AMERICAN EXPRESS

Merchant Operating Guide

Australia

April 2024

For changes in this edition please see the Summary of Changes Table

This guide is intended for use by Merchants that have entered into a legally binding Agreement with a Merchant Services Provider based in Australia to accept the American Express® Card.

DON'T *do business* WITHOUT IT℠

AMERICAN EXPRESS

AMERICAN EXPRESS

Summary of Changes

Change Bars

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

Chapter	Section/Subsection	Description of Change
Chapter 1, "Introduction"	Subsection 1.4.2, "Unscheduled Changes"	Updated release information and website.
Chapter 4, "Transaction Processing"	Subsection 4.2.2, "Unattended Terminals"	Modified references from Customer Activated Terminals to Unattended Terminals and added requirements.
	Subsection 4.2.3.4, "Merchant-Presented Quick Response (MPQR)"	Added Merchant-Presented Quick Response procedures.
	Subsection 4.4.1, "Advance Payment"	Clarified verbiage and use.
	Subsection 4.4.2, "Aggregated – Internet"	Clarified verbiage and use.
	Subsection 4.4.3, "Delayed Delivery"	Clarified verbiage and use.
	Subsection 4.4.6, "Recurring Billing"	Updated reference from 4.4.11 "Split Shipment" to 4.4.6 "Merchant-Initiated Transactions" and updated Recurring Billing requirements.
Glossary of Terms		Added/modified definitions.

AMERICAN EXPRESS

Table of Contents

AMERICAN EXPRESS

List of Tables

AMERICAN EXPRESS

Introduction

1

1.1 About American Express

American Express was established more than 160 years ago and has undergone remarkable changes over the years. One characteristic has remained constant, however: our commitment to the core values of our founders. 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 our 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 a vast number of Transactions daily, forging relationships between Cardmembers and Merchants. We help build the businesses of millions of Merchants, from neighbourhood shops to multinational corporations.

1.2 About the Merchant Operating Guide

We are pleased to provide the *American Express Merchant Operating Guide*. It offers best practices, helpful tips, and available tools to assist your businesses. You can be more successful if you have access to and understand Card acceptance policies and procedures.

To serve all Merchants consistently, we require them to operate under the *Merchant Operating Guide*.

This *Merchant Operating Guide* sets forth the policies and procedures governing your acceptance of the American Express® Card. 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*.

1.2.1 Intended Audience for this Guide

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

- are physically located and maintain a bank account at a financial institution in Australia;
- have an estimated annual American Express Charge volume that meets the program requirements as communicated to you by your Merchant Services Provider; and,
- transact in Australian currency (AUD) only and receive payment from its Merchant Services Provider into a local bank account.

1.3 Organisation of the Merchant Operating Guide

Information boxes like this one are displayed throughout the *Merchant Operating Guide* to highlight important information such as definitions, fraud alerts, helpful tips, and further information.

The *American Express Merchant Operating Guide* is designed to meet the needs of busy Merchants. The content is organised into:

- global policies that apply to your Establishment, and
- country-specific policies that apply to your Establishments located in the specific country listed.

You should read the global policies together with any country-specific policies that follow. The two sections are organised one after the other, making it easier to read and find the information you need.

In the event of any conflict between the global policies and country-specific policies, the requirements of the country-specific policies take precedence. In the event of any conflict between the Agreement and Applicable Law, the requirements of law govern.

The *Merchant Operating Guide* follows the flow of the Transaction process—from Card acceptance, to Authorisation, to Submission, to Settlement, to Disputed Charges, to Chargebacks. To make it easier for you to locate the information you need quickly, the *Merchant Operating Guide* was designed with the following functionality:

- Important information is identified throughout the *Merchant Operating Guide* using the information boxes to the left of the main text.
- Point-and-click links to and from chapters are identified by blue underlined text when viewing the *Merchant Operating Guide* online.
- A table of contents and comprehensive glossary are provided in the *Merchant Operating Guide*.
- Capitalised terms used in the *Merchant Operating Guide* have the meanings ascribed to them in the Glossary of Terms. In addition, certain specialised terms also appear and are defined in the chapter or section in which they are used.
- All amounts referenced herein are stated in Australian Dollars.

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 as set forth in Subsection 1.4.1, "Scheduled Changes" and Subsection 1.4.2, "Unscheduled Changes" below. You agree to accept all such changes (and further to abide by the changed provisions of the *Merchant Operating Guide*) except where Applicable Law takes precedence. You may obtain the latest version of the *Merchant Operating Guide* by visiting www.americanexpress.com.au/merchantopguide, or by contacting your Merchant Services Provider.

1.4.1 Scheduled Changes

The *Merchant Operating Guide* is published twice each year, in April and October. We may change the provisions of the *Merchant Operating Guide* in scheduled changes as follows:

- a release of scheduled changes, to be published every April, with changes that shall take effect in the following October or on such other date as we set forth in the *Merchant Operating Guide*, and
- a release of scheduled changes, to be published every October, with changes that take effect in the following April or on such other date as we set forth in the *Merchant Operating Guide*.

Where a scheduled change is to take effect during the period between two editions of the *Merchant Operating Guide*, we will also include the change in the edition of the *Merchant Operating Guide* covering the period during which the change shall take effect, noting the effective date of the change.

1.4.2 Unscheduled Changes

American Express may also change the provisions of the *Merchant Operating Guide* in separate unscheduled releases at any time, which shall take effect ten (10) days after the release is posted to www.americanexpress.com.au/merchantopguide unless another effective date is specified in the notice.

AMERICAN EXPRESS

Doing Business with American Express

2

2.1 Introduction

At American Express, we feel privileged to do business with Merchants like you and want to help make the process of accepting Cards as simple as possible. The *Merchant Operating Guide* explains the policies and procedures related to accepting American Express Cards. It also highlights some of the services and tools that can help your business. This chapter outlines some general concepts that relate to doing business with American Express.

2.2 Benefits of Accepting the American Express Card

The decision you have made to accept the American Express Card demonstrates a commitment to the millions of Cardmembers who carry the Card. Accepting the Card allows you to:

- offer your customers the convenience of paying with American Express Cards, and
- improve retention by allowing customers with recurring Charges to pay automatically.

2.3 Merchant Information

Incorrect information may result in servicing issues. For example, if your business name changes and American Express is not notified, your customers may not recognise the Charge on their statements. This could result in Disputed Charges. Please contact your Merchant Services Provider if your business information changes.

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 autodialed 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. In addition, you may continue to receive marketing communications from American Express while American Express updates its records to reflect your opt-out choice.

American Express may include your Marks, details and those of your Establishments in guides, directories, lists, and other marketing materials in connection with your acceptance of the Card. American Express may also have our Affiliates and selected third parties do this on our behalf or for their own benefit. If you do not agree, you must notify your Merchant Services Provider in writing.

2.4 Compliance with the Technical Specifications

A vast number of Transactions traverse, and are processed by, the American Express Network. Merchants, processors, Terminal Providers, and others must conform to the *American Express Technical Specifications* in order to connect to and transact on the Network.

Each Authorisation request and Transaction, including data contained therein, must comply with the *American Express Technical Specifications*, any other (or different) requirements of our local operating centres and Applicable Law. We reserve the right to modify the *American Express Technical Specifications* or requirements of our local operating centres.

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.

2.4.1 Merchant Category Codes

If you are unsure of the MCC assigned to you, please contact your Merchant Services Provider. We also recommend that you review your Authorisation and Submission data periodically to ensure it accurately represents your industry classification. If it is not accurate, please contact your Merchant Services Provider.

You must use the Merchant Category Code (MCC) that most closely represents your business and industry classification. You must use the most accurate MCCs in all Authorisations and Submissions. If you have multiple, clearly distinct businesses that may qualify for more than one MCC, 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 primary business.

If the MCC used in the Submission does not match the MCC of the corresponding Authorisation, you agree to remediate the mismatch as soon as possible, at your own expense and in accordance with any instructions you may receive from us or your Merchant Services Provider. Failure to comply with MCC data requirements may result in the assessment of non-compliance fees. Please work with your Merchant Services Provider if you have questions related to your MCC assignment.

We reserve the right to require corrections to the MCC assignments if we determine, in our sole discretion, an incorrect MCC was assigned.

2.4.2 Compliance with Payment Product Terms and Conditions

We offer various payment processing solutions and products. If you choose to utilise one or more such products, you and your Merchant Services Provider must comply with the corresponding terms and conditions, which we may update from time to time, and which are available at www.americanexpress.com/merchantspecs. In the event of any conflict between the terms and conditions of the payment processing product and the Merchant Operating Guide, the terms and conditions of the payment processing product will prevail. All products and services may not be available to all Merchants.

2.5 Establishment Closing

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

- Notify your Merchant Services Provider and follow their guidelines for notification of Establishment closing.
- Your 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.
- If you are 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 your websites and catalogues).
- Your 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.

2.6 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 organisations, 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 acknowledge that your business name and the name of your principals may be reported to the MATCH™ (Member Alert to Control High Risk Merchants) listing maintained by MasterCard. 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.

2.7 Permitted Uses of Merchant Information

For the purpose of communicating your acceptance of the Card, American Express may use your name, address (including website addresses or URLs), customer service telephone numbers, and/or industry classification in any media at any time. The information is based on that what you have provided to your Merchant Services Provider or that is otherwise publicly available. In addition, the information you provide to your Merchant Services Provider may be transferred to American Express or its Affiliates throughout the world, for example, to process transactions and provide you with American Express products or services. Regardless of where American Express processes your information, American Express still protects it in the manner described in its online privacy statement and according to all Applicable Laws. For more information on American Express' Online Privacy Statement, please visit https://www.americanexpress.com/au/about-us/disclosures/privacy-statement/.

AMERICAN EXPRESS

Card Acceptance

3

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 world's leading card issuers, 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.

3.2 Treatment of the American Express Brand

You may issue policies related to customer identification, and define minimum Charge amounts, subject to Applicable Law and your Agreement with your Merchant Services Provider.

For the past 160 years, American Express has built a brand that is synonymous with trust, integrity, security, quality, and customer service. American Express works diligently to uphold its reputation, and restrict Merchants from engaging in activities that would harm American Express' business or 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,
- criticise or mischaracterise the Card or any of American Express' services or programmes,
- 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 Authorisation or submitting Transactions (or both).

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 to you) as prominently and in the same manner as any Other Payment Products.

American Express' corporate logo, the "American Express® Blue Box" logo, is the strongest visual symbol of American Express' image. The "Blue Box" represents and reinforces the high quality service and values of American Express. The appropriate version of the "Blue Box" logo must be displayed on all point-of-purchase materials and signs. The following guidelines apply to your use of the "Blue Box" logo in communications:

- Maintain at least 1/3 "X" (where "X" is equal to the height of the Blue Box Logo) between the Logo and any accompanying element
- The "Blue Box" logo minimum size is 3/8" and 1/2" is the preferred size.
- The "Blue Box" logo must always be shown in the pre-approved "American Express blue" or, in one- or two-colour communications, black.

You must not use American Express' Marks in any way that injures or diminishes the goodwill associated with the American Express Mark, nor in any way (without American Express' prior written consent) indicate that American Express endorses your goods or services. You shall only use American Express' Marks as permitted by the Agreement and shall cease using American Express' Marks upon termination of the Agreement.

For additional guidelines on the use of American Express' Marks, contact your Merchant Services Provider.

3.3 Prohibited Uses of the Card

You must not accept the Card for any of the following:

- any Transactions in the Prohibited Business Types set forth in Section 10.2, "Prohibited Merchants",
- 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,
- 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,
- damages, losses, penalties, or fines of any kind, except as provided in Section 4.4.9, "Property Damage to Accommodations and Other Rentals",
- unlawful/illegal activities, fraudulent business transactions or when providing the goods or services is unlawful/illegal (e.g., unlawful/illegal online internet sales of prescription medications or controlled substances; sales of any goods that infringe the rights of a Rights-holder under laws applicable to American Express, you, or the Cardmember),
- overdue amounts or amounts covering returned, previously dishonoured or stop-payment cheques (e.g., where the Card is used as a payment of last resort),
- amounts that represent repayment of a cash advance including, but not limited to, payday loans, pawn loans, or payday advances,
- sales made by third parties, sales for goods and/or services provided by third parties, or Entities conducting business in industries other than yours, or

An example of selling something that infringes the rights of a Rights-holder, is the sale of counterfeit goods.

- other items of which American Express or your Merchant Services Provider notifies you.

You must not use the Card to verify your customer's age.

For more information on prohibited industries, and on how American Express monitors such uses of the Card, see Chapter 10, "Risk Evaluation".

3.4 Prohibited Merchants

Some Merchants, and/or some of their Establishments, are not eligible (or may become ineligible) to accept the Card. Such Merchants or Establishments will be denied the privilege to accept the Card if it is determined that they meet one or more of the criteria for a prohibited Merchant, including the criteria set forth in Chapter 10, "Risk Evaluation". For additional information regarding Prohibited Merchants, contact your Merchant Services Provider directly.

3.5 Treatment of American Express Cardmember Information

Remember, if the Agreement terminates, Cardmember Information can only be retained according to the Payment Card Industry Data Security Standard (PCI DSS), which is available at www.pcisecuritystandards.org.

Any and all Cardmember Information is confidential and the sole property of the Issuer, American Express or its Affiliates.

Except as otherwise specified, you must not disclose Cardmember Information, nor use nor store it, other than to facilitate Transactions at your Establishments in accordance with the Agreement.

For more information about protecting Cardmember Information, see Chapter 8, "Protecting Cardmember Information".

AMERICAN EXPRESS

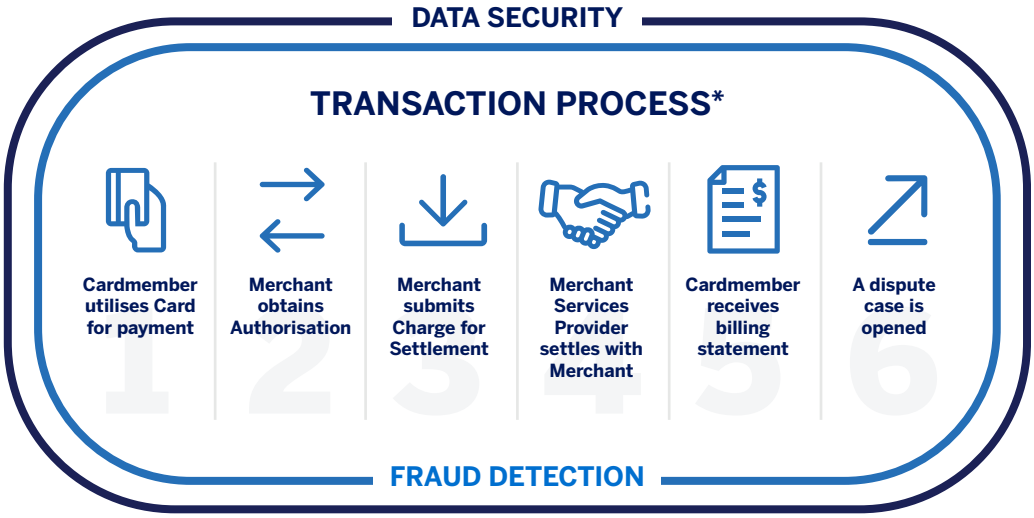
Transaction Processing

4

4.1 Transaction Process

The first step in understanding the Card acceptance process is to understand the American Express Transaction process.

The following graphic illustrates the high level phases that occur throughout the Transaction process. We will refer to this Transaction process at various points throughout the *Merchant Operating Guide*.



* This graphic is for illustration purposes only and is not to be construed as limiting or waiving American Express' rights with respect to Cardmember Information or other information.

Merchants are not required to have the Cardmember re-enter the Transaction Data because when Cardmembers make an Application-initiated Transaction or pay using other mobile phone or tablet , the Transaction Data collected to facilitate the Card Not Present Charge has already been provided directly by the Cardmember.

All valid Transactions begin with a Cardmember's decision to make a purchase. Whether the physical Card is used to facilitate a Card Present Charge, or the Cardmember provides their 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, you must:

- clearly and conspicuously, disclose all material terms of sale before obtaining an Authorisation, 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) about 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 assessed non-compliance fees and/ or have your Card acceptance privileges at your Establishments suspended or disentitled.

Transaction Data

All information required by American Express evidencing one or more Transactions, including information obtained at the point of sale, information obtained or generated during Authorisation and Submission, and any Chargeback.

4.2 In-Person Charges

American Express offers a variety of fraud prevention solutions that can be enabled at the point of sale. Contact your Merchant Services Provider for information related to fraud prevention solutions that may be available for your use.

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

4.2.1 No PIN Programme

The No PIN Programme does not provide protection against all Chargebacks. Even if an Establishment and Charge qualify under the No PIN Programme, you may still be subject to Chargeback for reasons unrelated to your failure to obtain a PIN from the Cardmember at the point of sale. Consult with your Merchant Services Provider for more information about Disputed Charges and Chargebacks.

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

To qualify for the No PIN Programme, 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 PIN Programme 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 Evaluation". 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 Programme.

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 PIN Programme, American Express will not exercise Chargeback for such Charges based solely on your Establishment's failure to obtain the Cardmember's PIN at the point of sale.

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

Note: Obtaining Cardmember signature on Card Present Transactions is optional to complete a Charge Record, and at your discretion, unless required by Applicable Law.

4.2.2 Unattended Terminals

Charges for purchases at Customer Activated Terminals (CATs) or payment kiosks will be accepted provided you meet the requirements for Charge Records as detailed in Section 4.5, "Charge and Credit Records" as well as comply with the *Technical Specifications* (see Section 2.4, "Compliance with the Technical Specifications"). Please contact your Merchant Services Provider for additional information on CAT requirements.

You must:

- include in all requests for Authorisation full Magnetic Stripe stream or Chip Card Data;
- ensure the Charge complies with the Technical Specifications, including flagging all requests for Authorisation and all Charge submissions with a CAT indicator, where technically feasible;
    - follow any additional Authorisation procedures that we may provide to you if you accept the Card at an unattended terminal that is part of, or attached to, a fuel dispenser; and
    - ensure that the unattended terminals notifies the Cardmember if the Transaction is declined, where technically feasible.

4.2.3 Electronic Charges

Electronic POS Systems automatically capture required information from the Card so it can be used to request Authorisation 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 recognised 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 about your POS System's capabilities.

4.2.3.1 Magnetic Stripe Card Charges

Only the person whose name appears on an American Express Card is entitled to use it. Cards are not transferable.

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

1. Verify that the Card is not visibly altered or mutilated (see Chapter 9, "Fraud Prevention" for additional information),
2. 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 4.2.3.3, "Contactless Chip Card Charges"),
3. Obtain an Authorisation Approval,
4. Verify the Card's Expiration Date,
5. Match the Card Number and the Expiration Date on the Card to the same information on the Charge Record, and
6. Ensure the name that prints on the Charge Record matches the name on the front of the Card.*
7. If you choose or are required by Applicable Law to obtain a Cardmember signature, see Subsection 4.2.3.2.1, "Obtaining Signature for In-Person Charges".

* 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 4.2.5, "Actions for In-Person Charges" and proceed accordingly.

4.2.3.2 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. 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 complete the Transaction without a PIN. You can also set your POS System to prompt the Cardmember to sign for the Charge (a Chip and signature Charge). See Subsection 4.2.3.2.1, "Obtaining Signature for In-Person Charges".

   For 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 4.2.3.1, "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 PIN Programme (see Section 4.2.1, "No PIN Programme" for additional information).
3. Obtain an Authorisation Approval.
4. Verify the Card's Expiration Date.
5. Match the Card Number and the Expiration Date on the Card to the same information on the Charge Record, and
6. Ensure the name that prints on the Charge Record matches the name on the front of the Card.*
7. If you choose or are required by Applicable Law to obtain a Cardmember signature, see Subsection 4.2.3.2.1, "Obtaining Signature for In-Person Charges".

   * 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.

In the case of Chip and PIN Transactions, if the PIN is not validated, you may be liable for Chargebacks unless your Establishment and the Charge qualify for the No PIN Programme (see Section 4.2.1, "No PIN Programme".

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 you upgrade your POS System for Chip and PIN acceptance for Other Payment Products, then you must comply with the Technical Specifications and other requirements American Express makes available.

If you are presented with a Chip Card and manually key the Transaction, you may be subject to counterfeit, lost/stolen and non-received fraud Chargebacks.

4.2.3.2.1 Obtaining Signature for In-Person Charges

If you choose or are required by Applicable Law to obtain signature on a manual imprint, printed, or electronic Card Present Charge, you must:

1. Obtain signature and verify that the signature is identical to the name on the Card*, and
2. Compare the signature (when obtained) on the Charge Record with the signature on 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.

4.2.3.3 Contactless Chip Card Charges

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 Chip Card to be read via a contactless reader, you must:

1. Capture Magnetic Stripe or Chip Card Data using the contactless reader, and
2. Obtain an Authorisation Approval.

For contactless Charges that are $100 or less, a signature is not required. Section 4.2.1, "No PIN Programme" 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 authorisation approval was obtained.

For Charges above $100, or if any of the following exclusions apply, follow the Card acceptance procedures outlined in either Subsection 4.2.3.1, "Magnetic Stripe Card Charges", Subsection 4.2.3.2, "Contact Chip Card Charges", or Subsection 4.2.3.5, "Digital Wallet Payments".

Exclusions:

- Prohibited Merchants or prohibited Transactions (or both) as defined in Chapter 10, "Risk Evaluation". 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.

4.2.3.4 Merchant-Presented Quick Response (MPQR)

If you have the ability to process MPQR Transactions, you must:

- have the Cardmember use their Mobile Device to scan the MPQR code;
- display the Quick Response (QR) code, which can be dynamic or static, for scanning by the Cardmember;
- ensure the MPQR code is not altered or tampered with;
- receive a notification that the Transaction has been approved and check the Transaction amount is correct before providing the goods or services. If you do not receive the notification, you should contact us to confirm the status of the MPQR Transaction;

- contact us or decline the Transaction if you are suspicious of the Cardmember or receive notification from us to do so; and
- retain records of MPQR Transactions. These can be in the form of a notification from us, an invoice, or other documentation of the Transaction.

4.2.3.5 Digital Wallet Payments

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.

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. 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.
2. Obtain an Authorisation Approval.
3. If you choose or are required by Applicable Law, obtain a signature, see Subsection 4.2.3.2.1, "Obtaining Signature for In-Person Charges".
4. If applicable, have the Cardmember complete a Consumer Device Cardholder Verification Method (CDCVM) on contactless initiated Transactions.
5. Continue to include an indicator in the Authorisation that the Transaction is a contactless Transaction, if applicable.
6. 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 4.2.3.1, "Magnetic Stripe Card Charges", or
   - Subsection 4.2.3.2, "Contact Chip Card Charges".

For Application-initiated Transactions, you should follow Card Not Present Charge policy as described in Section 4.3, "Card Not Present Charges".

For a Transaction to be recognised 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 Authorisation and Submission that the Transaction is a Digital Wallet Application-initiated Transaction (see Section 2.4, "Compliance with the Technical Specifications").

4.2.4 Key-Entered Charges

Only the person whose name appears on an American Express Card is entitled to use it. Cards are not transferable.

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 minimise your risk of Chargebacks, avoid manually key-entered Transactions whenever possible.

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. Key-enter the data,
3. Obtain an Authorisation Approval,
4. Verify the Card's Expiration Date,
5. Match the Card Number and the Expiration Date on the Card to the same information on the Charge Record, and
6. 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.

You may still be subject to other fraud Chargebacks, including counterfeit, lost, stolen, and non-received for manually key-entered Transactions.

You may also validate the Card's presence by performing Card Identification (CID) verification. See Subsection 9.10.1, "Card Not Present Fraud Tools" for additional information.

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.

4.2.5 Actions for In-Person Charges

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

Table 4-1: Actions for In-Person Charges

If	Then
The Card is obviously altered or counterfeit.	Do not accept the Card.
The Cardmember is attempting to use the Card outside of its Valid Dates. **Note:** Cards are valid through the last day of the month on the front of the Card.	Do not accept the Card. Advise the Cardmember to contact the customer service number on the back of the Card.
It appears that someone other than the Cardmember is attempting to use the Card.	Do not accept the Card. Indicate that the Cards are non-transferable and that only the Cardmember is permitted to use the Card.
The signature does not match the name on the Card.	Contact your Merchant Services Provider with a Code 10.
You are unable to obtain Authorisation electronically.	Contact your Merchant Services Provider to obtain an Authorisation.
The Authorisation is Declined.	Do not accept the Card and follow your internal policies for handling various Authorisation responses. See Section 5.8, "Possible Authorisation Responses".

If	Then
The customer presents an unsigned Card.	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.
The customer's signature on the Charge Record does not appear to match the customer's signature on the Card.	Contact your Merchant Services Provider with a Code 10, or if you prefer, simply decline to accept the Card.
The Card Numbers and Valid Dates on the Card do not match the Charge Record.	
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).	
The appearance of the Card, or the actions of the customer appear suspicious.	

4.3 Card Not Present Charges

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 Cardmember Information as described below | **Obtain an Authorisation Approval** | **Submit the Charge to American Express**

For Card Not Present Charges, you must create a Charge Record as described in Section 4.5, "Charge and Credit 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 authorising. American Express will not Chargeback for such Charges based solely upon a Cardmember claim that they 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 authorised 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 Authorisation 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.

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.

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.

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).

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

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

4.4 Other Charges

4.4.1 Advance Payment

Advance Payment Charges are available for 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, and travel-related services (e.g., tours, guided expeditions).

Purchases involving Advance Payment Charges generally carry a higher level of risk than other Charges, due to the fact that goods and services are not provided at the time the Charge is processed.

Check your Merchant Services Provider's policies for withholding settlement for part or all of such Charges until it is determined that the risk has diminished.

If you offer Cardmembers the option or require them to make Advance Payment Charges, 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 Authorisation. The Cardmember's consent must include:
  - their 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 Authorisation, and 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 4.5, "Charge and Credit 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.

To minimise your risk of a Disputed Advance Payment Charge, always:

- clearly disclose all reservation, sales, cancellation, and refund policies and
- retain a copy of the Cardmember's written consent, including a detailed description and expected delivery date of the goods and/or services to be provided in a format that easily allows you to respond to an Inquiry.

If you cannot deliver goods and/or services (e.g., because custom-ordered merchandise cannot be fulfiled), 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 fulfiled.

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.

Specific industries may have additional requirements or obligations to process Advance Payments.

4.4.2 Aggregated – Internet

To minimise 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).

This Subsection 4.4.2, "Aggregated – Internet" applies to Transactions processed by your Establishments conducting business over the internet. When processing Aggregated Charges, you must meet the following criteria:

- Clearly disclose your intent and obtain 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 Authorisation.
- 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 Authorisation of no more than USD $15 (fifteen United States Dollars) or its equivalent in local currency or such other amount as notified to you by your Merchant Service Provider.
- Create a Charge Record for the full amount of the Aggregated Charge.
- The amount of the Aggregated Charge must not exceed USD $15 (or such other amount as notified to you) or the amount for which you obtained Authorisation which ever is lower.
- Submit each Charge Record in accordance with Section 6.5, "Submission Requirements – Electronic". ACharge will be deemed "incurred" for purposes of this subsection, 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 (and/or refund as applicable) that comprises the Aggregated Charge, and
  - the date and the amount of the Aggregated Charge.

4.4.3 Delayed Delivery

To minimise your risk of a Disputed Charge with Delayed Delivery Charges, always:
- clearly disclose all sales and refund policies and
- retain a copy of the Cardmember's written consent in a format that easily allows you to respond to an Inquiry.

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 Authorisation,
- Obtain a separate Authorisation 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 within seven (7) days of the Charge being incurred. 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 obtain Authorisation 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.

4.4.4 Credentials-on-File

If you store Cardmember account data for Transaction processing you must ensure the Credentials-on-File include any Cardmember account data, including, but not limited to, Primary Account Number (PAN) or Token, that is stored by or on behalf of Merchants.

You must obtain Cardmember consent before storing Cardmember credentials. It is recommended that you process an initial Authorisation upon receiving Cardmember consent to store credentials.

You may store Cardmember credentials to initiate Merchant-Initiated Transactions (MITs). Cardmembers may also use their stored credentials to initiate Transactions.

You must adhere to our Specifications (see Section 2.4, "Compliance with the Technical Specifications").

4.4.5 Merchant-Initiated

A Merchant-Initiated Transaction (MIT) is a Transaction that is initiated by the Merchant through use of Credentials-on-File without direct participation from the Cardmember.

Merchants must obtain Cardmember consent to initiate an MIT, or a series of MITs, after storing a Cardmember's credentials. Cardmember consent for MITs and Credentials-on-File may be obtained simultaneously.

It is recommended that Merchants submit MITs only after an initial Cardmember-Initiated Transaction (CIT) or an initial Authorisation accompanying a Cardmember's request to store credentials.

It is recommended that Merchants submit MITs with the following data elements in the Authorisation Request:

- Merchant-Initiated Transaction (MIT) indicator
- Original Transaction Identifier (O-TID)

Merchants must adhere to the requirements in Section 4.3, "Card Not Present Charges" when processing MITs.

4.4.6 Recurring Billing

To minimise 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.

For more tips on reducing Chargebacks, see Chapter 11, "Chargebacks and Inquiries".

Recurring Billing is a payment method where the Cardmember consents and authorises the Merchant to Charge the Cardmember's Card account on a periodic basis (e.g., membership fees to health clubs, magazine subscriptions, and insurance premiums). Each payment may be for a variable or a fixed amount. Merchants should adhere to the requirements in Subsection 4.4.5, "Merchant-Initiated" when processing Merchant-Initiated Charges for Recurring Billing.

Before submitting your first Recurring Billing Charge you must:

- clearly and conspicuously disclose all material terms of the offer including, if applicable, the fact that Recurring Billing Charges will continue until the option is canceled by the Cardmember;
- obtain the Cardmember's express consent to bill their Card and the Recurring Billing Charges terms before submitting the first Recurring Billing Charge;
- obtain the Cardmember's name, the Card number, the Cardmember's signature (if applicable), Card expiry date, the Cardmember's billing address, and a statement confirming consent for you to charge their Card for the same or different amounts at specified or different times;
- 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;
- comply with any instructions of which your Merchant Services Provider may reasonably notify you;
- notify the Cardmember that they are able to discontinue Recurring Billing Charges at any time and provide contact details for canceling Recurring Billing Charges; and

- ensure that your process for cancellation of Recurring Billing is simple and expeditious.

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.

The method you use to secure the Cardmember's consent must contain a disclosure that you may receive updated Card account information from the financial institution issuing the Cardmember's Card. You must retain evidence of such consent for two (2) years from the date you submit the last Recurring Billing Charge.

If notification is required prior to each varying Recurring Billing Charge, you must notify the Cardmember of the amount and date of each Recurring Billing Charge:

- at least ten (10) days before submitting each Charge; and
- whenever the amount of the Charge exceeds a maximum Recurring Billing Charge amount specified by the Cardmember.

In addition to our other Chargeback rights, American Express may exercise Chargeback for any Charge that does not meet the requirements set forth in this Subsection 4.4.6, "Recurring Billing"" and Subsection 4.4.6.1, "Introductory Offers". We may exercise our Chargeback rights for any Charge of which you have notified the Cardmember and to which the Cardmember does not consent or if you process Recurring Billing Charges after the Cardmember or we have notified you that the Cardmember has withdrawn consent for Recurring Billing Charges.

Before submitting any Recurring Billing Charge you must:

- obtain Authorisation; and
- create a Charge Record including indicators that the Transaction is a Recurring Billing Charge.

4.4.6.1 Introductory Offers

If you offer Cardmembers an option to make Recurring Billing Charges that include an Introductory Offer, you must comply with all requirements set forth in this Section 4.4.6, "Recurring Billing" policy in addition to the following requirements:

- Clearly and conspicuously disclose all material terms of the Introductory Offer to the Cardmember, including a simple and expeditious cancellation process that allows the Cardmember to cancel before submitting the first Recurring Billing Charge.
- Obtain the Cardmember's express consent to accept the terms and conditions of the Introductory Offer.
- Send Cardmember a confirmation notification in writing upon enrolment in the Introductory Offer.
- Send Cardmember a reminder notification in writing before submitting the first Recurring Billing Charge, that allows the Cardmember a reasonable amount of time to cancel.

4.4.7 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 Authorisation, 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.
- You must create a Charge Record for a Prepaid Card as you would any other 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 an American Express 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.

For information about processing Prepaid Cards, call the customer service number on the back of the Card in question.

4.4.8 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 4.4.8.1, "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 recognised 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.

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".

4.4.8.1 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 9.9, "Travelers Cheque and Gift Cheque Security Features".
- Obtain authorisation – American Express recommends obtaining an authorisation to reduce the chances of accepting fraudulent cheques. American Express offers a variety of authorisation tools. See authorisation methods in the following table to determine your course of action:

Table 4-2: Acceptance Procedures

If	Then
The signature and countersignature are a reasonable match (they look alike, but may not be identical)	Accept the cheque. There is no need to obtain any identification.
You suspect that the countersignature may be false, or you did not watch the customer countersign	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.
The signatures are not the same, or if there is a question regarding the validity of the cheque	Call the Travelers Cheque/Gift Cheque Customer Service at 1-866-296-5198.
You suspect that the Travelers cheque being presented is fraudulent	Use any of the following methods to verify that the cheque you are accepting is authentic: • Perform a smudge test (see Chapter 9, "Fraud Prevention" for details). • Obtain online Authorisation at www.americanexpress.com/verifyamextc.

4.4.9 Property Damage to Accommodations and Other Rentals

If a Cardmember expressly consents to use the Card to pay for Property Damage Fees and/or smoking fees to a rented accommodation or equipment, you may accept the Card, provided you have complied with following conditions for payment for such fees, and we classify the rental as one of the following:

- Lodging accommodations
- Trailer parks and campground rental
- Motor home rental
- Boat rental
- Bicycle rental
- Motorcycle rental

- Equipment rental

Conditions for Payment for such fees:

- The Card was used as the original payment method for the accommodations or rental.
- You must provide in writing, to the Cardmember, an itemised list and description of the property and/or smoke damage which has occurred.
- Prior to submitting a Charge, you must obtain the Cardmember's agreement in writing[1] to:
  - Accept responsibility for the fees associated with the property and/or smoke damage.
  - Select American Express as the payment method for the fees associated with the property and/or smoke damage.
  - Accept the total amount for which the Cardmember is responsible, and that the final billed amount can be up to 15% more than the estimated amount. No amounts in excess of 115% of the disclosed amount shall be charged to the Cardmember's Card, without the express prior written consent of the Cardmember.
- You must obtain Authorisation for the amount of the fees associated with the property and/or smoke damage each time a Charge is submitted.
- You must prepare a Charge Record separate from the Charge Record for the rental or lodging stay. You must adhere to all requirements outlined in Chapter 4, "Transaction Processing" for completion of the Charge Record. In addition, you must observe the following:
  - After the exact fee associated with the property and/or smoke damage has been determined and the Charge is ready for Submission, you must provide the Cardmember with an itemised summary; insert the amount on the Charge Record (in no event in excess of the estimated amount plus 15% agreed to by the Cardmember).
- In addition to the other Chargeback rights contained in the Agreement, we may exercise Chargeback rights with respect to any Charge for damages which is not submitted in accordance with all the procedures contained within the Agreement, including the provisions of this Section 4.4.9, "Property Damage to Accommodations and Other Rentals".
- You must not include the following in an Authorisation Request or in a Charge Submission:
  - Losses due to theft of the equipment.
  - Losses due to theft of property or equipment from within a rental accommodation.
  - Loss of revenue due to the loss of use of the rental equipment or lodging accommodations.
- You must submit the Charge to us within 90 calendar days of check-out or rental return date.

4.4.10 Split Shipment

A split shipment Transaction occurs when a Cardmember makes a single purchase of multiple individually priced goods and the goods are delivered to the Cardmember in multiple shipments. Unit prices and items sold as a set must not be billed as separate Charges. You may obtain a single Authorisation and submit multiple Charge Records for the purpose of completing a split shipment Transaction. The Authorisation will be valid for up to seven (7) days after the Authorisation date. Section 5.3, "Authorisation Time Limit" .

To accept the Card for split shipment Transactions, you must:

- State your full cancellation and refund policies;
- Advise the Cardmember of the Authorisation amount that will be requested;
- Disclose and obtain the Cardmember's consent that the items from the purchase will be delivered separately and billed as separate Charges;

1. The Cardmember's consent must be provided in writing after the damages have occurred and without any threat or duress.

- Provide the estimated delivery date(s);
- Submit a Charge Record only after each item has shipped.

4.5 Charge and Credit Records

4.5.1 Charge Records

You must create a Charge Record for every Charge. For each Charge submitted electronically, you must create an electronically reproducible Charge Record, that complies with the *Technical Specifications*. See Section 2.4, "Compliance with the Technical Specifications".

The Charge Record (and a copy of the customer's receipt) must disclose the Authorisation Approval code and your return and/or cancellation policies.

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 except in the case of hotel charges, or Split Shipment Transactions. See Subsection 4.4.10, "Split Shipment".

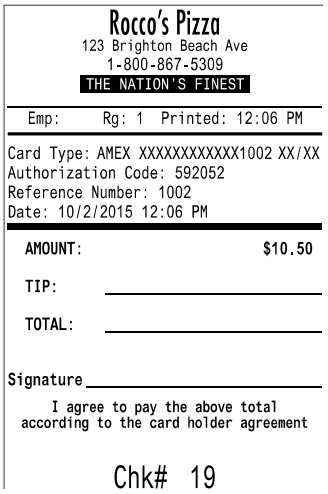
For all Charge Records, you must:

1. Submit the Charge to your Merchant Services Provider for payment.
2. Retain the original or electronically stored 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.

You may be able to create more than one Charge Record if the purchase qualifies for a Delayed Delivery Charge. See Subsection 4.4.3, "Delayed Delivery".

The retention time frame for the original or electronically stored Charge Record is twenty-four (24) months from the date you submitted the corresponding Charge to us.

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.


Rocco's Pizza
123 Brighton Beach Ave
1-800-867-5309
THE NATION'S FINEST

Emp: Rg: 1 Printed: 12:06 PM

Card Type: AMEX XXXXXXXXXXX1002 XX/XX
Authorization Code: 592052
Reference Number: 1002
Date: 10/2/2015 12:06 PM

AMOUNT: $10.50

TIP: _____

TOTAL: _____

Signature _____

I agree to pay the above total
according to the card holder agreement

Chk# 19

4.5.2 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 2.4, "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,
- your Establishment name and address and, if applicable, store number, and
- your Merchant Number.

For all Credit Records, you must:

1. Submit the Credit through your Merchant Services Provider.
2. Retain the original or 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 the original or electronically stored Credit Records is twenty-four (24) months from the date you submitted the corresponding Credit to your Merchant Services Provider.

Pursuant to Applicable Law, truncate the Card Number and do 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.

4.5.3 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. If you choose to support Authorisation for Credit, obtain an Authorisation.
2. Create a Credit Record.
3. Compare the last four digits on the Charge Record against the Card presented (when applicable).
4. Have the Cardmember sign the Credit Record (optional).
5. 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. 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 Merchant Number of the Establishment where the Charge 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.

If you choose to support Authorisation on Credit and receive a decline Authorisation response, apply your established store policy.

Contact your Merchant Services Provider for additional information and guidance on processing Credits.

4.6 Use of Third Parties

As a Merchant, you make decisions and choices on behalf of your business each and every day. Some Merchants choose to deal directly with us for all aspects of the Transaction process; others enlist the assistance of various third parties to provide them with services. These third parties are your Covered Parties and may include:

- Merchant Services Provider/Service Providers/processors,
- Terminal Providers,
- Vendors, and
- Other agents contracted to operate on your behalf.

You may retain, at your expense, such third parties; however, you remain financially and otherwise liable for all obligations (including confidentiality obligations and compliance with the *Technical Specifications*), services, and functions they perform under the Agreement for you, such as the technical requirements of authorising and submitting Transactions to us, as if you performed such obligations, services, and functions.

You are responsible and liable for all problems and expenses caused by your Merchant Services Provider and/or third parties, including any Settlement payments misdirected to other parties because of the misprogramming of your Point of Sale (POS) System by your Merchant Services Provider and/or third parties.

AMERICAN EXPRESS

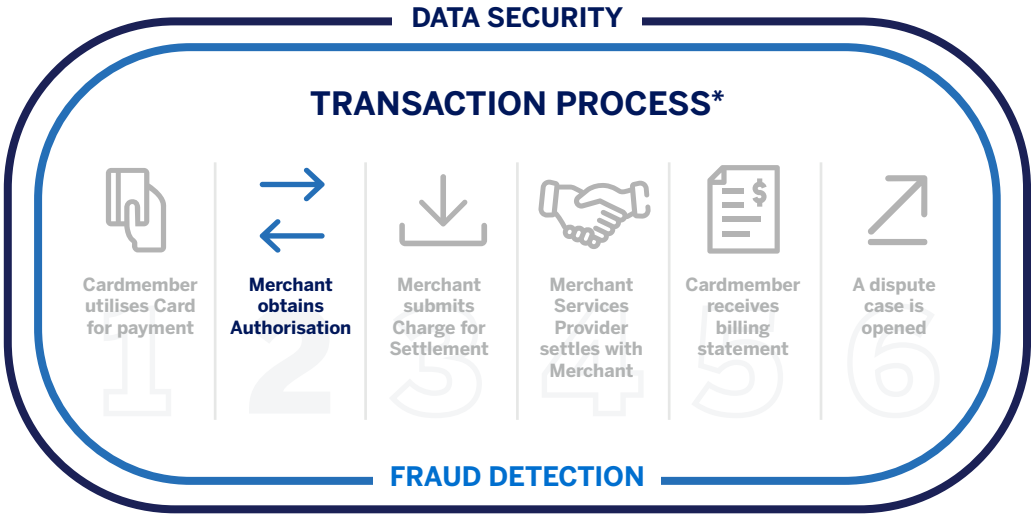
Authorisations

5

5.1 Transaction Process

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

If you choose to support Authorisation for Credit, you shall comply with the Authorisation requirements as applicable.



* This graphic is for illustration purposes only and is not to be construed as limiting or waiving American Express' rights with respect to Cardmember Information or other information.

5.2 The Purpose of Authorisation

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

For every Charge, you are required to obtain an Authorisation Approval except for Charges under a Floor Limit (see Section 5.6, "Floor Limit"). For every Credit, we recommend that you obtain an Authorisation Approval for the full amount of the refund in accordance with Section 4.5.3, "Processing a Credit".

The Authorisation Approval must be for the full amount of the Charge except for Merchants and/or Transaction types that we classify in the industries listed in Section 5.4, "Estimated Authorisation".

An Authorisation 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, (iv) you will not be subject to a Chargeback, or (v) the Charge you submit will not be rejected.

5.3 Authorisation Time Limit

Authorisation Approvals for Charges are valid for seven (7) days after the Authorisation date. You must obtain a new Approval if you submit the Charge to your Merchant Services Provider more than seven (7) days after the original Authorisation date.

Authorisation Approvals for Credit are valid for seven (7) days. After seven (7) days, we recommend that you obtain a new Approval for Credit Authorisation.

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 Authorisation requests is Declined, do not provide the goods or services or submit the Charge. If you do, you will be subject to a Chargeback.

For Estimated Authorisation time frames see Section 5.4, "Estimated Authorisation".

5.4 Estimated Authorisation

If you are classified or it is determined that you operate in one of the following industries, then the following Estimated Authorisation procedures apply where the final Charge amount is not known at the time of Authorisation.

You may only obtain an Estimated Authorisation in the industries listed below. Do not overestimate the Authorisation amount. You must obtain the Cardmember's consent to such estimated amount prior to requesting the Authorisation.

You must submit the corresponding Charge no later than the Estimated Authorisation Timeframe. For any amount of the Charge that exceeds the amount for which you obtained an Authorisation you must obtain the Cardmember's consent.

If the final amount of the Charge is:

- no greater than the amount for which you obtained Authorisation plus the applicable Estimate Authorisation percentage listed below of that amount, no further Authorisation is necessary; or
- greater than the amount for which you obtained Authorisation by more than the applicable Estimated Authorisation percentage listed below of that amount, you must obtain a new Authorisation. If you fail to obtain such Authorisation, or your request for such Authorisation is declined, American Express will have Chargeback rights for the amount in excess of the original Authorisation amount plus the applicable Estimated Authorisation percentage of that amount. For the avoidance of doubt, American Express will have Chargeback rights for the final amount of the Charge for reasons other than the failure to obtain an approved Authorisation.

Estimated Authorisation percentages listed below do not apply to Partially Approved Authorisations.

An Estimated Authorisation is valid for the applicable Estimated Authorisation time frame listed below. You must obtain a new Approval if you do not submit the Charge to us within the Estimated Authorisation time frame.

We recommend that you perform an additional Authorisation as soon as the Charge amount exceeds the original Authorisation by the Estimated Authorisation percentage in the table in this section as follows:

- For Authorisations obtained intermittently – at least once per day.
- For Authorisations for estimated amounts at the point the amount of costs incurred exceeds the Authorisation for estimated amounts by more than Estimated Amount percentage.

For example, in the lodging industry:

If the Authorisation was for $1,000, and the total of purchases was no more than $1,150, no further Authorisation is necessary. However, if the total purchases were $1,200, and you did not obtain additional Authorisation, then we have Chargeback rights up to $50.

Table 5-1: Estimated Charge Amount

Industry	MCC	Estimated Charge Variance +/-	Authorisation Validity Period
Eating Places, Restaurants	5812	30%[2]	7 days
Drinking Places	5813	30%[2]	7 days
Grocery Stores (Card Not Present)	5411	15%[1]	7 days

Industry	MCC	Estimated Charge Variance +/-	Authorisation Validity Period
Retail Stores (Card Not Present)	All MCCs	15%[1]	7 days
Taxicabs & Limousines	4121	20%	7 days
Lodging	7011	15%	Duration of stay
Motor Home & RV Rentals	7519	15%	7 days
Fast Food Restaurants	5814	30%[2]	7 days
Beauty & Barber Shops	7230	20%	7 days
Health & Beauty Spas	7298	20%	7 days

[1]The 15% Estimated Charge variance for Retail and Grocery only applies to Card Not Present Charges.

[2]The Estimated Charge variance at Restaurant, Fast Food, and Drinking Places for debit and prepaid Charges is 20%.

5.5 Partial Authorisation

Partial Authorisation is an optional functionality of Prepaid and Debit Cards that allows Merchant to obtain an Authorisation for less than the requested purchase amount. The Issuer can approve the Authorisation for a partial amount when the Cardmember does not have sufficient funds to cover the full purchase amount requested. The Cardmember, then, has the option to pay for the outstanding amount of the purchase by other means.

Partial Authorisation is not supported for the following Transaction types:

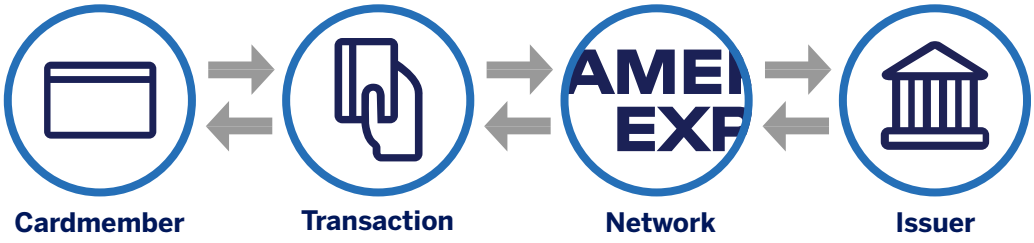
- Cross-border Transactions (Transactions in which the Merchant's currency is different than the Issuer's currency)
- Recurring Billing

5.6 Floor Limit

American Express maintains a zero-dollar Floor Limit on all Charges regardless of the amount. If any one Charge, or series of Charges, made on the same day by any one Cardmember at the Establishment, is equal to or greater than this Floor Limit, the Establishment must request Authorisation.

5.7 Authorisation Process

Cardmember	Transaction	Network	Issuer
The Cardmember provides you with the Card or the Card Information.	The POS System captures the Card Information and transfers it to the American Express Network.	The Network sends the Approval request to the Issuer.	The Issuer Approves or declines the request.
Upon receiving the decision of the Approval or decline of the request, you will be able to complete or deny the Transaction and inform the Cardmember.	The POS System displays the Approval or decline of the request.	The American Express Network relays the information back to the POS System.	The Issuer communicates the Approval or decline back to the American Express Network.



5.8 Possible Authorisation Responses

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

Table 5-2: Authorisation Response

Authorisation Response	What It Means
Approved	The Charge or Credit is approved.
Partially Approved (for use with Prepaid and Debit Cards only)	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. For Split Tender, you may follow your policy on combining payment on Prepaid and Debit Cards with any Other Payment Products or methods of payment.
Declined or Card Not Accepted	The Charge is not approved. Do not provide the goods or services or submit the Charge. 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. If you submit the Charge after receiving a Decline, American Express may reject the Charge or you will be subject to a Chargeback. The Credit is not approved. Inform the Cardmember promptly that the Credit has been Declined. You may apply your established store policy.
Pick up	You may receive an Issuer point of sale response indicating that you must pick up the Card. Follow your internal policies when you receive this response. Never put yourself or your employees in unsafe situations. Contact your Merchant Services Provider for further information regarding a Pick Up Card response.

5.9 Obtaining an Authorisation

Failure to comply with the *American Express Technical Specifications* for Authorisation may impact your ability to successfully process Transactions. For example, we may not be able to issue an Authorisation response or process the Charge at Submission (see Section 6.5, "Submission Requirements – Electronic").

You must ensure that all Authorisation requests comply with the *Technical Specifications* (see Section 2.4, "Compliance with the Technical Specifications"). If the Authorisation request does not comply with the *Technical Specifications*, the Authorisation was Declined, or for which no Approval code was obtained, American Express may reject the Submission or American Express may exercise 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 Authorisation then you must follow the requirements for key-entered Charges. See Subsection 4.2.4, "Key-Entered Charges" for additional information.

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

Occasionally, obtaining an electronic Authorisation may not be possible (e.g., due to POS System problems, System Outages, or other disruptions of an electronic Charge).

5.10 Card Identification (CID) Number

Card Identification (CID) Number

CID is a four-digit number printed on the face of the Card.

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

If, during the Authorisation, 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, 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.

5.11 Authorisation Reversal

It is a good practice to reverse an Authorisation for an Approved Charge if you do not intend to submit a Charge to your Merchant Services Provider within the Authorisation time limits. See Section 5.12, "Pre-Authorisation". You may reverse an Authorisation for a corresponding Charge by:

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

After a Charge Record has been submitted, an Authorisation 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 4.5.3, "Processing a Credit".

5.12 Pre-Authorisation

A pre-Authorisation is an Authorisation 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).

AMERICAN EXPRESS

Submissions

6

6.1 Introduction

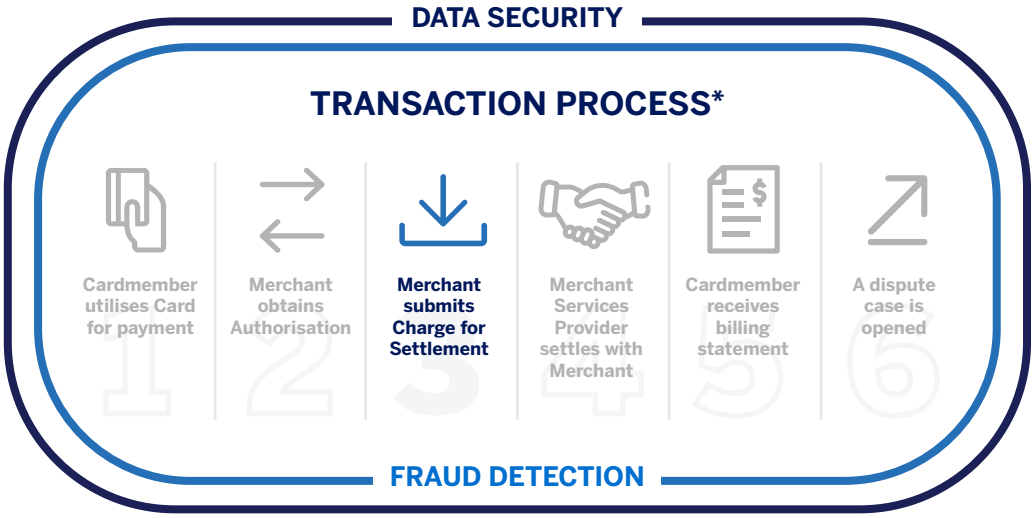
Merchants are familiar with commitments that keep their business running smoothly. One such commitment is to submit Transactions conducted at your Establishments to your Merchant Services Provider for payment.

Since payment cannot occur until the Transactions are submitted, you are encouraged to submit Transactions daily even though you have up to seven (7) days to do so.

See Section 4.2, "In-Person Charges" and Section 4.5.3, "Processing a Credit" for additional information.

6.2 Transaction Process

Collect Transactions during the business day and submit them to us, through your Merchant Services Provider, usually at the end of a day. If you have any Submission problems, contact your Merchant Services Provider.



* This graphic is for illustration purposes only and is not to be construed as limiting or waiving American Express' rights with respect to Cardmember Information or other information.

6.3 Purpose of Submission

After we receive the Submission, we process it and settle with your Merchant Services Provider. Your Merchant Services Provider will then settle directly with you in accordance with the payment plan, speed of payment, and payment method, you have arranged with them.

Transactions will be deemed accepted on a given business day if processed by us before the close of business.

Please contact your Merchant Services Provider for additional information on submitting Transactions, processing cutoff times, and payment procedures.

6.4 Submission Process

After you collect the Transactions during your business day, we encourage you to submit them to your Merchant Services Provider daily.

Following the instructions displayed in your POS System, you can submit your Transactions to be processed and Settled.

Payments cannot occur until the Transactions are Submitted, received, and processed through your Merchant Services Provider.

6.5 Submission Requirements – Electronic

For additional information about retaining information, see Section 4.5, "Charge and Credit Records" and Section 8.4, "Standards for Protection of Encryption Keys, Cardholder Data, and Sensitive Authentication Data".

Besides impacting your Transaction processing, failure to comply with the *Technical Specifications* may increase your Disputed Charges. For instance, for a Card Not Present Charge, if you do not provide a customer service telephone number or web address, Cardmembers who do not recognise Charges, may initiate "no knowledge" Inquiries rather than contact you directly to identify the Charge.

You must submit Transactions electronically in accordance with your Merchant Services Provider's instructions.

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

A Submission or Batch must comply with the *American Express Merchant Operating Guide*, including the *Technical Specifications* (see Section 2.4, "Compliance with the Technical Specifications"). Failure to follow these requirements could result in a rejection of your Submission or Batch or delay in your payment (or both). If a Submission or Batch rejects, you may not be paid until the Submission or Batch is corrected and resubmitted. You must work with your Merchant Services Provider to correct the error, then resubmit. For Submissions which fail to comply with the *Technical Specifications*, American Express has the right to Chargeback.

You must submit Charges and Credits only in Australian Dollars.

6.5.1 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 4.4.2, "Aggregated – Internet" 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 4.4.3, "Delayed Delivery" and Section 4.4.1, "Advance Payment" for additional information.

6.5.2 Credit Submissions

You must submit all Credits to your 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. Please contact your Merchant Services Provider for additional information regarding Credit submission requirements.

6.6 Submission Requirements – Paper

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

6.7 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 mid-day and again in the evening).

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

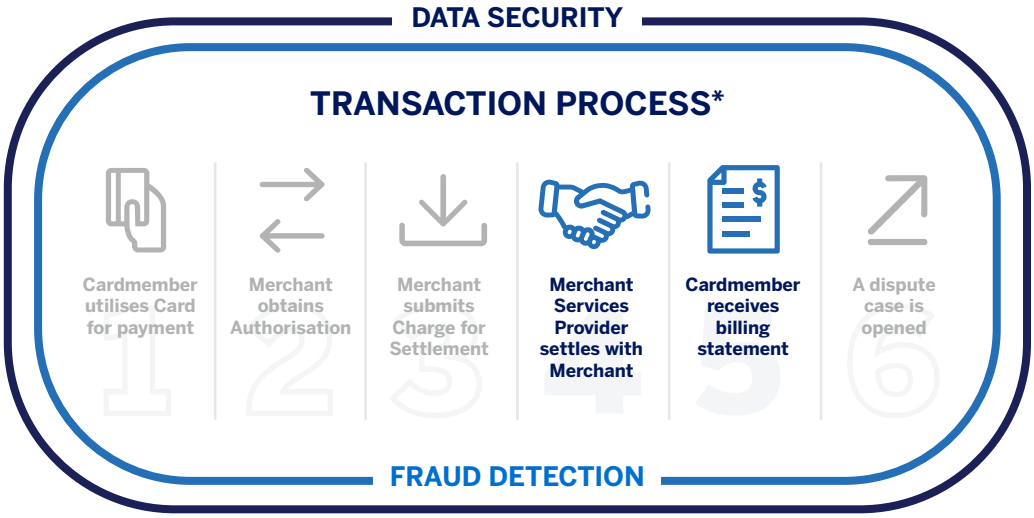
AMERICAN EXPRESS

Settlement

7

7.1 Transaction Process

After we receive a Submission file, we begin the process of settling. Settlement of payment from American Express will be made directly to your Merchant Services Provider.



* This graphic is for illustration purposes only and is not to be construed as limiting or waiving American Express' rights with respect to Cardmember Information or other information.

7.2 Settlement Amount

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

7.3 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.

7.4 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.

AMERICAN EXPRESS

Protecting Cardmember Information

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 these Data Security Requirements.

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:

American Express Card, or Card – Any card, account access device, or payment device or service bearing American Express' or an affiliate's name, logo, trademark, service mark, trade name, or other proprietary design or designation and issued by an issuer or a card account number.

Approved Point-to-Point Encryption (P2PE) Solution – A solution that is included on PCI SSC list of validated solutions or validated by a PCI SSC Qualified Security Assessor P2PE Company.

Approved Scanning Vendors (ASVs) – An Entity that has been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to certain PCI DSS requirements by performing vulnerability scans of internet facing environments. See Section 8.7, "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.

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

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

Cardholder Data Environment (CDE) – The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.

Cardmember – 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 – Information about American Express Cardmembers and Card Transactions, including names, addresses, card account numbers, and card identification numbers (CIDs).

Charge – A payment or purchase made on a Card.

Chip – An integrated microchip embedded on a Card containing Cardmember and account information.

Chip Card – 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 our materials).

Chip-Enabled Device – A point-of-sale device having a valid and current EMVCo (www.emvco.com) approval/certification and be capable of processing AEIPS compliant Chip Card Transactions.

Credit – The amount of the Charge that you refund to Cardmembers for purchases or payments made on the Card.

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 (POS) equipment or systems, or payment processing solutions, Entities associated to your American Express merchant account, and any other party to whom you may provide Cardholder Data or Sensitive Authentication Data (or both) access in accordance with the Agreement.

Data Incident – An incident involving the compromise or suspected compromise of American Express encryption keys, or at least one American Express Card account number, in which there is:

- unauthorised access or use of Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) that are stored, processed, or transmitted on your equipment, systems, and/or networks (or the components thereof) of yours or the use of which you mandate or provide, or make available;
- use of such Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) other than in accordance with the Agreement; and/or
- suspected or confirmed loss, theft, or misappropriation by any means of any media, materials, records, or information containing such Encryption Keys, Cardholder Data, or Sensitive Authentication Data (a combination of each).

Data Incident Event Window – The window of intrusion (or similarly determined period of time) set forth in the final forensic report (e.g., PCI Forensic Investigator (PFI) report), or if unknown, up to 365 days prior to the last Notification Date of potentially Compromised Card Numbers involved in a Data Compromise reported to us.

Data Security Requirements (DSR) – The American Express data security policy, as described in Chapter 8, "Protecting Cardmember Information" of the *Merchant Operating Guide*.

EMV Specifications – The specifications issued by EMVCo, LLC, which are available at www.emvco.com.

EMV Transaction – An integrated circuit card (sometimes called an "IC Card," "chip card," "smart card," "EMV card," or "ICC") Transaction conducted on an IC card capable point of sale (POS) terminal with a valid and current EMV type approval. EMV type approvals are available at 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

Forensic Incident Final Report Template – Means the template available from the PCI Security Standards Council, which is available at www.pcisecuritystandards.org.

Issuer – 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.

Level 1 Merchant – 2.5 million American Express Card Transactions or more per year; or any Merchant that American Express otherwise deems a Level 1 Merchant.

Level 2 Merchant – 50,000 to 2.5 million American Express Card Transactions per year.

Level 3 Merchant – 10,000 to 50,000 American Express Card Transactions per year.

Level 4 Merchant – Less than 10,000 American Express Card Transactions per year.

Merchant – The Merchant and all of its affiliates that accept American Express Cards under a 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.

Merchant Level – The designation assigned to Merchants related to their PCI DSS compliance validation obligations, as described in Section 8.7, "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 for the Secure Software Framework, including the Secure Software Standard and Secure Software Life Cycle Standard, which are available at https://www.pcisecuritystandards.org/document_library/?document=sec_sware_faag.

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

Payment Card Industry Security Standards Council (PCI SSC) Requirements – The set of standards and requirements related to securing and protecting payment card data, including the PCI DSS and PA DSS, available at 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.

PCI DSS – Payment Card Industry Data Security Standard, which is available at 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.

PCI PIN Security Requirements – The Payment Card Industry PIN Security Requirements, which are available at www.pcisecuritystandards.org.

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.

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 Authorisations or to collect Transaction data, or both.

Primary Account Number (PAN) – The meaning given to it in the then current Glossary of Terms for the PCI DSS.

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 8.7, "Periodic Validation of Merchant Systems".

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.

Targeted Analysis Programme (TAP) – A programme that provides early identification of a potential Cardholder data compromise in your Cardholder Data Environment (CDE). See Section 8.3, "Targeted Analysis Programme (TAP)".

Token – The cryptographic token that replaces the PAN, based on a given index for an unpredictable value.

Transaction – A Charge or a Credit completed by means of a Card.

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 Targeted Analysis Programme (TAP)

Cardholder Data compromises may be caused by data security gaps in your Cardholder Data Environment (CDE). Examples of Cardholder Data compromise include, but are not limited to:

- **Common Point of Purchase (CPP)**: American Express Cardmembers report fraudulent Transactions on their Card accounts and are identified and determined to have originated from making purchases at your Establishments.
- **Card Data found**: American Express Card and Cardholder Data found on the world wide web linked to Transactions at your Establishments.
- **Malware suspected**: American Express suspects that your business is using software infected with or vulnerable to malicious code.

TAP is designed to identify potential Cardholder Data compromises.

You must, and you must cause your Covered Parties to, comply with the following requirements upon notification from American Express or your Merchant Services Provider, of a potential Cardholder Data compromise.

- You must promptly review your CDE for data security gaps and remediate any findings.
  - You must cause your third-party vendor(s) to conduct a thorough investigation of your CDE if outsourced.
- You must provide a summary of action taken or planned after your review, evaluation, and/or remediation efforts upon notification from American Express or your Merchant Services Provider.
- You must provide updated PCI DSS validation documents in accordance with Section 8.7, "Periodic Validation of Merchant Systems".
- As applicable, you must engage a qualified PFI to examine your CDE if you or your Covered Party:
  - Cannot resolve the Cardholder Data compromise within a reasonable period of time, as determined by American Express, or

- Confirm that a Data Incident has occurred and comply with the requirements set forth in Section 8.5, "Data Incident Management Obligations".

If you cannot meet these obligations, your Merchant Services Provider may have the right to terminate the Agreement in accordance with its terms as well as impose non-compliance fees on you.

8.4 Standards for Protection of Encryption Keys, Cardholder Data, and Sensitive Authentication Data

Remember if the Agreement terminates, Cardholder Data can only be retained according to the PCI DSS which is available at pcisecuritystandards.org

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 PCI DSS and other PCI SSC Requirements applicable to your processing, storing, or transmitting of Cardholder Data or Sensitive Authentication Data no later than the effective date for implementing that version of the applicable Requirement, and
- use, when deploying new or replacement PIN Entry Devices or Payment Applications (or both), only those that are PCI-Approved.

You must protect all American Express 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 8.7, "Periodic Validation of Merchant Systems" except as otherwise provided in that section).

8.5 Data Incident Management Obligations

You must notify your Merchant Services Provider immediately and in no case later than seventy-two (72) hours after discovery of a Data Incident. In addition:

- You must conduct a thorough forensic investigation of each Data Incident.
- For Data Incidents involving 10,000 or more unique Card Numbers, you must engage a PFI to conduct this investigation within five (5) days following discovery of a Data Incident.
- The *unedited* forensic investigation report must be provided to your Merchant Services Provider in accordance with their time frame for completing such information.
- You must promptly provide to your Merchant Services Provider all Compromised Card Numbers. American Express reserves the right to conduct its own internal analysis to identify Card Numbers involved in the Data Incident.

Forensic investigation reports must be completed using the current Forensic Incident Final Report Template available from PCI. Such report 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 (i) providing a plan for remediating all PCI DSS deficiencies, and (ii) participating in the American Express compliance programme (as described below). Upon your Merchant Services Provider's request, you shall provide validation by a QSA that the deficiencies have been remediated.

Notwithstanding the foregoing paragraphs of this Section 8.5, "Data Incident Management Obligations":

- American Express may, in its sole discretion, require you to engage a PFI to conduct an investigation of a Data Incident for Data Incidents involving less than 10,000 unique Card

Numbers. Any such investigation must comply with the requirements set forth above in this Section 8.5, "Data Incident Management Obligations", and must be completed within the time frame required by American Express.

- American Express may, in its sole discretion, separately engage a PFI to conduct an investigation for any Data Incident and may charge the cost of such investigation to you.

You must work with your Merchant Services Provider and American Express to rectify any issues arising from the Data Incident, including consultations 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.

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.

8.6 Reserved

8.7 Periodic Validation of Merchant Systems

You must take the following actions to validate under PCI DSS annually and every 90 days as described below, 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.

There are four actions required to complete validation:

Action 1 – Participate in American Express' PCI compliance programme under this policy.

Action 2 – Understand your Merchant Level and Validation Requirements.

Action 3 – Complete the Validation Documentation that you must send to your Merchant Services Provider.

Action 4 – Send the Validation Documentation to your Merchant Services Provider within the prescribed timelines.

Action 1 - Participate in American Express' Compliance Programme under this Policy

Level 1 Merchants and Level 2 Merchants, as described below, must participate in American Express' PCI Compliance Programme under this policy by providing the full name, email address, telephone number, and physical mailing address of an individual who will serve as their general data security contact. You must submit this information to your Merchant Services Provider. You must notify your Merchant Services Provider if this information changes, providing updated information where applicable. Your failure to provide such contact information may result in the assessment of non-compliance fees. Please contact your Merchant Services Provider for more information regarding its data security compliance requirements.

American Express may designate, at our sole discretion, certain Level 3 and Level 4 Merchants' participation in American Express' compliance programme under this policy by sending them written notice. Any such Merchant must enrol in the compliance programme no later than ninety (90) days following receipt of the notice.

Action 2 - Understand 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 8-1: Merchant Validation Documentation

Merchant Level/ Annual American Express Transactions	Report on Compliance Attestation of Compliance (ROC AOC)	Questionnaire Attestation of Compliance (SAQ AOC) AND Quarterly External Network Vulnerability Scan (Scan)
Level 1/ 2.5 million or more	Mandatory	Not applicable
Level 2/ 50,000 to 2.5 million	Optional	SAQ AOC mandatory (unless submitting a ROC AOC); scan mandatory with certain SAQ types
Level 3/* 10,000 to 50,000	Optional	SAQ AOC optional (mandatory if required by American Express); scan mandatory with certain SAQ types
Level 4/* 10,000 or less	Optional	SAQ AOC optional (mandatory if required by American Express); scan mandatory with certain SAQ types

* For the avoidance of doubt, Level 3 and Level 4 Merchants need not submit Validation Documentation unless required at American Express' discretion, but nevertheless must comply with, and are subject to liability under all other provisions of these Data Security Requirements.

American Express reserves the right to verify the completeness, accuracy, and appropriateness of your PCI Validation Documentation. American Express may require you to provide additional supporting documents for evaluation in support of this purpose. Additionally, American Express has the right to require you to engage a QSA or PFI.

Table 8-2: Service Provider

Validation Documentation		
Report on Compliance Attestation of Compliance (ROC AOC) – (Annual Requirement)	Self-Assessment Questionnaire Attestation of Compliance (SAQ AOC) – (Annual Requirement)	Approved Scanning Vendor External Network Vulnerability Scan Summary (ASV Scan) – (90 Day Requirement)
The Report on Compliance documents the results of a detailed onsite examination of your equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed or transmitted. The Report on Compliance must be performed by: • a QSA or • you and attested by your chief executive officer, chief financial officer, chief information security officer, or principal The AOC must be signed and dated by a QSA or Internal Security Assessor (ISA) and the authorised level of leadership within your organisation and provided to your Merchant Service Provider at least once per year.	The Self-Assessment Questionnaires allow self-examination of your equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed, or transmitted. There are multiple versions of the SAQ. You will select one or more based on your Cardholder Data Environment. The SAQ may be completed by personnel within your Company qualified to answer the questions accurately and thoroughly or you may engage a QSA to assist. The AOC must be signed and dated by the authorised level of leadership within your organisation and provided to your Merchant Service Provider at least once per year.	An external vulnerability scan is a remote test to help identify potential weaknesses, vulnerabilities, and misconfigurations of internet-facing components of your Cardholder Data Environment (e.g., websites, applications, web servers, mail servers, public-facing domains, or hosts). The ASV Scan must be performed by an Approved Scanning Vendor (ASV). If required by the SAQ, the ASV Scan Report Attestation of Scan Compliance (AOSC) or executive summary including a count of scanned targets, certification that the results satisfy PCI DSS scanning procedures, and compliance status completed by ASV, must be submitted to your Merchant Service Provider at least once every 90 days. ROC or AOC are not required to provide an AOSC or ASV Scan executive summary unless specifically requested. For the avoidance of doubt, Scans are mandatory if required by the applicable SAQ.

Visit pcisecuritystandards.org for:
- Lists of Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs)
- Self Assessment Questionnaires (SAQs)
- The Attestation of Compliance (AOC) and Attestation of Scan Compliance (AOSC)

Action 3 - Complete the Validation Documentation

Level 1, Level 2, and certain Level 3 and Level 4 Merchants must submit the Validation Documentation marked "mandatory validation documentation" in the table in Action 2.

- Level 1 Merchants' Validation Documentation must include the AOC from the annual onsite security assessment report.
- Level 2 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 2 Merchants may choose to submit the AOC from the annual onsite security assessment report if preferred.

- Level 3 Merchants and Level 4 Merchants are not required to submit Validation Documentation unless requested by American Express (but must comply with, and are subject to liability under, all other provisions of this policy).

Action 4 – Send the Validation Documentation to your Merchant Services Provider

All Merchants required to participate in the American Express PCI Compliance Programme must submit the Validation Documentation marked "mandatory" in the tables in Action 2.

You must submit your Validation Documentation to your Merchant Services Provider as instructed by them. If you have general questions about the programme 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 authorised 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.

8.7.1 Merchants Not Compliant with PCI DSS

If you are not compliant with the PCI DSS, then you must submit one of the following documents:

- An Attestation of Compliance (AOC) including "Part 4. Action Plan for Non-Compliant Status"
- A PCI Prioritized Approach Tool Summary and Attestation of Compliance (PASAOC)

Each of the above documents must designate a remediation date, not to exceed twelve (12) months following the document completion date, in order to achieve compliance. You must submit the appropriate document(s) 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".

8.7.2 Non-Validation Fees and Termination of Agreement

American Express and your Merchant Services Provider have the right to impose non-validation fees and terminate the Agreement if you do not fulfil these requirements or fail to submit 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.

8.8 Reserved

8.9 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.

For further information about American Express Data Security requirements, please visit www.americanexpress.com.au/dsr

For information about PCI Security Standards, LLC:

- PCI Data Security Standards
- Self Assessment Questionnaire
- List of Qualified Security Assessors
- List of Approved Scanning Vendors
- List of PCI Forensic Investigators

www.pcisecuritystandards.org

AMERICAN EXPRESS

Fraud Prevention

9

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 programmes that can help to mitigate the chances of fraud on American Express Cards and reduce this cost to your business.

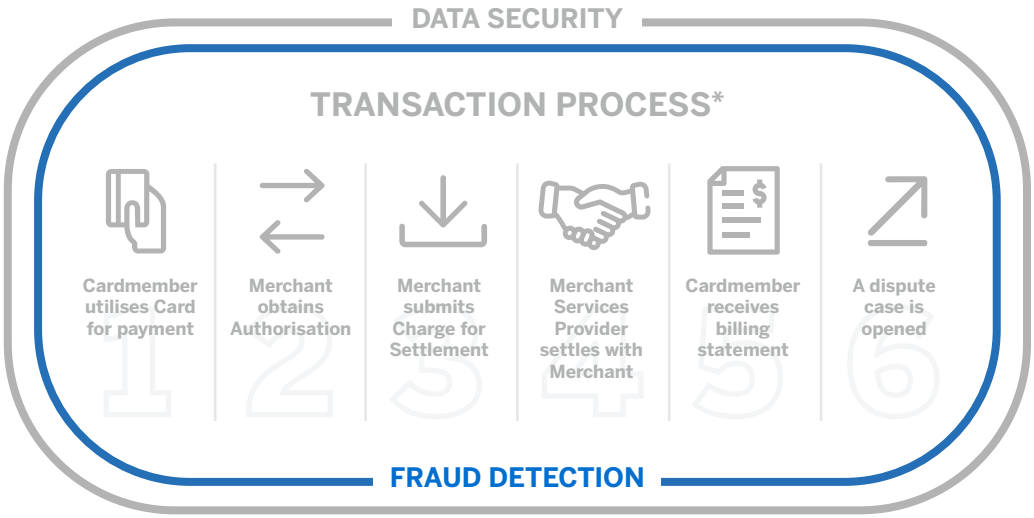
Some Merchants may not be eligible to participate in the full suite of fraud tools and fraud liability shift programmes offered. Additionally, American Express may, in our sole discretion, immediately suspend or terminate a Merchant from using any fraud tool or participation in any fraud liability shift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

This chapter 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 Transaction Process

Our primary strategy for combating fraudulent Card use is to address it at the point of Authorisation. To accomplish this, we work with Merchants and their Merchant Services Providers to implement best practices and fraud mitigation tools.

While fraud usually is thought of as a deceptive act at the point of sale, detection can actually occur during any stage in the Transaction process. For this reason, "fraud detection", as depicted in the following graphic, applies throughout the entire Transaction process.



* This graphic is for illustration purposes only and is not to be construed as limiting or waiving American Express' rights with respect to Cardmember Information or other information.

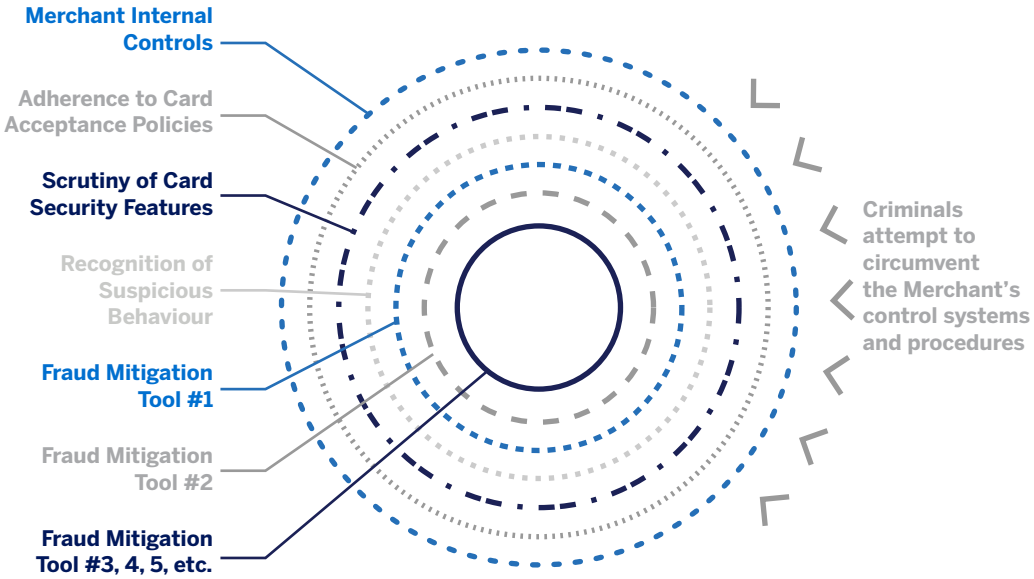
9.3 Strategies for Deterring Fraud

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.

The following illustration compares data captured during a standard Card Not Present Charge (left) with the amount of data that can be captured when fraud mitigation tools are implemented (right).

DATA CAPTURED

Card Not Present Charge: **Standard**	Card Not Present Charge: **Our Suite of Fraud Mitigation Used**
Card: 37XXXXXXXXX2009 **Amount:** $257 **Merchant:** Internet Merchant XXXXXXXX01	**Card:** 37XXXXXXXXX2009 **Name:** C.F. Frost **Amount:** $257 **Merchant:** Internet Merchant XXXXXXXX01 **CID Number:** XXXX **AAV:** 2213 E Main **AAV Name:** C.F. Frost **AAV Phone:** 814-880-1234 **Email:** cffrost@ispprovider.net **IP Address:** 122.22.15.18 **Host Name:** PHX.QW.AOL.COM **Ship to Address:** Level 26, 45 Mount Street, North Sydney NSW 2060 **Ship to Phone:** 415.555.5555 **Ship to Country:** Australia

9.4 Card Acceptance Policies

A critical component in your overall fraud mitigation strategy is to follow your Merchant Services Provider's operating instructions, including our Card acceptance procedures as defined in Chapter 4, "Transaction Processing". These procedures can also serve as a your first line of defence against potential fraud. The additional layers of fraud mitigation mentioned previously can supplement this line of defence.

9.5 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 our 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.

The four-digit CID Number is located on the front of the Card where the three-digit CSC is located on the back of the Card. These codes are considered Card security features and can validate that the Card is present for a Charge. You should prompt your customers for the four-digit CID Number.

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 9.7, "Prepaid Card Security Features" and Section 9.9, "Travelers Cheque and Gift Cheque Security Features".

9.5.1 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 your 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 programme, educate yourself and all your personnel on how to identify a potentially altered Card.

9.6 Recognising Suspicious Activity

No single factor by itself is indicative of risk; however, when a combination of factors is present during a Transaction, additional scrutiny is warranted. If you have any doubts of suspicious activity call in a Code 10.

Diligently scrutinising behaviours and circumstances can help prevent you from being victimised 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.

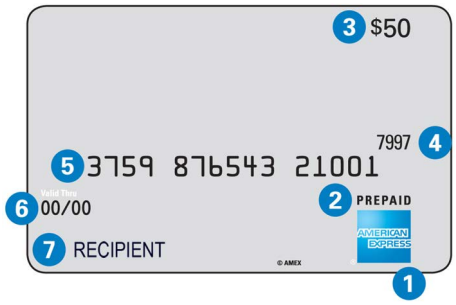
If you suspect Card misuse, follow your internal store policies, and immediately call your Merchant Services Provider with a Code 10. **Never put yourself or your employees in unsafe situations, nor physically detain or harm the holder of the Card.**

9.7 Prepaid Card Security Features

You are responsible for following all our Prepaid Card acceptance procedures in Section 4.4.7, "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.

9.8 Recognising Suspicious Activity for Prepaid Cards

American Express recommends that you follow the procedures in the preceding Section 9.6, "Recognising 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.

9.9 Travelers Cheque and Gift Cheque Security Features

We offer a variety of cheque verification solutions to help you avoid accepting fraudulent cheque products. For more details about Authorisation solutions, contact us via email at tconlineAuthorizations@aexp.com.

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 4.4.8, "Processing Travelers/Gift Cheques". American Express also recommends that you follow the procedures in the preceding Section 9.6, "Recognising 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 recognise an authentic Cheque.

9.10 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 2.4, "Compliance with the Technical Specifications"), and
- you provide high quality data in the Authorisation 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.

9.10.1 Card Not Present Fraud Tools

Table 9-1: Card Not Present Fraud Tools

	Card Identification (CID) Verification Tool	Automated Name and Address Verification	Email Verification	Billing Phone Number Verification	Enhanced Authorisation
Description	You request the four-digit CID number printed on the Card from the Cardmember and send it with the Authorisation request to the Issuer. Issuer compares the CID number provided with that on file for the Card and, based on the comparison, returns a match code to you.	You request name and address information from the Cardmember at the point of sale, and provide this information electronically during Authorisation, through your POS terminal. Issuer compares the name and address information you provided with Cardmember's billing records and provides a response code indicating full, partial, or no match.	You request email address from the Customer at the point of sale, and provide this information electronically during an Authorisation. Issuer compares the email address you provided with email addresses on file at American Express and returns a match result.	You request billing phone number from the Customer at the point of sale, and provide this information electronically during an Authorisation. Issuer compares the phone number you provided with Cardmember billing phone number and returns a match result.	Provides additional data elements in Authorisation requests describing the transaction and enabling a more informed Authorisation decision.
Purpose	Helps to ensure that the person placing the order actually has the Card in their possession and is not using a stolen Card Number.	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.	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.	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.	Helps mitigate fraud before a Transaction is authorised by analysing key data elements submitted with Authorisation requests. Data elements include shipping address, transaction origin, and airline ticket details.
How To Implement	Contact your Merchant Services Provider	Contact your Merchant Services Provider	Contact your Merchant Services Provider	Contact your Merchant Services Provider	Contact your Merchant Services Provider

9.10.2 Card Present Fraud Tools

Table 9-2: Card Present Fraud Tools

	Card Identification (CID) Verification Tool	Track 1	Chip	Terminal ID	Code 10
Description	You request the four-digit CID number printed on the Card from the Cardmember and send it with the Authorisation request to the Issuer. Issuer compares the CID number provided with that on file for the Card and, based on the comparison, returns a match code to you.	POS terminal captures data encoded in the Track 1 of the Magnetic Stripe and sends it to the Issuer with the Authorisation request. Issuer compares information in track to information on file and sends approval decision.	Chip technology uses an embedded microchip to encrypt card information, making it more difficult for unauthorised users to copy or access the data. Data can only be accessed when the Card is inserted into a chip-enabled terminal.	Captures a numeric identifier uniquely assigned to each POS device and sends it to the Issuer with each Authorisation request.	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.
Purpose	Helps to ensure that the person making the purchase is not using an altered or duplicated Card.	Can signal tampering and alteration of the Card's Magnetic Stripe.	Provides enhanced protection against fraud from lost, stolen, and counterfeit Cards.	Helps detect high risk patterns of a particular POS device.	Enables your Merchant Services Provider to speak with an American Express Authoriser on a card present transaction they assess as high risk.
How To Implement	Contact your Merchant Services Provider	Contact your Merchant Services Provider	Contact your Merchant Services Provider	Contact your Merchant Services Provider	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 Authorisation 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.

AMERICAN EXPRESS

Risk Evaluation

10

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) if we determine or have reason to believe, in our sole discretion, that you meet any of the following criteria:

- Participation as a Merchant on our Network or acceptance of Cards (or both) by you or any of your Establishments may cause us 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 or any of your Establishments are involved (or knowingly participate or have participated) in a fraudulent or illegal activity.
- You or any of your Establishments 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.

Additionally, American Express may terminate acceptance of Cards by you or any of your Establishments if:

- You are listed on the U.S. Department of Treasury, Office of Foreign Assets Control, Specially Designated Nationals and Blocked Persons List (available at www.treas.gov/ofac).
- You are listed on the U.S. Department of State's Terrorist Exclusion List (available at www.state.gov).
- You are located in or operating under license issued by a jurisdiction identified by the U.S. Department of State as a sponsor of international terrorism, by the U.S. Secretary of the Treasury as warranting special measures due to money laundering concerns, or as noncooperative with international anti-money laundering principles or procedures by an intergovernmental group or organisation of which Australia is a member.
- Your verifiable physical address is not located in Australia.
- You or any of your Establishments fall into one of the following categories and/or accept Transactions for the prohibited activities displayed in the following table:

Table 10-1: Prohibited Business Types

Prohibited Business Types	Description	Merchant Category Code (MCC)
Airlines & air carriers (including charter airlines)	All airline and air carrier merchants, including charter airlines.	3000-3302; 4511
Bail/bail bond	A sum of money paid by a criminal defendant to be released from jail under the condition that they appear for court appearances.	9223

Prohibited Business Types	Description	Merchant Category Code (MCC)
Bankruptcy services	A company or agency that is in the business of recovering money owed on delinquent accounts or supporting the bankruptcy process. Examples include: bankruptcy lawyers and bankruptcy debt collection services.	—
Bullion	Bulk metal in bars or ingots. Examples include: • Gold, silver, platinum, palladium bullion • Gold, silver, platinum, palladium bars • Precious metals	—
Car rental agencies	Branded and unbranded car rental agencies (e.g., Avis, Budget, Hertz).	7512
Cash at Point of Sale/Cash on Card	Cash-like transactions from financial and non-financial institutions. Examples include: money orders, post offices, funding source for payroll.	6051
Charities	A non-profit, non-political organisation that collects donations, including fundraising.	8398
Check cashing/guarantee	A business that provides customers with a way to turn a check into cash without having to rely on a bank account.	—
Child pornography	An individual or entity providing or associated with the visual depiction of a minor engaged in obscene or sexually explicit conduct, whether made or produced by electronic, mechanical, or other means.	—
Collection agencies	A company that lenders use to recover funds that are past due. Examples include: debt collection agencies, factoring companies, and liquidators.	7322

Prohibited Business Types	Description	Merchant Category Code (MCC)
Commercial leasing	A business that conveys land, real estate, equipment, or other property to another for a specified time in return for regular periodic payment. Examples include commercial real estate and commercial vehicles, such as trucks and marine vessels. **This does not include residential Real Estate Agents and Managers – Rentals (MCC 6513).**	—
Credit financing	A merchant that provides financing to customers, earning revenue on that financing via fees and/or interest. Examples include: credit cards, personal loans, student loans, car loans, mortgage payments.	6010 6011 6012 6051
Credit restoration	A service aimed at improving credit ratings by disputing errors and outdated claims with credit bureaus.	—
Cryptocurrency	Digital asset recognised as a medium of exchange, unit of account and/or store of value that employs blockchain technology and cryptography to submit, authenticate, and verify Transactions.	6051
Dating and escort services	A business, agency, or person who, for a fee, provides or offers an escort.	7273
Debt repayment (past due or defaulted)	A company collecting payment of overdue debt. Examples include: payment to a collection agency, factoring company, liquidator, or insolvency practitioner/lawyer.	7322
Digital file hosting (Cyberlockers)	Online data hosting services that provide remote storage space within a secure storage architecture that can be accessed globally over the Internet. Cyberlockers can also be referred to as 'online storage' or 'cloud storage'.	—

Prohibited Business Types	Description	Merchant Category Code (MCC)
Door-to-door sales	Unsolicited individual (who may go from door to door) selling goods and/or services with immediate payment expected. Examples include: magazine subscriptions, satellite dish sales, security systems, and solar panels.	5963
Foreign exchange	A business or financial institution that has the legal right to exchange one currency for another currency. Examples include: airport kiosk bank.	6051
Gambling	The wagering of money or something of value on an event with an uncertain outcome, with the primary intent of winning money or material goods. Examples include: • Regulated (real money) betting, including casino, poker, sports betting, lottery tickets • Advance-deposit wagering, including horse/dog racing • Fantasy sports • Skill-based, pay-to-play games that award monetary prizes • Games of chance that are not free to enter and award monetary prizes • Government-owned and other lotteries • Gambling chips • Gambling credits	7800 7801 7802 7995 9406

Prohibited Business Types	Description	Merchant Category Code (MCC)

Indirect acceptor models	A payment intermediary that contracts with American Express to facilitate payments to multiple, eligible third-party End Beneficiaries. The Indirect Acceptor accepts the Card, but does not send Card information to the End Beneficiary and pays eligible End Beneficiaries using another method, such as bank transfer, cheque, or wire.
	Examples include:
	• Digital Wallet Operator offering any of the following payment functionality to allow Cardmembers to make purchases or transfer funds through one or more methods:
	  • Staged Back-to-Back Transaction
	  • Peer to Peer (P2P) Transaction
	  • Stored Value Transaction (sometimes called Top Up)
	• Bill Payment Provider
	• Marketplaces
	• Instalment Payment Transactions (sometimes called Buy Now Pay Later).
		—

Investments	A purchase made for speculative purposes, or with the intent of future profit or appreciation. Examples include, but are not limited to securities (stocks, bonds, commodities, and mutual funds) wine with delivery that exceeds one (1) year from purchase, and investment on futures.	—
Licensed insolvency practitioners	A professional intermediary in insolvency procedures.	—
Lodging – Hotels, Motels, Resorts (including "branded" Central Reservation Services)	Branded and unbranded lodging establishments (e.g., Best Western, Hilton, Marriott).	7011

Prohibited Business Types	Description	Merchant Category Code (MCC)
Marijuana-related businesses	Any individual or entity that manufactures, processes, distributes, or dispenses marijuana, or byproducts or derivatives of marijuana, whether for recreational or medicinal purposes, and whether or not subject to a governmental licensing regime.	—
Massage parlours	A business or person that provides massage services.	7297
Multi-level marketing / pyramid selling (also referred to as Direct Marketing – Inbound/Outbound Telemarketing)	A sales system that uses one or more of the following practices: • Participants pay money for the right to receive compensation for recruiting new participants. • A participant is required to buy a specific quantity of products, other than at cost price for the purpose of advertising, before the participant is allowed to join the plan or advance within the plan. • Participants are knowingly sold commercially unreasonable quantities of the product or products (this practice is called inventory loading). • Participants are not allowed to return products on reasonable commercial terms.	5966 5967
Online adult entertainment	A business or entity that provides internet adult digital content.	—
Payday lending	A company that lends customers money at high interest rates on the agreement that the loan will be repaid when the borrower receives their next pay-check.	—
Person-to-Person Payments	A service that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile device.	6538
Pharmacies (Card Not Present)	Online pharmacies selling prescription drugs and products.	—

Prohibited Business Types	Description	Merchant Category Code (MCC)
Political party donations	Contributions, funds, goods, or services raised to promote the interests for a national, state, or local political party, candidate, or campaign.	8651
Prostitution	A person or business providing sexual services in return for payment.	—
Real Estate Down Payments	An initial payment when the real estate is purchased on credit.	6012 6051
Securities Brokers/Dealers	A business or individual that is licensed to buy, sell, and broker securities, stocks, bonds, commodities, and mutual funds.	6211
Steamships & cruise lines (incl. onboard cruise shops)	Steamship and cruise line merchants.	4411
Telemarketing – travel related	A business that telemarkets travel related products or services or other travel arrangements.	5962
Timeshares	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.	7012
Tobacco and smokeless tobacco retailers (Card Not Present)	Tobacco, smokeless tobacco, and e-cigarette retailers that submit Card Not Present Transactions. Example includes: vaping products.	—
Travel agencies and tour operators	A business that provides travel information and booking services.	4722
Virtual currency	Digital money not authorised or adopted by a government. Issued and controlled by its developers and used and accepted among members of a specific virtual community.	6051
Wire transfers in-person (not online)	A business that specialises in the transfer of money from one location to another.	4829

This list is not exhaustive and American Express may, in its sole discretion, consider other prohibited merchant categories and modify this list accordingly.

Please contact your Merchant Services Provider for more information on prohibited merchant categories and activities.

Mixed Business

If any segment of your or any of your Establishments business falls into any of the aforementioned business types, you and your Establishments must not accept the Card for those Transactions. If you or any of your Establishments accept the Card for these Transactions, American Express will exercise Chargeback. American Express may also place you or any of your Establishments in one of American Express' Chargeback programmes, cancel or disentitle acceptance of Cards by you or any of your Establishments, and/or request termination of your merchant agreement with your Merchant Services Provider (or take any combination of these actions).

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
- 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,
- requiring corrective action by the Merchant, 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 we determine put us at risk and/or whose business has excessive occurrences of fraud.

If we determine, in our sole discretion, that you meet the criteria for one or more of the High Risk Merchant categories, we may place you in a Chargeback programme and/or terminate Card acceptance.

We consider you to be "high risk" if you meet at least one criterion in the following table:*

Table 10-2: High Risk Merchants

Category	Description
High risk industry	Your type of business has had historically high occurrences of fraud and Disputed Charges with us or as compared to other similarly situated Merchants (or both). Examples of high risk industries include: internet electronic delivery and facilitators.

Category	Description
Performance	You have recent high occurrences of fraud that present an excessive risk to us. You have had high occurrences of fraud and/or high fraud amounts for a number of consecutive months.
Cancelled derogatory	Your Agreement was cancelled due to unsatisfactory activity.
Fictitious	You accept Cards fraudulently.
Prohibited	You are not eligible to accept the Card on the American Express Network. For prohibited criteria see Section 10.2, "Prohibited Merchants".

* This list is not exhaustive and American Express may, in its sole discretion, consider other criteria as high risk and modify this list accordingly.

10.3.2 Fraudulent, Deceptive, or Unfair Business Practices, Illegal Activities, or Prohibited Uses of the Card

If we determine or have reason to believe, in our sole discretion, 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 our Cardmembers; or in business practices that we deem fraudulent, deceptive, and/or unfair, we may take corrective action on you, which may include but is not limited to:

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

Table 10-3: Risk Management Definitions

Factoring	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).
Collusion	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.
Marketing fraud	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 unauthorised sales to a valid Card account).
Identity theft	Identity theft is the assumption of another person's identity to gain access to their finances through fraudulent Merchant setup or fraudulent Transactions.

Illegal activities, fraudulent (other than marketing), unfair or deceptive business practices, or prohibited uses of the Card	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, "Prohibited Uses of the Card"), American Express may apply the corrective actions listed above.

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

AMERICAN EXPRESS

Chargebacks and Inquiries

11

11.1 Introduction

This chapter describes how American Express processes Chargebacks and Inquiries.

Highlights of this chapter include:

- a discussion of the American Express Disputed Charge process,
- a review of Chargeback and Inquiry reasons,
- an overview of the American Express Chargeback policies, and
- tips for avoiding Chargebacks and Inquiries, and preventing fraud.

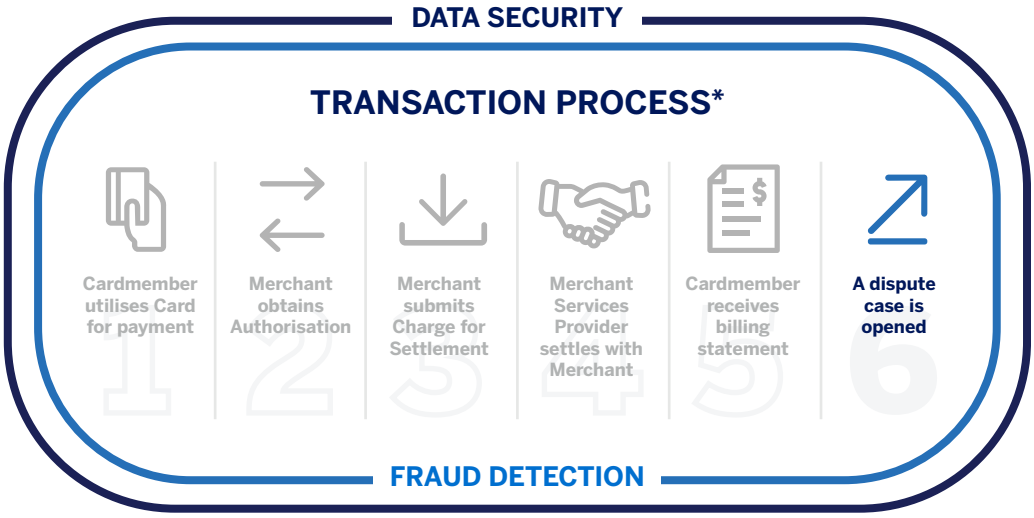
11.2 Transaction Process

Charges may be disputed for a variety of reasons. In general, most Disputed Charges stem from:

- Cardmember dissatisfaction with some aspect of the purchase, (e.g., a failure to receive the merchandise, duplicate billing of a Charge, incorrect billing amount),
- an unrecognised Charge where the Cardmember requests additional information, or
- actual or alleged fraudulent Transactions.

If a Cardmember disputes a Charge, American Express opens a case. We may also open cases when Issuers or the Network initiates disputes. If a case is opened, we may initiate a Chargeback to you immediately or send you an Inquiry.

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

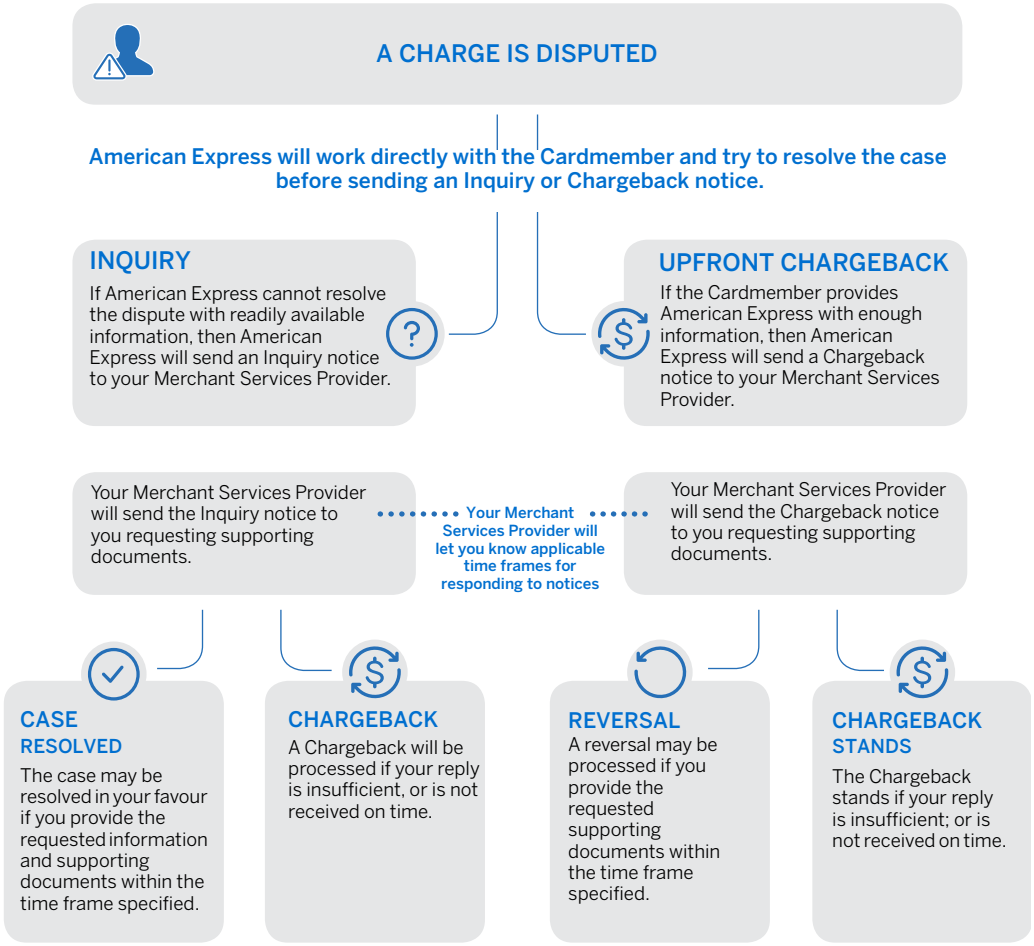


* This graphic is for illustration purposes only and is not to be construed as limiting or waiving American Express' rights with respect to Cardmember Information or other information.

11.3 Disputed Charge Process

11.3.1 Mapping out the Disputes Process

Most disputes begin when a Cardmember contacts American Express with a question or problem with a specific Transaction. Disputes can be complicated. This step-by-step flowchart can help make the process clearer, so you know what to expect if a Charge is disputed.



11.3.2 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.

11.3.3 American Express has Chargeback rights:

- whenever Cardmembers bring Disputed Charges, as described in this chapter, 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 sending incomplete or incorrect Transaction Data in 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 Authorisation 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.

11.4 How We Chargeback

We may Chargeback by (i) deducting, withholding, recouping from, or otherwise offsetting against our payment to your Merchant Services Provider for a Charge you submitted; or (ii) reversing a Charge for which we have not paid you. Our failure to demand payment does not waive our Chargeback rights.

Your Merchant Services Provider may have additional rights and remedies with respect to Disputed Charges. Please contact your Merchant Services Provide for more information on their Chargeback procedures.

11.5 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 agreement in writing 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.

AMERICAN EXPRESS

Specific Industries

12

12.1 Introduction

This chapter 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 obtained the Cardmember's approval in writing on the agreement/bill of sale 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 their 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 authorising 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 their 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 authorising 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 6.5, "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 6.5, "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 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 Australian Dollars.
- Your physical address in Australia.
- 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.

12.5 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.

12.6 Oil/Petroleum

In some countries, additional policies and procedures are applicable to Merchants classified in the oil/petroleum industry.

For information about CATs, see Subsection 4.2.2, "Unattended Terminals".

If you are classified in the oil and petroleum industry, your Merchant Services Provider may place you in the Fraud Full Recourse Programme if you accept Charges originating at a CAT gas pump. For information about Customer Activated Terminals, see Section 4.2.2, "Unattended Terminals".

12.6.1 Requirements

You must:

- Submit dealer location data along with each Authorisation request and each Submission file. Dealer location data consists of your business:
  - dealer number (store number)
  - name
  - street address
  - city
  - postal code

12.6.2 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-Authorisation request at your CAT based on a good faith estimate of the final charge amount.
- For higher Charges such as diesel, adjust the pre-Authorisation amount to accommodate the higher Charges.
- Set your CAT gas pumps to shut off when they reach the pre-Authorisation amount.
- Request a separate Authorisation for purchases that exceed the original pre-Authorisation amount.

AMERICAN EXPRESS

Glossary of Terms

Advance Payment Charge
A Charge for which full payment is made in advance of Merchant providing the goods and/or rendering the services to the Cardmember.

Affiliate
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
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
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
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
American Express Australia Limited.

American Express Brand
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
(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
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
(i) any law, statute, regulation, ordinance, or subordinate legislation in force from time to time to which Merchant or its Merchant Services Provider is subject, (ii) the common law as applicable to them from time to time, (iii) any court order, judgement, or decree that is binding on them, and (iv) any directive, policy, rule, or order that is binding on them and that is made or given by a regulator or other government or government agency of any Territory, or other national, federal, commonwealth, state, provincial, or local jurisdiction.

Application-initiated Transaction
A Transaction initiated by an electronic device (including but not limited to, a mobile telephone, tablet, or wearable device) utilising a merchant software application within the electronic device.

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

Assured Reservation Programme
A programme 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 Programme is available to the following industries: hotel, trailer park/campground, vehicle, aircraft, bicycle, boat, equipment, motor home, and motorcycle rentals.

Authorisation/Authorised
The process by which a Merchant obtains an Approval for a Charge in accordance with the Agreement.

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

Batch
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 (if obtained), '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
A four-digit number printed on the Card. See Section 5.10, "Card Identification (CID) Number" for additional information.

Card Not Present Charge
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
The unique identifying number that the Issuer assigns to the Card when it is issued.

Card Present Charge
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 Programme
A programme that permits Cardmembers to charge the payment of an Advance Payment Charge to their Cards when a deposit is required.

Cardmember (also referred to as Card Member)
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
Any information about Cardmembers and Transactions, including, but not limited to, Transaction Data, and Cardmember name, addresses, Card Numbers, and CID Numbers.

Cardmember-Initiated Transaction (CIT)
A Transaction which involves the direct participation of the Cardmember.

Charge
A payment or purchase made on the Card, excluding any payment or purchase that you route to a network other than the American Express Network.

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

Charge Record
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 charged back to you, 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
An integrated microchip embedded on a Card containing Cardmember and account information.

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

Code 10
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 Authorisation.

Collusion
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 Evaluation".

Compelling Evidence
Additional types of documentation provided by the Merchant to demonstrate the Cardmember participated in the Transaction, received goods or services, or benefited from the Transaction. Please contact your Merchant Services Provider for additional information regarding Compelling Evidence.

Consumer Device Cardholder Verification Method (CDCVM)
An Issuer approved, American Express recognised Cardholder Verification Method whereby the Cardmember's credentials are verified on a Mobile Device.

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

Covered Parties
Any or all of your employees, agents, representatives, subcontractors, processors, Service Providers, providers of your point-of-sale (POS) equipment or systems, or payment processing solutions, Entities associated with your American Express merchant account, and any other party to whom you may provide Cardholder Data or Sensitive Authentication Data (or both) access in accordance with the Agreement.

Credentials-on-File
Any Cardmember account data, including but not limited to PAN or Token, that is stored by Merchants. Merchants may store Credentials-on-File to initiate Merchant-Initiated Transactions and Cardmembers may use their Credentials-on-File to initiate Cardmember-Initiated Transactions.

Credit
The amount of the Charge that Merchant refunds to Cardmembers for purchases or payments made on the Card.

Credit Record
A record of Credit that complies with American Express' requirements.

Cryptocurrency
A digital asset recognised as a medium of exchange, unit and/or store of value that employs blockchain technology and cryptography to submit and verify Transactions.

Customer Activated Terminal (CAT)
An unattended POS System (e.g., gasoline pump, vending machine, check-out kiosk). Sometimes referred to as an unattended terminal in our materials.

Data Security Requirements (DSR)
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.com.au/dsr.

Debit Card
Any Card that accesses a demand deposit, current, savings, or similar account, excluding any Card bearing a Third Party Issuer's name or Marks without the Marks of American Express. A Transaction is settled from the accessed account. A Debit Card is not a Prepaid Card.

Decline
A message denying the Merchant's request for Authorisation.

Delayed Delivery Charge
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 Goods or Services
Digital merchandise or services downloaded or accessed via Internet or another file transfer process (e.g., movies, applications, games, virus scanning software).

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

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

Digital Wallet Magnetic Secure Transmission Transaction
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
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
A Charge about which a claim, complaint, or question has been brought.

E-commerce Transaction
The purchasing of physical or Digital Goods or Services using the Internet, an application, or electronic network on either a personal computer or Mobile Device including, but not limited to, Internet Transactions or Digital Wallet Application-initiated Transactions.

Entity
A corporation, partnership, sole proprietorship, trust, association, or any other legally recognised entity or organisation.

Establishments
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 Authorisation
An Authorisation for an estimated amount that differs from the final submission amount.

Estimated Lodging Charge
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
The rental rate multiplied by the rental period reserved by the Cardmember, plus taxes and any known incidental amounts.

Expiration Date
The month and year on which a Card expires (sometimes referred to as "valid thru" or "active thru" date).

Expresspay
An American Express programme that enables Contactless transactions.

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

Fraud Full Recourse Programme
One of American Express' Chargeback programmes.

High Risk Merchant
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 Programme.

Immediate Chargeback Programme
One of American Express' Chargeback programmes.

In-Person Charge
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
A request for information about a Disputed Charge.

Instalment Payment Transaction
A transaction that represents a single instalment payment in a series of instalments over a fixed period.

Internet Electronic Delivery
The delivery of Digital Goods or Services purchased on the internet via an internet or an electronic network download or another file transfer process (e.g., images or software download).

Internet Order
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.

Introductory Offer
A free or reduced cost trial, promotion, or other similar offer for a limited period of time that allows Cardmembers to try a product or service before the Card is billed for the regular price of the product or service.

Issuer
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.

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

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

Merchant
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
An account established by Merchant Services Provider upon entering into an Agreement with a Merchant.

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

Merchant-Initiated Transaction (MIT)
A Transaction based on a prior agreement between Cardmember and Merchant that is initiated by the Merchant without direct participation from the Cardmember, through Merchant use of Account Data on File.

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

Merchant Operating Guide
The *American Express Merchant Operating Guide*, which is available at www.americanexpress.com.au/merchantopguide/

Merchant Services Provider
An Entity authorised under the American Express OptBlue® Programme to accept Charges from a Merchant pursuant to an Agreement or a Payment Facilitator authorised to accept Charges from a Merchant. These services may include, but are not limited to, processing transactions, facilitating authorisations 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
An Issuer approved and American Express recognised 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)
A generic term for a system comprising of a commercial off-the-shelf mobile computing device with cellular or Wi-Fi data connectivity (such as a phone, tablet, or laptop) that may be used in conjunction with a Card-reading peripheral to accept contact and/or Contactless Transactions.

Network—See American Express Network or Network.

No PIN Programme
A programme that allows an Establishment to not request a signature or PIN from Cardmembers. See Section 4.2.1, "No PIN Programme" for additional information.

Original Transaction Identifier (O-TID)
A Transaction Identifier (TID) generated by the AEGN during an Authorisation Request for a Cardmember-Initiated Transaction which links all subsequent Merchant-Initiated Transactions back to the original Cardmember-Initiated Transaction.

Other Payment Products
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 Programme
One of American Express' Chargeback programmes.

Payment Facilitator
A provider of Payment Services, formerly referred to as Payment Aggregator, Payment Service Provider or PSP in American Express materials.

Payment Services
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)
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
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 Authorisations or to collect Transaction Data, or both.

Prepaid Card
A Card that is marked "Prepaid" or bearing such other identifiers used by American Express from time to time.

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

Property Damage Fee
An additional sum of money that may be charged to a Cardmember in relation to property damage that has been sustained to the rental accommodation (or property therein) or rental equipment (or part thereof) during the stay or rental period for which the Merchant is able to demonstrate the genuine costs incurred or required to repair or replace the property or equipment.

Recurring Billing
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).

Rental Establishments
Long-term rentals used as primary residences.

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

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

Settlement
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
The use of multiple forms of payment (e.g., prepaid products, cash, American Express Card) for a single purchase.

Submission
The collection of Transaction Data sent to American Express.

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

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

Telecommunications
Communication services, including personal communication services; cellular, paging, long distance, etc.

Third Party Issuer
A third party Card Issuer whose Cards are accepted by the Merchant under the Agreement.

Token
A surrogate value that replaces the Card Number.

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

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

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

Transmission Data
The same as Card Data except for the requirements to include: Cardmember name, Expiration Date, the Cardmember's signature (if obtained); and the words "No Refund" if the Merchant has a no refund policy.

URL
Uniform Resource Locator, a term used to identify an internet address.

Valid Dates
The dates on the Card that indicate the first and last date the Card can be used to make purchases.

We, our and us
American Express Australia Limited.

You and your
The individual or Entity that executes the Agreement with a Merchant Services Provider (sometimes called the "Merchant" or "Establishment" in this *Merchant Operating Guide).*