- as provided elsewhere in the Agreement.

Contact your Merchant Services Provider for additional information and guidance regarding Disputed Charges and Chargebacks.

11.3 Tips for Avoiding Chargebacks

Inquiries can be expensive and time consuming for all parties involved. Follow these general steps and you may avoid unnecessary Inquiries and Chargebacks:
- Keep track of all Charge Records.
- Issue Credits immediately after determining that a Credit is due.
- Disclose all terms and conditions of your sale/return/exchange/cancellation policies at the point of sale, on all Charge Records and customer receipts, and on your website.
- Contact your Merchant Services Provider to make sure the name that you provide in your Submission matches your business name.
- Submit Charges only after goods have been shipped or services have been provided.
- Advise Cardmembers when goods or services will be delivered or completed, and always advise the Cardmember of any delays.
- Obtain a Cardmember’s signature whenever completing a service or work order.
- Encourage Cardmembers at the point of sale to contact your business directly should there be any problems with their purchase. Include your telephone number or web address and an appropriate description of goods or services purchased in your Submission.
- Inform Cardmembers of your business name that will appear on their billing statement.
- Provide a cancellation number when applicable.
- Remind the Cardmember to retain any documents you have provided, along with shipping information when applicable.
Contents

12.1 Introduction
12.2 Auto Dealers
12.3 Business-to-Business (B2B)/ Wholesale Distribution
12.4 Charitable Donations
12.5 E-Commerce Businesses
12.6 Government/Utilities/Education
12.7 Insurance
12.8 Oil/Petroleum
12.9 Parking
12.10 Rental Establishments
12.11 Restaurants
12.12 Travel Industries
12.1 Introduction

This section states additional policies and procedures applicable to Merchants classified in specific industries. All other provisions and requirements of the Agreement apply to these Merchants as well. To the extent possible, the provisions of this Chapter 12, "Specific Industries" and the other provisions of the Merchant Operating Guide shall be interpreted to give each their full effect. However, if a conflict is deemed to exist between them, then the provisions of this Chapter 12, "Specific Industries" shall govern.

12.2 Auto Dealers

This section applies to Merchants classified in an 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 Cardmember setting forth the terms of the sale, including down payment price, and your cancellation policy.

- In addition to 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 which is disputed by the Cardmember, if such Disputed Charge cannot be resolved in your favour based upon unambiguous language contained in the written agreement/bill of sale.

- Should a Cardmember exercise his or her right to rescind the written agreement/bill of sale during any rescission period set forth in the Cardmember’s agreement with you or at law, you shall submit a Credit to your Merchant Services Provider promptly.

- If you are classified 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 Cardmember denies making or authorizing the Charge, American Express will have Chargeback rights for such Charge in addition to its 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 Cardmember 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 Cardmember, if such Disputed Charge cannot be resolved in your favour based upon unambiguous language contained in the written agreement/bill of sale.

Should a Cardmember exercise his or her right to rescind the written agreement/bill of sale during any rescission period set forth in the Cardmember’s agreement with you or at law, you shall submit a Credit to your Merchant Services Provider promptly.

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

12.3 Business-to-Business (B2B)/ Wholesale Distribution

If you are classified in the business-to-business (B2B) or wholesale distribution industries, and it is determined that you are not in the Telecommunications industry, then notwithstanding the prohibition in Section 3.3, "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 Cardmember whose prior methods of payment have been difficult to collect or uncollectable. An indicator of such difficulty, for example, may be the fact that you have sent an overdue customer account to collections.

For the purposes of Section 6.4, "Submission Requirements – Electronic", a Charge submitted by your Establishments classified in the foregoing industries will be deemed "incurred" on the date the Cardmember indicates to you that the Cardmember will pay for the goods or services purchased with the Card, so long as:

- this is a common practice in your industry, and
- does not constitute an attempt to obtain payment from the Cardmember when prior methods of payment have been difficult to collect or uncollectable.

Notwithstanding the restriction in Section 6.4, "Submission Requirements – Electronic", you must not submit any Charge until the goods have been shipped or services have been provided to the Cardmember. To the extent that you have clearly disclosed your intentions to the Cardmember and the Cardmember agrees, then you may submit the following types of Charges to your Merchant Services Provider before you ship the goods to the Cardmember:

- 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.
- Charges representing advance, partial, or full payment for goods that the Cardmember requests you to ship at a later date.
12.4 Charitable Donations

If you are a registered charity as defined under Subsection 248(1) of the Income Tax Act (ITA) and recognized by the Canada Revenue Agency as an Entity qualifying for tax exemption under paragraph 149(1)(f) of the ITA, then:

- You must provide your Merchant Services Provider, on request, documentation of such tax exempt status.
- You may accept the Card for charitable donations that:
  - are tax deductible to the payor as a charitable contribution under the ITA, or
  - include the receipt of an item or service of value (such as a meal or admission to an event or other incentive) where at least a portion of the amount is tax-deductible to the payor as a charitable contribution under the ITA.

12.5 E-Commerce Businesses

If you are operating a website or e-commerce business, you must include the following website information display requirements on your website:

- An accurate description of the goods/services offered, including the currency type for the Transaction. Transaction currency must be in Canadian Dollars.
- Your physical address in Canada.
- An email address and a telephone number for customer service disputes.
- Return/refund policy.
- A description of your delivery policy (e.g., No COD, No overnight).
- A description of your security practices (e.g., information highlighting security practices you use to secure Transactions on your systems, including Transactions conducted on the Internet).
- A statement of known export restrictions, tariffs, and any other regulations.

A privacy statement regarding the type of personal information collected and how the information is used. Additionally, you must provide to customers the option to decline being included in marketing campaigns or having their personal information included on lists sold to third parties.

12.6 Government/Utilities/Education

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 should feel free to use all forms of payment that you accept without being penalized for choosing a particular form of payment. To promote consumer 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. See Section 3.2, “Treatment of the American Express Brand”.

You must not impose a higher convenience fee, whether in the form of a flat fee or as a percentage of the final Transaction amount, on Charges than you impose on Other Payment
Products, except for electronic funds transfers, cash, and cheques. American Express views discrimination against Cardmembers as a breach of the Agreement.

If you are classified in the government, utilities, or education sectors, you may assess convenience fees on Charges, provided that they comply with the other requirements of this section.

You must clearly disclose the amount of convenience fees to the customer, which may include itemization on the customer receipt, invoice, or confirmation email, 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.

Your Merchant Services Provider can only assess a convenience fee when it accepts the Card for the foregoing Charges in compliance with the requirements of this section.

12.7 Insurance

This section contains provisions specific to Merchants classified in the insurance industry. 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 you issued. You must indemnify, defend, and hold harmless American Express and its Affiliates, successors, assigns, and Issuers, from and against all damages, liabilities, losses, costs, and expenses, including legal fees, to Cardmembers (or former Cardmembers) arising or alleged to have arisen from your termination or other action regarding their insurance coverage.

12.8 Oil/Petroleum

If you are classified in the oil and petroleum industry, your Merchant Services Provider may place you in the Fraud Full Recourse Program if you accept Charges originating at a CAT gas pump. For information about Customer Activated Terminals, see Section 4.4, “Customer Activated Terminals”.

12.8.1 Oil/Petroleum Requirements

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 your 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
12.8.2 Oil/Petroleum Recommendations

American Express has implemented several policies and fraud prevention tools to assist in combating fraud at the gasoline pump. Work with your Merchant Services Provider for additional information on these policies and to determine which fraud prevention tools are supported.

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.

12.9 Parking

This section contains provisions specific to Merchants classified in the parking industry. When the number of parking days is agreed upon when the Cardmember leaves the motor vehicle with you, or you provide a parking pass valid for a predetermined number of parking days, you must submit the Charge immediately. If the number of parking days is not known when the Cardmember leaves the motor vehicle with you, you must not submit the Charge until the last day of parking. See Section 4.6, "Charge Records" for additional information.

12.10 Rental Establishments

This section applies to Merchants classified in the Rental Establishments industries.

Customers should feel free to use all forms of payment that you accept without being penalized for choosing a particular form of payment. To promote consumer choice, Merchants 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. See Section 3.2, "Treatment of the American Express Brand". You must not impose a higher convenience fee, whether in the form of a flat fee or as a percentage of the final Transaction amount, on Charges than you impose on Other Payment Products, except for electronic funds transfers, cash, and cheques.

If you are classified as a Rental Establishment, you may assess convenience fees on Charges, provided that you comply with the other requirements of Chapter 4, "Transaction Processing" and this section, as follows:

- You must clearly disclose the amount of convenience fees to the customer, which may include itemization on the customer receipt, invoice, or confirmation email, 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.
Your Merchant Services Provider can only assess a convenience fee when it accepts the Card for Charges in compliance with the requirements of this section.

### 12.11 Restaurants

If you are classified in the restaurant or bar industry, then the following Authorization procedures apply where the final Charge amount is not known at the time of Authorization.

As of January 13, 2018, you must inform the Cardmember of any estimated amount for which Authorization will be requested and obtain the Cardmember’s consent to the estimated amount before initiating the Authorization Request.

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>The final restaurant or bar Charge is not greater than the Authorization obtained for the estimated Charge amount plus 20%</td>
<td>No additional Authorization is required.</td>
</tr>
<tr>
<td>The final restaurant or bar Charge amount is greater than the Authorization obtained for the estimated Charge amount by more than 20%</td>
<td>You must obtain an additional Authorization for the amount of the Charge that exceeds the amount for which you have already obtained Authorization. If (a) you fail to obtain Authorization for the additional amount, or (b) your request for such Authorization is declined, and the Cardmember fails to pay the Charge for any reason, American Express will have Chargeback rights for Authorization* for the portion of the final Charge amount in excess of the amount of the Authorization amount obtained plus 20%.</td>
</tr>
</tbody>
</table>

* American Express will maintain Chargeback rights for other reasons up to the amount of the entire submitted Charge.

When submitting the Charge, only include the initial Approval. See Section 4.6, “Charge Records” for additional information on paying a single bill with multiple Cards.

### 12.12 Travel Industries

Additional policies and procedures are applicable to Merchants classified in the lodging and vehicle rental industries. In addition, the Assured Reservations Program is available to Merchants in the lodging, trailer park/campground, vehicle, aircraft, bicycle, boat, equipment, motor home, and motorcycle rentals (see Subsection 12.12.3, “Assured Reservations”).

#### 12.12.1 Lodging

This section applies to Merchants classified in the lodging industry, and includes special Authorization procedures and programs for check-in and check-out. The Assured Reservations and CARDeposit® programs allow certain Charges to be submitted that would otherwise not be allowed by American Express.

Skimming is the theft of payment Card information by an employee of an Establishment who uses a pocket-sized electronic device (a.k.a. “skimmer”) to copy Cardmember information from the Card’s Magnetic Stripe. For Fraud Prevention tools, see Chapter 9, “Fraud Prevention”.

For example:

If the Authorization was for $100 and the total bar tab, which includes tax and tip, was no more than $120, no further Authorization is necessary. However, if the total bar tab was $150, and you did not obtain additional Authorization or your Authorization request is declined, then American Express has Chargeback rights up to $30.

American Express will maintain Chargeback rights for other reasons up to the amount of the entire submitted Charge.
12.12.1.1 Lodging — Special Authorization Procedures

When Cardmembers opt to pay for lodging stays on the Card, you must follow these procedures:

- **Upon check-in:**
  - Determine the estimated amounts of Charges based upon the room rates and the number of days that the Cardmember expects to stay, plus taxes and other known incidental amounts (Estimated Lodging Charges).
  - As of January 13, 2018, you must inform the Cardmember of the Estimated Lodging Charges for which Authorization will be requested and obtain the Cardmember’s consent to the estimated amount before initiating the Authorization Request.
  - Obtain Authorization for the full amount of the Estimated Lodging Charge.
  - Do not overestimate the Authorization amount.
  - An Authorization is valid for the duration of the lodging stay.

- **Upon check-out:**

  | If | Then |
  |-----------------------------------------------|
  | The final Charge amount charge is no greater than the total of the Estimated Lodging Charge plus 15% of the Estimated Lodging Charge | No further Authorization is required. |
  | The final Charge amount exceeds the Estimated Lodging Charge by more than 15% | You must obtain Authorization for any additional Charge amount that exceeds the Estimated Lodging Charge. If you a) fail to obtain such Authorization for the additional amount, or b) your request for such Authorization is Declined, and the Cardmember fails to pay the Charge for any reason, American Express may exercise its Chargeback rights for the portion of the final Charge amount in excess of the Approved Estimated Lodging Charge. |

We recommend that you perform an additional Authorization as soon as the Charge amount exceeds the original Authorization by 15%. For example: If the Cardmember extends the stay, before allowing the additional stay, obtain Authorization for the additional stay (plus incidentals) that exceeds the original Authorization for estimated amounts by 15%.

For example: If the Authorization was for $1,000 and the total of lodging Charges were no more than $1,150, no further Authorization is necessary. However, if the total lodging Charges were $1,200, and you did not obtain additional Authorization, then American Express would have Chargeback rights up to $50.
12.12.1.2 Assured Reservations — Lodging

Assured Reservations means a Cardmember’s accommodation is guaranteed by you to be held until the published check-out time on the date following the scheduled arrival date, as indicated by the Cardmember when making the Assured Reservation. You must honour Assured Reservations.

Lodging Merchants may submit "no show" charges, if they comply with the provisions of the Assured Reservations Program and the Cardmember does not use or cancel the reservation in accordance with program requirements.

Your Assured Reservations Program responsibilities include the following:

- When accepting an Assured Reservation, you must advise the Cardmember that, if the Cardmember does not claim the Assured Reservation, or cancel it within the time specified in your stated reservation policy, the Cardmember may be charged for one (1) night’s lodging plus applicable taxes. If the Cardmember does not claim the Assured Reservation or cancel in accordance with your stated reservation policy, you may bill the Cardmember for a "no show" Charge.

- If the Cardmember cancels an Assured Reservation, you must provide a cancellation number to the Cardmember and maintain a record of the cancellation number.

- Use the proper "no show" indicator, when submitting a "no show" Charge. If you are unsure of how to transmit using this code, contact your Merchant Services Provider.

If you do not honour the Assured Reservations Program requirements your obligation to the Cardmember is the following:

- Pay for one (1) night’s accommodation at a comparable property, located nearby.
- Pay for transportation to the alternate location.
- Pay for a three (3)-minute telephone call.
- Use good faith efforts to forward all communications to the Cardmember at the alternate location.

Failure to meet the previously-mentioned obligations may result in a Chargeback if the Cardmember disputes a "no show" Charge.

If American Express receives disproportionate numbers of Disputed "no show" Charges, you must work with your Merchant Services Provider to reduce the number of disputes. If such efforts fail to reduce the number of disputes, you may be placed in a Chargeback program.

12.12.1.3 CARDeposit Program

As a lodging Merchant, if you require room deposits, you must participate in the CARDeposit program. You must accept the Card for payment of CARDeposits. Your CARDeposit program responsibilities include the following:

- Follow all requirements for an Advance Payment Charge, as described in Section 4.12, "Advance Payment Charges".
- Upon arrival, the Cardmember must show the Card. If the Cardmember does not have the Card, other identification must be shown.
Ensure the Charge Record contains the words "CARDeposit" on the Cardmember signature line or, for Charge Records submitted electronically, the appropriate indicator on the Charge Data. If you are unsure of how to submit the Charge using the appropriate indicator, contact your Merchant Services Provider.

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>The CARDeposit is cancelled</td>
<td>You must send a written cancellation notice showing the cancellation number to the Cardmember within three (3) business days from the date of such cancellation. If a refund is due, pursuant to your advance deposit cancellation policy, you must include the appropriate indicator or submit a Credit form with the words &quot;CARDeposit Cancellation&quot; on the Cardmember signature line. If you are unsure of how to submit using the appropriate indicator, contact your Merchant Services Provider.</td>
</tr>
<tr>
<td>An arrival date of a CARDeposit is changed</td>
<td>You must send the Cardmember a written confirmation of the change within three (3) business days from the date the reservation was changed.</td>
</tr>
</tbody>
</table>
| You are unable to honour a CARDeposit that was not previously cancelled | Your obligation to the Cardmember includes the following:  
  - You must issue a Credit for the CARDeposit.  
  - You must pay for accommodations at a comparable location nearby, until the duration of the original reservation expires (up to fourteen (14) nights) or until accommodations become available at the original location, whichever occurs first.  
  - You must provide transportation to and from the alternate location once a day until the original accommodations are available.  
  - You must pay for one, three (3)-minute call to advise of the move to the alternate location, and one, three (3)-minute call to advise of the return to the original location. |

**12.12.1.4 Emergency Check-in**

If a Cardmember whose Card is lost or stolen requests check-in, you must call your Merchant Services Provider, request "Authorization for an Emergency Check-in," and follow the instructions.

**CARDeposit Program**

A program that permits Cardmembers to charge the payment of an Advance Payment Charge to their Cards when a deposit is required.
12.12.2 Vehicle Rentals

This section applies to Merchants classified in the vehicle rental industry. When Cardmembers opt to pay for vehicle rentals (not to exceed four (4) consecutive months) on the Card, you must comply with these procedures.

12.12.2.1 Vehicle Rentals — Special Authorization Procedures

Upon rental of the vehicle:

- Determine the estimated amount of the Charge (Estimated Vehicle Rental Charge). The Estimated Vehicle Rental Charge shall be determined by multiplying the rental rate by the rental period reserved by the Cardmember, plus any known incidentals. You must not overestimate this amount or include an amount for any possible damage to or theft of the vehicle.

- As of January 13, 2018, you must inform the Cardmember of the Estimated Vehicle Rental Charge for which Authorization will be requested and obtain the Cardmember’s consent to the estimated amount before initiating the Authorization Request.

- Obtain Authorization for the full amount of the Estimated Vehicle Charge.

- If you fail to obtain Authorization for the Estimated Vehicle Rental Charge and submit the Charge, and the Cardmember fails to pay the Charge for any reason, American Express will have Chargeback rights for the full amount of the Charge.

- An Authorization for Estimated Vehicle Rental Charges is valid for the duration of the rental agreement.

Upon return of the vehicle:

We recommend that you perform an additional Authorization as soon as the Charge amount exceeds the original Authorization by 15%. For example: If the Cardmember extends their rental period, before allowing the additional rental period, obtain Authorization for the additional rental cost (plus incidentals) that exceeds the original Authorization for estimated amounts by 15%.

For example: If the Authorization was for $1,000, and the final rental amount was no more than $1,150, no further Authorization is necessary. However, if the total final rental amount was $1,200, and you did not obtain additional Authorization, then American Express will have Chargeback rights up to $50.

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>The final Charge amount does not exceed the Estimated Vehicle Rental Charge plus 15%</td>
<td>No further Authorization is required.</td>
</tr>
<tr>
<td>The final Charge exceeds the Estimated Vehicle Rental Charge by more than 15%</td>
<td>You must obtain Authorization for any additional Charge amount that exceeds the Estimated Vehicle Rental Charge. If you a) do not obtain an Authorization for the additional amount, or b) request Authorization for the additional amount but Authorization is declined, and the Cardmember fails to pay the Charge for any reason, American Express will have Chargeback rights for the portion of the final Charge amount in excess of the Approved Estimated Vehicle Rental Charge plus 15%.</td>
</tr>
</tbody>
</table>
### If A Cardmember decides to extend a rental period

<table>
<thead>
<tr>
<th>Then</th>
<th>You must request Authorization for the estimated Charge amount that will be in excess of the Estimated Vehicle Rental Charge.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authorization approved – If Authorization is granted, the amount of the subsequent Authorization will be added to the original Estimated Vehicle Rental Charge and that total will be considered the Estimated Vehicle Rental Charge.</td>
</tr>
<tr>
<td></td>
<td>Authorization declined – If Authorization is declined, the original Estimated Vehicle Rental Charge amount will remain the Estimated Vehicle Rental Charge.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Then</th>
<th>You must request Authorization for the additional amount not previously approved for Authorization.</th>
</tr>
</thead>
</table>

### 12.12.2.2 Prepayment on Vehicle Rentals

If you permit Cardmembers to make Charges with the Card for vehicle rentals where Cardmembers elect to prepay for a vehicle rental over the phone, at the counter, and via your company websites (not on any other third-party reservation system) (Prepaid Rental), you must:

- Follow all requirements for an Advance Payment Charge, as described in Section 4.12, "Advance Payment Charges".
- Ensure that your vehicle rental contract with the Cardmember contains the terms and conditions of said reservation and cancellation policies.

### 12.12.2.3 Assured Reservations — Vehicle Rentals

Assured Reservations means a Cardmember’s reservation is guaranteed by you to be held until the vehicle return time, as indicated by the Cardmember when making the Assured Reservation. You must honour Assured Reservations.

Vehicle Rental Merchants may submit “no show” charges, if they comply with the provisions of the Assured Reservations Program and the Cardmember does not use or cancel the reservation in accordance with program requirements. See Subsection 12.12.3, "Assured Reservations" for details.

### 12.12.2.4 Capital Damages

If a Cardmember voluntarily opts to use the Card to pay for property damage to a rented vehicle (Capital Damages), you may accept the Card, provided you have complied with all of the following conditions for payments of such items:

- The Card was used for the vehicle rental at the time the vehicle was checked out.
- You must provide in writing, to the Cardmember, an itemized list of specific damages which have occurred.
You must secure from the Cardmember written acknowledgement of responsibility for the Capital Damages. The Cardmember’s acknowledgement must be made freely and without any threat or duress.

You must advise the Cardmember, in writing, of the total estimated amount for which the Cardmember may be responsible. No amounts in excess of 110% of the disclosed amount shall be charged to the Cardmember’s Card, without the express prior written consent of the Cardmember.

A description of the damage, acknowledgement of responsibility, and designation of the estimated amount of damage will be set forth on a single form (Acknowledgement of Responsibility Form). See Appendix A, "Acknowledgement of Responsibility" for a copy of the form.

You must obtain Authorization for the amount of the Capital Damages each time an Acknowledgement of Responsibility Form is completed.

On each occasion the Cardmember has chosen to use the Card for Capital Damages, you must prepare a Charge Record separate from the Charge Record for the rental. You must adhere to all requirements outlined in Chapter 4, "Transaction Processing" for the completion of the Charge Record. In addition, you must observe the following:

■ After the exact amount of the Capital Damages has been determined, you must provide the Cardmember with itemized notice of damages; insert the amount of the Capital Damages on the Charge Record (in no event in excess of the estimated amount plus 10% agreed to by the Cardmember in the Acknowledgement of Responsibility Form).

■ For Charge Records submitted on paper or by other non-electronic means, you must write “Capital Damages” on the signature line; for electronic Submission you must provide the indicator. For instructions on how to provide the indicator, contact your Merchant Services Provider.

■ In addition to the other Chargeback rights contained in the Agreement, American Express may exercise its Chargeback rights with respect to any Charge for Capital Damages that is not submitted in accordance with all the procedures outlined in Chapter 4, "Transaction Processing", Section 12.12.2, "Vehicle Rentals", and within the Agreement.
12.12.3 Assured Reservations

Assured Reservations means:

- For accommodation reservations (including hotel and trailer park/campground): a Cardmember’s accommodation is guaranteed by you to be held until the published check-out time on the date following the scheduled arrival date, as indicated by the Cardmember when making the Assured Reservation.

- For vehicle, aircraft, bicycle, boat, equipment, motor home, and motorcycle rentals: a Cardmember’s reservation is guaranteed by you to be held until the return time, as indicated by the Cardmember when making the Assured Reservation.

You must honour Assured Reservations. You may submit “no show” Charges, if you comply with the provisions of the Assured Reservations Program and the Cardmember does not use or cancel the reservation in accordance with program requirements.

Your Assured Reservations Program responsibilities include the following:

- When accepting an Assured Reservation, you must advise the Cardmember that, if the Cardmember does not claim the Assured Reservation, or cancel it within the time specified in your stated reservation policy, you may bill the Cardmember for a “no show” Charge as follows:
  - For accommodation reservations (including hotel and trailer park/campground): one (1) night’s accommodation plus applicable taxes.
  - For vehicle, aircraft, bicycle, boat, equipment, motor home, and motorcycle rentals: one (1) day’s rental or the daily/hourly incremental equivalent of the rental rate agreed upon in the rental agreement, plus applicable taxes.

- If the Cardmember cancels an Assured Reservation, you must provide a cancellation number to the Cardmember and maintain a record of the cancellation number.

- Use the proper “no show” indicator, when submitting a “no show” Charge. If you are unsure of how to transmit using this code, contact your Merchant Services Provider.

If you do not honour the Assured Reservation Program requirements, you must provide comparable accommodations, and/or services, when reasonably available, at no additional cost to the Cardmember, in accordance with the rental agreement. Merchants classified in the Lodging industry are also subject to the requirements set forth in Subsection 12.12.1.2, “Assured Reservations — Lodging”.

Failure to satisfy the previously-mentioned obligations may result in a Chargeback if the Cardmember disputes a “no show” Charge.

If a disproportionate numbers of Disputed “no show” Charges are received, you must work to reduce the number of disputes. If such efforts fail to reduce the number of disputes, you may be placed in a Chargeback program.
13.1 Arbitration Agreement (as to Claims involving American Express)
13.1 Arbitration Agreement (as to Claims involving American Express)

In the event that a Merchant or its Merchant Services Provider is not able to resolve a Claim against American Express, or a claim against Merchant Services Provider or any other entity that American Express has a right to join, this section explains how Claims may be resolved through arbitration. Merchant or American Express may elect to resolve any Claim by binding individual arbitration. Claims will be decided by a neutral arbitrator.

(a) Asserting a Claim. The parties agree to use commercially reasonable efforts to settle any Claim within 30 days following the time that a Claim is raised or shorter time period as either party may determine. All Claims will be resolved exclusively by arbitration pursuant to this Section, except as otherwise provided for herein. Solely in this section, Claim means any claim (including initial claims, counterclaims, cross-claims, and third party claims), dispute, or controversy between Merchant and Amex Bank of Canada whether based in contract, tort (including negligence, strict liability, fraud, or otherwise), or statutes, regulations, or any other theory, arising from or relating to this Agreement, or the relationship resulting from this Agreement, including the validity or enforceability or scope of this Arbitration provision. Claim also includes any claim, dispute, or controversy that may arise from or relates to the ordinary business practices of Merchant Services Provider or American Express, policies and procedures including Merchant Services Provider’s rights to Chargeback, create reserves, and debit Merchant’s Bank Account.

(b) Arbitration. A Claim that is not resolved directly between the parties will be resolved pursuant to this Section and the National Arbitration Rules (Rules) of ADR Institute of Canada, Inc. (Administrator) or its successors or replacement Administrator. For a copy of the Rules, to file a Claim, or for other information about the Administrator contact: ADR Institute, 234 Eglinton Avenue East, Suite 405, Toronto, Ontario M4P 1K5; email admin@adrcanada.ca. Prior to the initiation of any Claim, Amex Bank of Canada has the right to change or replace the Administrator or the Rules in its sole discretion.

(c) Small Claims Court Proceedings and Complaint Procedures. Notwithstanding anything to the contrary in this Section, Merchant may pursue any Claim without resort to arbitration in a small claims court of the province or territory of Merchant’s main business office in Canada, so long as the Claim is individual, within the jurisdiction of, and pending only in that court. Merchant may also access our complaint escalation procedures set forth in the Agreement between Merchant Services Provider and Merchant.

(d) Consolidation. The parties agree that individual arbitration provides a more efficient and cost effective method of resolving Claims than court litigation. All Claims will be arbitrated on an individual basis. Claims brought by Merchant against Amex Bank of Canada or by Amex Bank of Canada against Merchant may be joined, heard one after the other, or consolidated as the arbitrator may direct in arbitration with Claims brought by or against someone other than Merchant, if agreed to in writing by all parties. The parties further agree that the arbitrator will have no jurisdiction or authority to consider any Claim brought on a class action or representative party basis.
(e) **Arbitration Procedures and Appeal.** The arbitrator will take reasonable steps to preserve the privacy of individuals and of business matters and the Confidentiality provisions of the Rules. Where the Claim being arbitrated is for an amount less than $50,000, there will be no oral discoveries or oral hearing subject to the discretion of the arbitrator to direct otherwise. The arbitrator's decision will be final and binding. However, where an appeal is not prohibited by statute, any party can appeal the award to an appeal panel administered by the Administrator, which will consider anew any aspect of the initial award objected to by the appealing party. Where the award under appeal is for $50,000 or less, the appeal will be to a single appeal arbitrator and where the award under appeal is for more than $50,000, the appeal will be to a three-member appeal panel. The appealing party will have 30 days from the date of entry of the written arbitration award to notify the Administrator that it is exercising the right of appeal. The Administrator will then notify the other party that the award has been appealed. The Administrator will appoint the appeal panel that will conduct arbitration pursuant to the Rules and issue its decision within 120 days of the date of the appealing party's written notice. The decision of the three-member appeal panel will be by majority vote. The appeal decision will be final and binding and there will be no further appeal. The appeal decision will be considered as a final award.

(f) **Location of Arbitrations/Payment of Fees.** Any arbitration hearing that Merchant attends will take place in the province or territory of Merchant’s main business office in Canada. If Merchant does not have a business office in Canada, then the arbitration hearing will take place in Toronto, Ontario. The arbitrator and, where applicable, the appeal panel shall be entitled to fix the costs and expenses of the arbitration, including reasonable legal fees, the costs and expenses of the arbitration and appeal, and the fees of the arbitrator, appeal panel, and Administrator.

(g) **Definition.** For purposes of this Section 13.1, "Arbitration Agreement (as to Claims involving American Express)", (i) Amex Bank of Canada includes any of Amex Bank of Canada’s Affiliates, licensees, predecessors, successors, or assigns, any purchasers of any receivables, and all agents, directors, and representatives of any of the foregoing, (ii) Merchant includes any of Merchant’s Affiliates, licensees, predecessors, successors, or assigns, any purchasers of any receivables and all agents, directors, and representatives of any of the foregoing; and Claim shall have the meaning set out herein.

(h) **Continuation.** This Section 13.1, "Arbitration Agreement (as to Claims involving American Express)" will survive termination of the Merchant Agreement, any legal proceeding to collect a debt, any bankruptcy and any sale of Merchant, or their respective assets (in the case of a sale, its terms will apply to the buyer). If any portion of this Section 13.1, "Arbitration Agreement (as to Claims involving American Express)" or of the Merchant Agreement is deemed invalid or unenforceable, it will not invalidate the remaining portions of this Section 13.1, "Arbitration Agreement (as to Claims involving American Express)", or the Merchant Agreement or any predecessor agreement, each of which shall be enforceable regardless of such invalidity.
Appendix A
Acknowledgement of Responsibility
Acknowledgement of Responsibility

**Name**

**Address**

**City, Province, Postal Code**

**Account Number**

**Renter**

Name of Renter:

Address:

City, Province, Postal Code:

Drivers License Number: Province:

**Identification of Vehicle**

Type of Vehicle: Year:

Model:

License Number: Province:

Registration Number:

Rental Agreement Number:

**Description of Damage**

Estimated Amount: Estimated Total:

By signing this form, the undersigned accepts full responsibility for the damage as set forth above, and agrees that the actual damage amount up to the estimated total amount set forth above, plus 10% thereof, may be charged to the undersigned's American Express Card account.

Authorization: Signature: Date:
**Advance Payment Charge** means a Charge for which full payment is made in advance of Merchant providing the goods and/or rendering the services to the Cardmember.

**Affiliate** means any Entity that controls, is controlled by, or is under common control with either party, including its subsidiaries. As used in this definition, "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an Entity, whether through ownership of voting securities, by contract, or otherwise. For the avoidance of doubt, but not by way of limitation, the direct or indirect ownership of more than 50% of (i) the voting securities or (ii) an interest in the assets, profits, or earnings of an Entity shall be deemed to constitute "control" of the Entity.

**Agency** means any Entity or line of business that uses Merchant’s Marks or holds itself out to the public as a member of Merchant’s group of companies.

**Aggregated Charge** means a Charge that combines multiple small purchases or refunds (or both) incurred on a Card into a single, larger Charge before submitting the Charge for payment.

**Agreement** means the merchant processing agreement or sponsored merchant agreement, the American Express Merchant Operating Guide, and any accompanying schedules and exhibits, collectively, between Merchant and its Merchant Services Provider.

**American Express** means Amex Bank of Canada.

**American Express Brand** means the American Express name, trademarks, service marks, logos, and other proprietary designs and designations and the imagery owned by American Express or an American Express Affiliate and the goodwill associated with all of the foregoing and with all the goods and services now and in the future provided, marketed, offered, or promoted by American Express or an American Express Affiliate.

**American Express Card** or **Cards** means (i) any card, account access device, or payment device or service bearing an American Express or an American Express Affiliate’s Marks and issued by an Issuer or (ii) a Card Number. Card also includes any card or other account access device or service issued by a Third Party Issuer and bearing such Third Party Issuer’s name or Marks but not the Marks of American Express, such as Japanese Credit Bureau (JCB) cards.

**American Express Network** or **Network** means the Network of Merchants that accept Cards and the operational, service delivery, systems, and marketing infrastructure that supports this Network and the American Express Brand.

**Applicable Law** means (i) any law, statute, regulation, ordinance, or subordinate legislation in force from time to time to which either party or its Affiliates are subject; (ii) the common law as applicable to them from time to time; (iii) any court order, judgement, or decree that is binding on a party or its Affiliates; (iv) any directive, policy, rule, guidance, standards, or order that is binding on them and that is made or given by a regulator, or other government or government agency department or other administrative body, commission, or bureau, or other body exercising adjudicative, Regulatory, judicial or quasi judicial powers, of any Territory, or other national, federal, commonwealth, state, provincial, or local jurisdiction; and (v) any codes of conduct or public commitments to which a party subscribes, whether such party is legally required to comply with orders so voluntarily acting reasonably, including the Code of Conduct.
Application-initiated Transaction is a Transaction initiated by an electronic device (including but not limited to, a mobile telephone, tablet, or wearable device) utilizing a merchant software application within the electronic device.

Approval/Approved means a message granting an Authorization in response to a request for Authorization from a Merchant, consisting of an Approval or other indicator.

Assured Reservation Program means a program that allows Cardmembers to contact a participating property or rental agency to make an Assured Reservation and guarantee the hotel reservation by giving their American Express Card. The Assured Reservation Program is available to the following industries: hotel, trailer park/campground, vehicle, aircraft, bicycle, boat, equipment, motor home, and motorcycle rentals.

Attestation of Compliance (AOC) means the declaration of the status of your compliance with the PCI DSS, in the form provided by the Payment Card Industry Security Standards Council, LLC.

Attestation of Scan Compliance (AOSC) means the declaration of the status of your compliance with the PCI DSS based on a network scan, in the form provided by the Payment Card Industry Security Standards Council, LLC.

Authorization/Authorized means the process by which a Merchant obtains an Approval for a Charge in accordance with the Agreement.

Bank Account means an account that Merchant holds at a bank or other financial institution.

Batch means a group of Transactions, submitted to your Merchant Services Provider, usually on a daily basis.

Card – See American Express Card or Cards.

Card Data includes the following elements: Cardmember name, Card Number, Expiration Date, Charge date, the amount of the Charge, the Approval, description of goods and services, Merchant name, Merchant address, Merchant Number and if applicable the Establishment number, Cardmember signature (for In-Person Transactions only), 'No Refund' if you have a no refund policy, and all other information as required from time to time by your Merchant Services Provider, American Express, or Applicable Law.

Card Identification (CID) Number means a four-digit number printed on the Card. See Section 5.7, "Card Identification (CID) Number" for additional information.

Card Not Present Charge means a Charge for which the Card is not presented at the point of sale (e.g., Charges by mail, telephone, fax or the internet).

Card Number means the unique identifying number that the Issuer assigns to the Card when it is issued.

Card Present Charge means a Charge for which the physical Card and Cardmember are present at the point of sale, including In-Person Charges and Charges made at CATs.

CARDeposit Program means a program that permits Cardmembers to charge the payment of an Advance Payment Charge to their Cards when a deposit is required. See Subsection 12.12.1.3, "CARDeposit Program" for additional information.
Cardmember (also referred to as Card Member) means an individual or Entity (i) that has entered into an agreement establishing a Card account with an Issuer or (ii) whose name appears on the Card.

Cardmember Information means any information about Cardmembers and Transactions, including, but not limited to, Transaction Data, and Cardmember name, addresses, Card Numbers, and CID Numbers.

Charge means a payment or purchase made on the Card.

Charge Data means Data to be included in Submissions of Charge Records.

Charge Record means a reproducible (both paper and electronic) record of a Charge that complies with American Express’ requirements and contains the Card Number, Transaction date, dollar amount, Approval, Cardmember signature (if applicable), and other information.

Chargeback when used as a verb, means (i) your Merchant Services Provider’s reimbursement from you for the amount of a Charge subject to such right, or (ii) your Merchant Services Provider’s reversal of a Charge for which it has not paid you; when used as a noun, means the amount of a Charge subject to reimbursement from you or reversal.

Chip means an integrated microchip embedded on a Card containing Cardmember and account information.

Chip Card means a Card that contains a Chip and could require a PIN as a means of verifying the identity of the Cardmember or account information contained in the Chip, or both, (sometimes called a "smart Card", an "EMV Card", or an "ICC" or "integrated circuit Card" in American Express’ materials).

Chip Card Data means the information contained in the Chip on a Chip Card that is used to process Transactions.

Code 10 “Code 10” is a phrase that a Merchant communicates to its Merchant Services Provider to alert of a possible suspicious Card and/or Transaction. Code 10 situations usually occur during Authorization.

Collusion means any Transaction, activity or agreement conducted by a Merchant or its agent with another party, including another Merchant or a Cardmember, which the Merchant knew or should have known was not legitimate, or carried out in violation of Chapter 10, “Risk Management”.

Consumer Device Cardholder Verification Method (CDCVM) means an Issuer approved, American Express recognized Cardholder Verification Method whereby the Cardmember’s credentials are verified on a Mobile Device.

Contactless means technology enabling a Card or Mobile Device embedded with a radio frequency component (currently, Expresspay) to communicate with a radio frequency-enabled POS device to initiate a Transaction. See also Expresspay.

Covered Parties means any or all of your employees, agents, representatives, subcontractors, Processors, service providers, providers of your POS Systems or payment processing solutions, and any other party to whom you may provide Cardmember Information access in accordance with the Agreement.

Credit means the amount of the Charge that Merchant refunds to Cardmembers for purchases or payments made on the Card.
Credit Record means a record of Credit that complies with American Express’ requirements.

Customer Activated Terminal (CAT) means an unattended POS System (e.g., gasoline pump, vending machine, check-out kiosk).

Data Security Requirements (DSR) means the American Express data security policy for Merchants, as described in Chapter 8, “Protecting Cardmember Information” of the Merchant Operating Guide and is also made available to Merchants at www.americanexpress.ca/dsr.

Decline means a message denying the Merchant’s request for Authorization.

Delayed Delivery Charge means a single purchase for which Merchant must create and submit two separate Charge Records. The first Charge Record is for the deposit or down payment and the second Charge Record is for the balance of the purchase.

Digital Wallet Application-initiated Transaction means an Application-initiated Transaction that is initiated by a digital wallet within a Mobile Device.

Digital Wallet Contactless-initiated Transaction means a contactless Transaction initiated by a digital wallet within a Mobile Device via the contactless interface.

Digital Wallet Magnetic Secure Transmission Transaction means a type of Digital Wallet Payment where a Transaction is initiated by a digital wallet within a Mobile Device via the magnetic stripe reader within a POS system.

Digital Wallet Payment means a Digital Wallet Contactless-initiated Transaction, Digital Wallet Application-initiated Transaction, and/or Digital Wallet Magnetic Secure Transmission (MST) Transaction conducted via a digital wallet, operated by an American Express approved third party wallet provider that resides on a Mobile Device.

Disputed Charge means a Charge about which a claim, complaint, or question has been brought.

Entity means a corporation, partnership, sole proprietorship, trust, association, or any other legally recognized entity or organization.

Establishments means any or all of your and your Affiliates’ locations, outlets, websites, online networks, and all other methods for selling goods and services, including methods that you adopt in the future.

Estimated Lodging Charge means the estimated amount of Charges based on the room rates and the number of days the Cardmember expects to stay, plus taxes and other known incidental amounts.

Estimated Vehicle Rental Charge means the rental rate multiplied by the rental period reserved by the Cardmember, plus taxes and any known incidental amounts.

Expiration Date means the month and year on which a Card expires (sometimes referred to as “valid thru” or “active thru” date).

Expresspay is an American Express program that enables Contactless transactions.

Floor Limit means a monetary threshold for a single Charge, at or above which Merchant must obtain an Authorization before completing the Charge.

Fraud Full Recourse Program means one of American Express’ Chargeback programs.
**High Risk Merchant** means a Merchant designation indicating that certain fraud Transactions conducted at the Merchant may be issued as a Chargeback to the Merchant under American Express' Fraud Full Recourse Program.

**Immediate Chargeback Program** means one of American Express' Chargeback programs.

**In-Person Charge** means a Card Present Charge excluding Charges made at CATs (e.g., a Charge taken at a Merchant attended retail location where the Card is swiped, read by a contactless reader, inserted into a Chip Card reader, or manually key-entered).

**Inquiry** means a request for information about a Disputed Charge.

**Internet Electronic Delivery** means the delivery of goods or services purchased on the internet via an internet download or another file transfer process (e.g., images or software download).

**Internet Order** means Card payment information that is taken via the World Wide Web, online (usually via a website payment page), email, intranet, extranet, or other similar network in payment for merchandise or services.

**Issuer** means any Entity (including American Express and its Affiliates) licensed by American Express or an American Express Affiliate to issue Cards and to engage in the Card issuing business.

**Keyed No Imprint Program** means a program that allows a Merchant to submit In-Person Charges without an imprint of the Card. See Section 4.15, "Keyed No Imprint Program" for additional information.

**Magnetic Stripe** means a stripe on the back of a Card that contains Cardmember and account information in machine readable form.

**Marks** are names, logos, service marks, trademarks, trade names, taglines, or other proprietary designs or designations.

**Merchant** means any seller of goods or services, non-profit, or government Entity that enters into an agreement with a Merchant Services Provider wherein the seller agrees to (i) permit any Cardmember to charge purchases of goods and services at or with such Merchant by means of the Card and (ii) transfer Transactions to American Express through Merchant Services Provider. Sponsored Merchants shall be included within the meaning of Merchants.

**Merchant Account** means an account established by Merchant Services Provider upon entering into an Agreement with a Merchant.

**Merchant Category Code** means the four (4) digit code used to identify the industry in which the Merchant is doing business.

**Merchant Number** means the unique merchant identification number (or MID) provided by Merchant Services Provider to Merchant for submitting transactions.

Merchant Services Provider means an Entity authorized under the American Express OptBlue® Program to accept Charges from a Merchant pursuant to an Agreement or a Payment Aggregator authorized to accept Charges from a Merchant. These services may include, but are not limited to, processing transactions, facilitating authorizations on purchases, and capturing data, merchant accounting, backroom operations (e.g., chargebacks and detecting fraud), provision of point of sale equipment, solutions, or systems, sales, or customer service.

Mobile Device means an Issuer approved and American Express recognized electronic device (including, but not limited to, a mobile telephone, tablet, or wearable device) that is enabled to initiate a Digital Wallet Payment Transaction.

Mobile Point of Sale (MPOS) means a handheld device used with a Card reading peripheral to accept Transactions using a cellular or Wi-Fi network.

Network – See American Express Network or Network.

No Signature/No PIN Program means a program that allows an Establishment to not request a signature or PIN from Cardmembers. See Section 4.16, “No Signature/No PIN Program” for additional information.

Notification Date means the date that American Express provides issuers with final notification of a Data Incident. Such date is contingent upon American Express’ receipt of the final forensic report or internal analysis and shall be determined in American Express’ sole discretion.

Other Payment Products means any charge, credit, debit, stored value, prepaid, or smart cards, account access devices, or other payment cards, services, or products other than the Card.

Partial Immediate Chargeback Program means one of American Express’ Chargeback programs.

Payment Aggregator means a provider of Payment Services (formerly referred to as “Payment Service Provider” or “PSP” and sometimes called an “aggregator” or “master merchant”).

Payment Card Industry Data Security Standard (PCI DSS) is the Payment Card Industry Data Security Standard, which is available at www.pcisecuritystandards.org.

Payment Services means the provision of payment services in connection with Transactions between Cardmembers and Sponsored Merchants whereby the Entity providing such services (and not the Sponsored Merchant), is the Merchant of record, submits Transactions under its Merchant Number and receives payment from us for Charges (among other things).

Personal Identification Number (PIN) mean a secret code for use with one or more American Express Network, Acquirer, or Issuer systems that is used to authenticate the user (e.g., a Cardmember) to that system.

Point of Sale (POS) System means an information processing system or equipment, including a terminal, personal computer, electronic cash register, contactless reader, Mobile Point of Sale (MPOS), or payment engine or process, used by a Merchant, to obtain Authorizations or to collect Transaction Data, or both.
**Prepaid Card** means a Card that is marked “Prepaid” or bearing such other identifiers used by American Express from time to time.

**Proof of Delivery** means a receipt which proves that the goods were delivered to the complete and valid shipping address provided by the Cardmember when the purchase was made.

**Recurring Billing** means an option offered to Cardmembers to make recurring Charges automatically on their Card (e.g., membership fees to health clubs, magazine subscriptions, and insurance premiums).

**Referral** means the message relayed during an Authorization request to Merchant through Merchant's POS System (e.g., "please call" or "refer to Issuer") requiring Merchant to telephone their Merchant Services Provider's Authorization Department for Approval.

**Rental Establishments** mean Long-term rentals used as primary residences.

**Reloadable Prepaid** means a Prepaid Card whereby once funds are depleted, it can be reloaded by adding funds to the Card.

**Rights-holder** means a natural or legal person or Entity having the legal standing and authority to assert a copyright or trademark right.

**Settlement** means the process by which your Merchant Services Provider compiles your debits and credits to calculate a net amount that will be applied to your Bank Account.

**Split Tender** means the use of multiple forms of payment (e.g., prepaid products, cash, American Express Card) for a single purchase.

**Submission** means the collection of Transaction Data sent to American Express.

**System Outage** is the interruption of either Merchant or Network systems or services (e.g., computer system failure, telecommunications failure, or regularly scheduled downtime).

**Technical Specifications** are the set of mandatory, conditional, and optional requirements related to connectivity to the Network and electronic Transaction processing, including Authorization and Submission of Transactions (sometimes called "specifications" in American Express’ materials), which American Express may update from time to time.

**Telecommunications** are communication services, including personal communication services; cellular, paging, long distance, etc. See Section 12.15, "Reserved" for additional information.

**Token** means a surrogate value that replaces the Card Number.

**Transaction** means a Charge or Credit completed by the means of a Card.

**Transaction Data** means all information required by American Express, evidencing one or more Transactions, including information obtained at the point of sale, information obtained or generated during Authorization and Submission, and any Chargeback.

**Transmission** is a method of sending Transaction Data to American Express whereby Transaction Data is transmitted electronically over communication lines.

**Transmission Data** is the same as Card Data except for the requirements to include: Cardmember name, Expiration Date, the Cardmember’s signature; and the words “No Refund” if the Merchant has a no refund policy.

**URL** means Uniform Resource Locator, a term used to identify an internet address.
Valid Dates are the dates on the Card that indicate the first and last date the Card can be used to make purchases.

Validation Documentation means the Attestation of Compliance rendered in connection with an Annual Onsite Security Assessment or SAQ, the AOSC and executive summaries of findings rendered in connection with Quarterly Network Scans, or the annual STEP Attestation. See Section 8.6, "Periodic Validation of Merchant Systems" for a list of documents and the policy’s requirements.

Voice Authorization means the Authorization of a Charge obtained by calling the Authorization Department of your Merchant Services Provider.

We, our and us means Amex Bank of Canada.

You and your means the individual or Entity accepting the Card under an Agreement with a Merchant Services Provider and (as applicable) its Affiliates conducting business in the same industry (sometimes called the "Merchant" or "Establishment" in this Merchant Operating Guide).