AMERICAN EXPRESS

Merchant Regulations

International

April 2026

DON'T *do business* WITHOUT IT℠

AMERICAN EXPRESS

This document was published on April 17, 2026 and is in full force and effect as of such date, except for changes that will become effective on October 16, 2026, or another date, as specified herein.

20260406

AMERICAN EXPRESS

Summary of Changes

Icons

Important updates are listed in the Summary of Changes Table and also indicated in the *Merchant Regulations* with a change bar. A change bar is a vertical line, usually in the left margin, that identifies added or revised text. Only substantial changes in the *Merchant Regulations* with potential impacts to a Merchant's operational procedures are indicated with a change bar as shown in the left margin.

Removed text is highlighted with a trash can icon placed in the margin next to any significant deletion of text, including sections, tables, paragraphs, notes, and bullet points. Removed text is referenced in this Summary of Changes using the section numbering from the previous publication to avoid confusion.

Blue lines bordering paragraphs indicate region-specific information.

Summary of Changes Table

Important updates are listed in the following table and are also indicated in the *Merchant Regulations* with a change bar.

Chapter	Section/Subsection	Description
Entire document		Minor updates throughout the *Merchant Regulations*, including capitalisation.
Chapter 1, "Introduction"	Section 1.2, "Changes in the Merchant Regulations"	• Added new provision outlining Merchant obligations and acceptance process for changes to the *Merchant Regulations*. • Revised language to address scheduled and unscheduled changes to the *Merchant Regulations*.
Chapter 2, "Transaction Processing"	Section 2.6.1.1, "Clearing Records"	Clarified Merchants' requirement to provide a copy of the original or electronic Clearing Record.
	Section 2.6.2.1, "General Requirements"	Clarified Merchants' requirement to provide a copy of the original or electronic Clearing Record.
Chapter 3, "Authorisation"	Section 3.3.1, "Estimated Authorisation"	Updated the Estimated Authorisation procedures for multi-month car rental periods.
	Section 3.3.2, "Estimated Charge Amount"	Updated the Authorisation Validity Period for Car Rentals, Lodging, and Steamships & Cruise Lines.
Chapter 6, "Indirect Acceptors"	Section 6.3.1, "Additional Requirements for Bill Payment Providers"	Expanded the restricted Merchant Category Codes (MCCs) for Airlines and Air Carriers and Car Rentals referenced in Table 6-3: Excluded Industries for Bill Payment Providers Facilitating Business Payments.
	Section 6.3.2, "Additional Requirements for Instalment Payment Transactions"	Expanded the restricted MCCs for Airlines and Air Carriers and Car Rentals referenced in Table 6-4: Excluded Industries for Instalment Payment Transactions.

Chapter	Section/Subsection	Description
	Section 6.3.4, "Excluded Industries for Indirect Acceptors"	Expanded the restricted MCCs for Airlines and Air Carriers and Car Rentals referenced in Table 6-5: Excluded Industries for Indirect Acceptors.
Chapter 8, "Regulations for Specific Industries"	Section 8.2.6, "Payment Facilitators"	Expanded the restricted MCCs for Airlines and Air Carriers and Car Rentals.
Glossary		Added/modified definitions.

AMERICAN EXPRESS

Table of Contents

AMERICAN EXPRESS

List of Tables

AMERICAN EXPRESS

Introduction

1

1.1 About the Merchant Regulations

a. The *Merchant Regulations* set forth the operational policies and procedures governing your acceptance of the American Express® Card. In the event of any conflict between the *Merchant Regulations* and Applicable Law, the requirements of law govern. The *Merchant Regulations* contain global policies that apply to your Establishments and country-specific policies that apply to your Establishments located in the specific country listed. In the event of any conflict between the global policies and country-specific policies, the requirements of the country-specific policies take precedence. In order to ensure that these policies and procedures are kept up to date, we will periodically update them as set out in these *Merchant Regulations*.

1.2 Changes in the Merchant Regulations

a. We reserve the right to change the *Merchant Regulations* (including by adding new terms or deleting or modifying existing terms) by providing the *Merchant Regulations* in electronic form at www.americanexpress.com/InternationalRegs or its successor website (as made available by us). Any future changes to the *Merchant Regulations* are set out in the Notification of Future Changes section of the *Merchant Regulations*. Revised versions of the *Merchant Regulations* will be published twice per year, in April and October, and the revised versions will be available on the website referred to above. In exceptional circumstances, it may be necessary to make changes to the *Merchant Regulations* outside of this cycle. If this is the case, we will notify you of any changes in accordance with your Agreement. No changes shall be effective less than thirty (30) days from the date of notice unless another effective date is necessary to comply with Applicable Law and is specified in the notice. If you do not accept a change to the *Merchant Regulations* communicated in accordance with this section, you must terminate acceptance of the American Express Card pursuant to the Agreement before the effective date of the change. By continuing to accept the American Express Card after the effective date of the change, you agree to be bound by the revised terms of the *Merchant Regulations*.

1.3 Prohibited Uses of the Card

a. Merchants must not accept the Card for any of the following:

- **i.** Any Transactions in the prohibited industries. Refer to Subsection 8.2.1, "Prohibited or Restricted Industries".
- **ii.** Transaction 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 a Merchant. This includes costs or fees over the normal price of the Goods or Services (plus applicable taxes) that the Cardmember has not specifically approved.
- **iii.** Submitting Clearing Records for amounts that do not correspond to the value of the Goods or Services provided. This restriction does not apply in the case of Partial Authorisations. Refer to Section 4.2, "Submitting Charges" and Subsection 3.3.5, "Partial Authorisation" for additional details on Partial Authorisations related requirements. Examples of forbidden Transactions include purchases at Merchants by the owners (or their family members) or employees contrived for cash flow purposes, or payments that Merchants have accepted in order to advance cash to Cardmembers in connection with the Transaction.
- **iv.** Capturing or processing Clearing Records on behalf of any other Merchant or non-Merchant, except as provided in Subsection 8.2.6, "Payment Facilitators" and Chapter 6, "Indirect Acceptors".
- **v.** Submitting more than one (1) Clearing Record for Goods or Services purchased in a single Transaction, except for airlines, cruise lines, and lodging Merchants, Split Shipment Transactions of Goods.
- **vi.** Splitting a single Charge by creating two (2) or more Clearing Records on a single Card for a single Charge in order to avoid Authorisation.
- **vii.** Unlawful/illegal activities, fraudulent business transactions or when providing the Goods or Services is unlawful/illegal.
- **viii.** Damages, losses, penalties, or fines of any kind, except as provided in Subsection 8.2.4.1, "Vehicle Rental",
- **ix.** Overdue amounts or amounts covering returned, previously dishonoured or stop-payment checks (e.g., where the Card is used as a payment of last resort),

x. Amounts that represent repayment of a cash advance including, but not limited to, payday loans, pawn loans, or payday advances, other items of which American Express notifies the Merchant.

1.4 Compliance with our Specifications

a. You must comply with our *Technical Specifications*, any other (or different) requirements of our local operating centres, and other documents required to support Authorisation, Submission, Communication, and Connectivity as found at www.americanexpress.com/merchantspecs, which may change from time to time. The American Express Network publishes the *Technical Specifications* twice a year, in April and October. Technical changes to implement or support, as well as any certification requirements and/or compliance dates, will be communicated six (6) months prior to publication in a Notice of Specification Changes (NOSC). Technical Bulletins may also be used to communicate changes occurring outside of the April and October publication schedule. Failure to comply with the *Technical Specifications* may impact your ability to successfully process Authorisation requests or Transactions (or both).

1.4.1 Merchant Category Codes

a. You must provide us with an accurate and complete description of your business so we can assign a Merchant Category Code (MCC) and industry classification to your Merchant Number. You must use the most accurate MCCs in all Authorisations and Submissions. If you have multiple, distinct businesses that may qualify for more than one MCC, we will assign the appropriate MCCs and Merchant Numbers. If you have multiple businesses, but a distinction between them is unclear, then we will assign the MCC most closely representing your primary business.

b. 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.

c. We reserve the right to require and implement corrections to the MCC assignments and use in our sole discretion and without advance notice.

1.4.2 Compliance with Payment Products Terms and Conditions

a. We offer various payment processing solutions and products. If you choose to utilise one or more such products, you and any third parties you enlist 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 Regulations*, the terms and conditions of the payment processing product will prevail. All products and services may not be available to all Merchants.

1.5 The American Express Bank Identification Numbers

a. Merchants may request American Express Bank Identification Number (BIN) files only for purposes specified in the BIN terms and conditions (T&C).

b. Merchants must agree with the BIN T&C located within the website listed below before BIN file request is fulfilled.

c. Requests for American Express BIN files are available at www.americanexpress.com/merchantspecs and can be accessed by entering your user ID and password.

d. **Note:** BIN files may be updated periodically.

1.6 Compliance with our Data Security Operating Policy

a. You must comply with our Data Security Operating Policy, as set forth in the Introduction to DSOP and Standards for Protection. You agree to be bound by and accept all provisions in that policy (as changed from time to time) as if fully set out herein and as a condition to your agreement to accept the Card. Under that policy you have additional (i) indemnity obligations if you suffer a Data Incident and (ii) obligations based on your Transaction volume, including providing to us documentation validating your compliance with the PCI DSS. Your data security procedures for the Card shall be no less protective than for other payment products you accept.

AMERICAN EXPRESS

Transaction Processing

2

2.1 Introduction

a. This chapter details American Express' policy regarding Merchants' Card acceptance and Charge processing procedures.

2.2 General Requirements

a. To accept the Card for Charges, Merchants must clearly and conspicuously:
   i. Disclose all material terms of sale before to obtaining an Authorisation.
   ii. Inform Cardmembers at all points of interaction (e.g., sales conducted in person, over the internet, mobile or via mail or telephone order) what Entity is making the sales offer, so that the Cardmember can clearly distinguish the Merchant from any other party involved in the interaction (e.g., a vendor of Goods or provider of Services the Merchant may engage, or another Merchant seeking to conduct business with the Cardmember).

b. The Transaction Data a Merchant collects to facilitate the Charge must be, or have been, provided directly to the Merchant by the Cardmember.

c. Merchants must not accept or have accepted Transaction Data from, nor shall Merchants provide or have provided Transaction Data to, any third parties other than their Covered Parties for the purposes of processing a Transaction authorised by a Cardmember.

2.3 In-Person Charges

a. In-Person Charges refer to Charges in which the Card and Cardmember are present at the Point of Sale (POS).

b. For all In-Person Charges, and regardless of the amount of the Transaction or the Floor Limit, the Merchant must:
   i. Have the Card present, except for Split Shipment Transactions of Goods.
   ii. Not accept a Card that is visibly altered, mutilated, or presented by anyone other than the Cardmember.
   iii. Ensure the Card is processed by a chip-capable POS device if the Card is chip-enabled or swiped through electronic data capture equipment.
   iv. Obtain an Authorisation.
   v. Notify the Cardmember immediately if the Card is declined.
   vi. Obtain a Cardmember signature if the Merchant chooses or is required by Applicable Law. Refer to Subsection 2.3.1, "Obtaining Signature for In-Person Charges". Signature must be obtained for the following MCCs:
      - 6010 – Financial Institutions – Manual Cash Disbursements
      - 6051 – Non-Financial Institutions – Foreign Currency, Cryptocurrency, Money Orders (not Wire Transfer), Scrip, and Travellers Checks
   vii. If applicable, obtain the Personal Identification Number (PIN) to authenticate the Cardmember. No PIN is required to authenticate the Cardmember if the Merchant and the Transaction qualify under the No Signature/No PIN Programme. Refer to Subsection 2.3.2, "No Signature/No PIN Programme" for more information.
   viii. Ensure that the Card is being used within the valid dates shown on the face of the Card. If only an Expiration Date appears on the Card, the date of Charge must be prior to this date.
   ix. Complete a single Transaction Receipt for the entire amount of the Charge Transaction, except for airlines, cruise lines, and lodging Merchants, and Split Shipment Transactions of Goods. The Merchant may accept separate forms of payments for the same Transaction (i.e., Cardmember wishes to pay for part of the Transaction with the Card and the balance with another form of payment).
   x. Match the Card Account number and Expiration Date appearing on the front of the Card to the same information on the back of the Card and/or printed on the terminal receipt by the POS terminal.

xi. Identify Merchants using Customer Activated Terminals (CATs) in the Authorisation Request message via the applicable indicator. All Transactions at CATs must be Authorised. Refer to the *Technical Specifications*, and Subsection 2.3.4, "Customer Activated Terminals" for more information.

xii. For keyed Transactions, key in the Card Account number, Expiration Date, and for embossed Cards, obtain an imprint of the Card so that the Card and Merchant data are legible on the Clearing Record. No imprint is required if the Transaction meets any of the conditions for exclusion for ISO 4527 – Missing Imprint (see Table 5-17: Missing imprint (ISO 4527 / F10)). "Signature on file" is not an acceptable signature. A pencil rubbing or photocopy of the Card is not considered proof of a valid imprint.

xiii. If suspicious of a Card or Cardmember, the Merchant is instructed to call American Express with a Code 10.

c. If the Merchant processes Charges manually or the electronic capture device is inoperable, the Merchant must Imprint the Card onto a Clearing Record that conforms to American Express' specifications as described in Subsection 2.6.1, "Charge Transactions". The Merchant may provide handwritten Card details on the Clearing Record only when:

i. A POS device is not available, and

ii. A Card imprinter is not available if a flat-printed Card is presented.

d. Failure to obtain an Imprint may subject the Transaction to an ISO 4527 – Missing Imprint Chargeback (see Table 5-17: Missing imprint (ISO 4527 / F10)) unless the Transaction meets any of the conditions for exclusion.

e. The Merchant is at risk of a Chargeback if a Charge proves to be fraudulent and the Merchant completes the Transaction when the Cardmember is present and does not have their Card.

f. In all cases, Merchants will be liable for fraudulent Charges arising from a failure to comply with American Express' Card acceptance procedures.

2.3.1 Obtaining Signature for In-Person Charges

a. If a Merchant chooses or is required by Applicable Law, to obtain a Cardmember signature on a manual imprint, printed, or electronic In-Person Charge, the Merchant must:

i. Obtain signature on the Transaction Receipt.

ii. If possible, verify that the name indicated by the signature is the same as the name on the Card.

iii. Verify that the signature on the Transaction Receipt matches the signature on the Card; except in the case of Prepaid Cards that may not include a signature.

b. If a Merchant requests Cardmember signature and the signature panel on the Card is blank, in addition to requesting an Authorisation, the Merchant must:

i. Require the Cardmember to sign the Card.

ii. Ask the Cardmember for an official form of identification bearing a signature, such as a driver's license or passport.

iii. Compare the signature on the Card to the official form of identification for consistency.

iv. If the Cardmember refuses to sign the Card, or if the signature is not consistent with the official form of identification provided by the Cardmember, the Transaction should not be completed.

c. Merchants may provide the Cardmember's written signature, or a signature obtained electronically on a POS device (for In-Person Charges) on the Clearing Record.

2.3.2 No Signature/No PIN Programme

a. The No Signature/No PIN (Cardholder Verification Method) Programme allows a Merchant to process a Card Present Transaction without obtaining the Cardmember's signature or PIN as required in Section 2.3, "In-Person Charges" unless required by Applicable Law, if all the following requirements are met:

i. The Merchant is in a designated country listed in the "No Signature/No PIN Programme and Contactless Transaction Limits" table in the *Technical Specifications*.

ii. The Transaction amount is equal to or less than the amount listed in the "No Signature/No PIN Programme and Contactless Transaction Limits" table in the *Technical Specifications*.

iii. The Merchant's MCC is not listed in Table 2-1: Ineligible Merchant Category Codes for the No Signature/No PIN Programme*.

iv. The Transaction is Authorised.

v. The indicator provided in the Submission request must indicate a Card Present and Cardmember Present Transaction.

b. The established threshold for Charges to qualify under the No Signature/No PIN Programme for Contactless and all other In-Person Charges is set forth in Section 8.1, "Country Specific Policies".

Table 2-1: Ineligible Merchant Category Codes for the No Signature/No PIN Programme*

MCC Code	Description
4814	Telecommunications Services
4816	Computer Network/Information Services
4829	Wire Transfers and Money Orders
4899	Cable and Other Pay Television Services
5542	Automated Fuel Dispensers
5964	Direct Marketing – Catalog Merchants
5966	Direct Marketing – Outbound Telemarketing Merchants
5967	Direct Marketing – Inbound Telemarketing Merchants
6010	Financial Institutions – Manual Cash Disbursements
6011	Financial Institutions Automated Cash Disbursements
6051	Non Financial Institutions – Foreign Currency, Money Orders (not Wire Transfer), Scrip, and Travellers Checks
7273	Dating and Escort Services
7297	Massage Parlours
7375	Information Retrieval Services
7393	Detective Agencies, Protective Agencies and Security Services

* Merchants in these MCCs must obtain a PIN if a Chip and PIN Card is presented at the Chip and PIN enabled POS device.

c. Obtaining Cardmember signature on Card Present Transactions is optional to complete a Clearing Record, and at the Merchant's discretion, unless required by Applicable Law.

d. **EEA/UK:** Save as expressly set out elsewhere, Transactions conducted within the European Economic Area (EEA) or United Kingdom (UK) will not qualify for the No CVM Programme unless it is a Contactless Transaction at an Expresspay enabled POS system.

2.3.3 Contact Chip Card Charges

a. For Chip and PIN Cards, the Merchant must ensure that their POS systems are capable of accepting Chip Cards, and, if applicable, are capable of PIN verification.

b. When presented with a Chip Card, the Card must be inserted into the reader of the POS system that must capture Chip Card Data (unless the Charge is processed through Contactless Technology, in which case the Merchant must follow the steps outlined in Subsection 2.3.5, "Contactless Chip Cards").

c. For Transaction amounts equal to or greater than the Contact Limit, and for Transactions that do not qualify for the No Signature/No PIN Programme (Subsection 2.3.2, "No Signature/No PIN Programme"), the POS system should advise the Cardmember to enter the PIN (a "Chip and PIN Transaction") or any other CVM, excluding Cardmember signature. Upon such advice, the Merchant must ensure that the Cardmember completes the applicable CVM when prompted by the POS system. Failure to capture the PIN may result in Chargebacks for lost, stolen, or non-received fraudulent In-Person Charges (see Fraud Liability Shift – Lost/Stolen/Non-Received (ISO 4799) in Subsection 5.6.3, "Fraud"). If the Merchant chooses to obtain a Cardmember signature, see Subsection 2.3.1, "Obtaining Signature for In-Person Charges".

d. If the Merchant is unable to complete a Chip Card Transaction due to a technical problem, the POS system should show an error message and either decline the Transaction or direct the Merchant to capture full magnetic stripe data by following the procedure for non-Chip Card Transactions (Section 2.3.6, "Non-Chip Cards").

e. If a Merchant swipes a Chip Card through the POS system when no technical problem exists, or at any time manually keys a Charge into the POS system, the Transaction may be declined and, if it is not, American Express may have Chargeback rights for fraudulent In-Person Charges (see Fraud Liability Shift – Counterfeit (ISO 4798) in Subsection 5.6.3, "Fraud").

f. In addition, Merchants will be liable for any losses that American Express may suffer and American Express will have Chargeback rights for fraudulent In-Person Charges, and/or we may terminate the Agreement, if:

   i. The POS system has not been upgraded to accept Chip Cards; or

   ii. The Merchant and their Processing Agent do not have the ability to capture and send Chip Card Data; or

   iii. The Merchant has not certified the POS with American Express to accept Chip Transactions or Chip and PIN Transactions..

g. If Merchant's POS is a capable Chip and PIN POS system that can process Chip Cards and a Chip Card is presented, American Express may exercise Chargeback for counterfeit, lost, stolen, or non-received fraud if a Chip Card with PIN functionality is presented and the Charge is not submitted as a Chip and PIN Charge because at the time of the Transaction, the Merchant's capable Chip and PIN POS was not configured to process the Chip and PIN Charge.

h. American Express will not exercise Chargeback for counterfeit, lost, stolen, or non-received fraud for Fallback Transactions, if after inserting the Chip Card, the Merchant's POS prompts the Merchant to complete the Transaction by swiping the Magnetic Stripe of the Card, provided that all applicable Card acceptance steps are followed as outlined in Subsection 2.3.6, "Non-Chip Cards".

i. If a Merchant is presented with a Chip Card and manually keys the Transaction, the Merchant may be subject to counterfeit, lost, stolen, or non-received Chargebacks in the event of a fraud dispute.

2.3.4 Customer Activated Terminals

a. Merchants must ensure that all (new, replaced, or existing) unattended chip-enabled offline or online capable Customer Activated Terminals (CATs) (except terminals using Contactless, Transit Access Terminals (TATs)) support "No CVM" for Contactless and AEIPS Transactions.

b. Merchants must ensure that the terminal examines the Chip CVM list in priority order and selects the first CVM supported by both the terminal and the Chip. Refer to the *Technical Specifications* for more information. In order to process Transactions through CATs, the Merchant must:

   i. Include in all requests for Authorisation the full magnetic stripe stream or Chip Card Data;

   ii. 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;

   iii. Follow any additional Authorisation procedures that American Express may provide the Merchant, if the Merchant accepts the Card at a CAT that is part of, or attached to, a fuel dispenser, or electric vehicle charging station;

   iv. Ensure that the CAT notifies the Cardmember if the Transaction is declined, where technically feasible.

c. If a CAT is not configured for Chip or Chip and PIN Transactions, then the Merchant may still accept the Card. However, if the Merchant does so, the Merchant will be liable for any losses and American Express will have Chargeback rights for fraudulent In-Person Charges made with lost, stolen, non-received, and /or counterfeit Chip Cards. See Subsection 2.3.3, "Contact Chip Card Charges" and Subsection 2.3.2, "No Signature/No PIN Programme".

2.3.5 Contactless Chip Cards

a. Merchants accepting Contactless payments are exempt from the requirements set forth in Section 2.3, "In-Person Charges", except for the following requirements:

- **i.** Merchants must complete a single Clearing Record for the entire amount of the Transaction. Merchants may accept separate forms of payment for the same Transaction (i.e., Cardmember wishes to pay for part of the Transaction with the Card and the balance with another form of payment).
- **ii.** Merchants must comply with the Card and Contactless terminal requirements as defined in the *Technical Specifications*.

b. The Merchant is at risk of a Chargeback if a Charge proves to be fraudulent and the Merchant completes the Transaction when:

- **i.** The Cardmember is present and does not have their Card or Mobile Device.
- **ii.** The Cardmember does not sign the Transaction Receipt, if required.

c. When a Cardmember presents a Chip Card or Mobile Device for a Contactless Transaction:

- **i.** If the Charge amount is equal or less than the Contactless Transaction limit and there is no CVM, the Merchant must capture the Charge Data using a Contactless reader and obtain an Authorisation.
- **ii.** If the Charge amount is over the Contactless Transaction limit and there is no CVM, or if the Merchant is unable to complete a Contactless Transaction, or if prompted by the POS, the Merchant must follow the process outlined in Section 2.3.3, "Contact Chip Card Charges" or Subsection 2.3.6, "Non-Chip Cards" as appropriate.

d. A Consumer Device Cardmember Verification Method (CDCVM) is required for Digital Wallet Contactless-initiated Transactions if both the Mobile Device and the Merchant's POS are capable of performing the verification. Merchants must create a Clearing Record for these Charges as described in Section 2.6, "Charge and Credit Clearing Records", including an indicator that the Transaction is a Digital Wallet Contactless-initiated Transaction.

e. Merchants should comply with the most current American Express Contactless-enabled POS requirements to ensure POS acceptance of Digital Wallet Contactless-initiated Transactions.

f. American Express will not exercise missing Imprint, counterfeit, lost, stolen, or non-received fraud Chargebacks for Contactless or Digital Wallet Contactless-initiated Transactions if the Merchant successfully verifies the Cardmember via CDCVM and meets all the criteria and requirements listed above. This does not apply to Disputed Charges involving other dispute reasons (e.g., Goods or Services disputes).

g. Merchants are required to comply with requests from American Express for written responses to Disputed Charges related to fraud for Contactless or Digital Wallet Contactless-initiated Transactions.

2.3.5.1 Merchant-Presented Quick Response

a. Merchants accepting Merchant Presented Quick Response (MPQR) are exempt from the requirements set forth in Section 2.3, "In-Person Charges", Subsection 2.3.2, "No Signature/No PIN Programme", and Section 2.4, "Card Not Present Charges", and must instead meet the requirements below.

b. If a Merchant has the ability to process MPQR Transactions, the Merchant must:

- **i.** Display the Quick Response (QR) code, which can be dynamic or static, for scanning by the Cardmember;
- **ii.** Have the Cardmember use their Mobile Device to scan the MPQR code;
- **iii.** Ensure the MPQR code is not altered or tampered with;
- **iv.** Receive a notification that the Transaction has been approved and check the Transaction amount is correct before providing the Goods or Services. If the Merchant does not receive the notification, they should contact American Express to confirm the status of the MPQR Transaction;
- **v.** Contact American Express or decline the Transaction if the Merchant is suspicious of the Cardmember or receives notification from American Express to do so; and
- **vi.** Retain records of MPQR Transactions (e.g., a notification from American Express, an invoice, or other documentation of the Transaction).

2.3.6 Non-Chip Cards

a. For In-Person Charges where the Card is not a Chip Card, the POS provides instructions for a Merchant to swipe, and the Merchant must:

i. Swipe the Card through the POS system (unless the Charge is processed through Contactless Technology, in which case the Merchant must follow the steps outlined in Subsection 2.3.5, "Contactless Chip Cards").

ii. Follow the steps outlined in Section 2.3, "In-Person Charges".

2.4 Card Not Present Charges

a. For Charges made by mail, telephone, or Internet, where the Card is not present, Merchants must comply with the following procedures:

i. Obtain an Authorisation for every Charge.

ii. Complete a Clearing Record as described in Section 2.6, "Charge and Credit Clearing Records" including an indicator designating both the Transaction as Card Not Present and the applicable Transaction type (i.e., mail, telephone, internet, recurring billing, standing Authorisation). Refer to the *Technical Specifications* for more information.

iii. All Internet Transactions must be submitted electronically and have a zero (0) Floor Limit.

iv. Use any separate Merchant Numbers provided by American Express for Internet Transactions.

v. Obtain the following information to proceed with the Transaction:

- Cardmember's name
- Card Account number or Token
- Expiration Date
- Cardmember's billing address
- Card Identification Number (CID) (optional)
- Shipping or delivery address

vi. If the order is shipped or delivered more than seven (7) days after the original Authorisation, obtain a new Authorisation before shipping or delivering the order. Charges may not be submitted for payment until the order is shipped. The Transaction Date of the Charge is the date the Goods are shipped or delivered.

vii. For Card Not Present Charges where Goods are to be collected from a designated store, Merchants must establish a process to ensure that the Goods are collected either by the Cardmember who placed the order, or by an authorised third party designated by the Cardmember at the time of placing the order;

viii. Immediately notify the Cardmember if the Transaction is declined.

b. If the Goods are to be collected by the Cardmember, the Card must be presented by the Cardmember upon collection and the Transaction should be treated as an In-Person Charge and comply with the provisions provided in Section 2.3, "In-Person Charges".

2.5 Other Charges

2.5.1 Advance Payments

a. Advance Payments allow Cardmembers to authorise Charges to their Card prior to Goods and/or Services being delivered when such a Payment is required (e.g., custom orders for Goods, entertainment / ticketing, tuition, room and board, fees at institutions of higher education, travel).

b. If a Merchant either requires or provides Cardmembers the option to make an Advance Payment, they must:

i. Obtain Authorisation;

ii. Complete a Clearing Record.

iii. State their full cancellation and refund policies, clearly disclose their intent and obtain written consent from the Cardmember to bill the Card for an Advance Payment before requesting an Authorisation. The Cardmember's consent must include:

a. Their agreement to all the terms of the sale (including price and any cancellation and refund policies); and

b. A detailed description and the expected delivery date of the Goods and/or Services to be provided (including, if applicable, expected arrival and departure dates);

c. If the Advance Payment is a Card Not Present Charge, the Merchant must also:

i. Ensure that the Clearing Record contains the words "Advance Payment" or "Advance Deposit"; and

ii. Within twenty-four (24) hours of the Charge being incurred, provide the Cardmember written confirmation of the following:

- The Advance Payment Charge
- The Charge amount
- Details of the Merchant's cancellation/refund policy
- The confirmation number (if applicable)
- A detailed description and expected delivery date of the Goods and/or Services to be provided (including expected arrival and departure dates, if applicable)

d. If a Merchant cannot deliver Goods and/or Services, and if alternate arrangements cannot be made, the Merchant must immediately issue a Credit for the full amount of the Advance Payment Charge that relates to the Goods or Services which cannot be delivered or fulfilled.

e. In addition to American Express' 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 the Merchant's favour based upon unambiguous terms contained in the terms of sale to which the Merchant obtained the Cardmember's written consent.

f. Specific industries may have additional requirements to process Advance Payments. Refer to Section 8.2, "Industry Specific Policies" for more information.

2.5.2 Aggregated Transactions

a. This section explains the requirements for Transactions processed by Merchants conducting business over the Internet and explains the general policies and rules that apply to the processing of multiple purchases as a single Aggregated Transaction.

b. Aggregated Transactions cannot exceed $15 (USD or local currency equivalent) and are considered Card Not Present. Transactions in excess of $15 USD are not eligible for Aggregated Transaction processing.

c. Merchants must comply with the following when processing Aggregated Transactions:

i. Prior to the Transaction being authorised, disclose that individual purchases may be aggregated and obtain the Cardmember's consent to combining such purchases into one (1) Aggregated Transaction.

ii. Each individual purchase or refund (or both) that comprises the Aggregated Transaction must be incurred under the same Establishment Number and on the same Card;

iii. Obtain an Authorisation in advance of a Transaction being aggregated;

iv. Create a Clearing Record for the full amount of the Aggregated Transaction, as indicated in Section 2.6, "Charge and Credit Clearing Records";

v. Provide the Cardmember with a confirmation containing:

a. The date, amount, and description of each individual purchase or refund (or both)

b. The date and the amount of the Aggregated Transaction.

vi. Submit a Clearing Record for each Aggregated Transaction within the timeframe outlined in Section 4.2, "Submitting Charges" and Section 4.3, "Submitting Credits"; and

vii. Ensure that a meaningful description of the products and/or Services that comprise a single Aggregated Transaction is included as part of the Submission to American Express.

2.5.3 Credentials-on-File

a. Merchants must obtain Cardmember consent before storing Cardmember credentials. American Express recommends that Merchants process an initial Authorisation upon receiving Cardmember consent to store credentials.

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

2.5.4 Merchant-Initiated Transactions

a. 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.

b. Merchants must adhere to the requirements in Section 2.4, "Card Not Present Charges", when processing MITs.

c. Merchants must obtain Cardmember consent to initiate an MIT, or a series of MITs. This may occur before or after storing a Cardmember's credentials.

d. American Express recommends that Merchants:

i. Only submit MITs after initial Cardmember-initiated Transactions (CIT).

ii. Submit MITs with the applicable Transaction indicators and data elements in the Authorisation Request as described in the *Technical Specifications*.

e. **EEA/UK:** For Merchants located in the EEA or UK, all of the requirements outlined in this Subsection 2.5.4, "Merchant-Initiated Transactions" are mandatory, even if listed above as recommended.

2.5.5 Recurring Billing

a. Recurring Billing is a payment method whereby the Cardmember expressly consents and authorises the Merchant to Charge the Cardmember's Card Account on a periodic basis for Goods or Services, agreed in writing by the Cardmember (e.g., membership fees to health clubs, magazine subscriptions, insurance premiums). Each Recurring Billing Charge may be for a variable or a fixed amount. Merchants should adhere to the requirements in Subsection 2.5.4, "Merchant-Initiated Transactions", when processing Merchant-Initiated Transactions for Recurring Billing.

b. Before submitting the first Recurring Billing Charge the Merchant must:

i. Disclose all material terms of the Recurring Billing Transaction Agreement to the Cardmember including, but not limited to, the duration of the Recurring Billing agreement, the amount, and frequency with which the Recurring Billing Transactions will be submitted, and including, if applicable, the fact that Recurring Billing Charges will continue until the option is cancelled by the Cardmember;

ii. Ensure Recurring Billing Transactions contain the Recurring Billing Indicator in the Authorisation and Submission messages.

iii. Submit an Authorisation Request for all Recurring Billing Transactions (see Section 2.4, "Card Not Present Charges" for details).

iv. Obtain the Cardmember's express consent to process Recurring Billing Transactions on their Card;.

v. Obtain the Cardmember's express consent to renewals.

vi. Retain documentation that validates the Cardmember's consent to process Recurring Billing Transactions. This documentation must be maintained for the length of the Recurring Billing agreement or two (2) years from the last Recurring Billing Transaction, whichever is longer.

vii. Obtain the Cardmember's name, the Card Account, signature (if applicable), Card expiry date, the Cardmember's billing address, and a statement confirming their consent for the Merchant to charge their Card for the same or different amounts at specified or different times;

viii. Provide the Cardmember written confirmation (e.g., email or facsimile) of the Transaction, including all material terms of the option and details of the cancellation or refund policy, within twenty-four (24) hours of incurring the first Recurring Billing Transaction;

ix. Comply with any instructions of which American Express may reasonably notify the Merchant;

x. Notify the Cardmember that they are able to discontinue Recurring Billing Transactions at any time and provide contact details for cancelling Recurring Billing Transactions;

xi. Provide a simple and expeditious cancellation process for Recurring Billing Transactions. This cancellation process must be clearly and conspicuously disclosed to the Cardmember at the time of their consent to submit Recurring Billing Transactions on their Card.

xii. Notify the Cardmember that they can revoke their consent to process Recurring Billing Transaction on their Card.

c. Any changes to the Recurring Billing Transaction agreement between the Merchant and the Cardmember must be made in accordance with the agreement with the Cardmember and Applicable Law. Such changes must take effect before submitting any subsequent Recurring Billing Transactions on the Card.

d. If the material terms of the Recurring Billing Transaction change after Submission of the first Recurring Billing Charge, the Merchant must 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.

e. The method the Merchant uses to secure the Cardmember's consent must contain a disclosure that the Merchant may receive updated Card Account information from the financial institution issuing the Cardmember's Card. The Merchant must retain evidence of such consent for two (2) years from the date the Merchant submits the last Recurring Billing Charge.

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

i. At least ten (10) days before submitting each Charge; and

ii. Whenever the amount of the Charge exceeds a maximum Recurring Billing Charge amount specified by the Cardmember.

g. In addition to other Chargeback rights, American Express may exercise Chargeback for any Charge that does not meet the requirements outlined in this Subsection 2.5.5.1, "Introductory Offers". American Express may also exercise Chargeback rights for any Charge of which the Merchant has notified the Cardmember and to which the Cardmember does not consent, or if the Merchant processes Recurring Billing Charges after the Cardmember, or if American Express has notified the Merchant that the Cardmember has withdrawn consent for Recurring Billing Charges.

h. The cancellation of a Card constitutes immediate withdrawal of that Cardmember's consent for Recurring Billing Charges. American Express is not required to notify the Merchant of such cancellation, nor have any liability to the Merchant arising from such cancellation. The Merchant must provide the Cardmember with a method of cancellation of Recurring Billing Charges that is clear, simple, and consistent with Applicable Law and must discontinue the Recurring Billing Transactions immediately if requested to do so by a Cardmember directly, through American Express, or the Card Issuer. If a Card Account is cancelled, or if a Cardmember directly through American Express or the Card Issuer withdraws consent to Recurring Billing Charges, the Merchant is responsible for arranging another form of payment (as applicable) with the Cardmember (or former Cardmember).

i. If a Cardmember withdraws consent but the Recurring Billing Merchant continues to submit Recurring Billing Transactions, American Express may reject the Transaction or the Merchant may be subject to Chargebacks.

j. If the Agreement is terminated for any reason, then the Merchant shall notify all Cardmembers for whom they have submitted Recurring Billing Charges of the date when the Merchant will no longer be accepting the Card. At American Express' option the Merchant will continue to accept the Card for up to ninety (90) days after any termination takes effect.

k. The Merchant will permit American Express to establish a hyperlink from American Express' website to their website (including its home page, payment page, or its automatic/recurring billing page) and list their customer service contact information.

l. **EEA/UK:** If the Merchant is located in the EEA or UK, and in relation to a Card issued in the EEA or UK, if the Merchant submits a Recurring Billing Charge for an amount which was not specified in full when the Cardmember provided consent to Recurring Billing Charges and the Merchant does not obtain the Cardmember's consent specifically in relation to the full exact amount of such Charge, American Express will have Chargeback rights for the full amount of the Charge for a period of one hundred and twenty (120) days

from submission of the applicable Charge, and thereafter for any disputed portion of such Charge (up to and including the full amount). If the Cardmember consents to an adjusted Charge amount, we may exercise our Chargeback rights accordingly. Nothing in this paragraph will prejudice our Chargeback rights generally in relation to Recurring Billing Charges.

2.5.5.1 Introductory Offers

a. Merchants who offer Recurring Billing that include an Introductory Offer to Cardmembers must comply with the following requirements in addition to those stated in this Subsection 2.5.5.1, "Introductory Offers":

- **i.** 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 the first Recurring Billing Transaction occurs;
- **ii.** Obtain the Cardmember's express consent accepting the terms and conditions of the Introductory Offer;
- **iii.** Send the Cardmember a confirmation notification in writing upon enrolment in the Introductory Offer; and
- **iv.** Send the Cardmember a reminder notification in writing before submitting the first Recurring Billing Transaction is set to occur, that allows the Cardmember a reasonable amount of time to cancel.

2.5.6 Delayed Delivery

a. For a Delayed Delivery Charge, the Merchant must:

- **i.** Clearly disclose intent and obtain written consent from the Cardmember to perform a Delayed Delivery Charge before you request an Authorisation;
- **ii.** Clearly mark the first Charge Clearing Record as a "deposit" and the second Charge Clearing Record as a "balance".
- **iii.** Obtain a separate Authorisation for each of the Delayed Delivery Charges on their respective Charge dates;
- **iv.** Submit the "balance" Transaction only after the Goods have been shipped or delivered, or Services are rendered;
- **v.** Submit each Delayed Delivery Charge Clearing Record within seven (7) days of the Charge being incurred. The Charge will be deemed "incurred":
  - **a.** For the deposit: on the date the Cardmember agreed to pay the deposit for the purchase
  - **b.** For the balance: on the date the Goods are shipped or provided or Services are rendered
- **vi.** Submit and obtain Authorisation for each part of a Delayed Delivery Charge under the same Establishment Number;
- **vii.** Adhere to the requirements in Subsection 2.5.4, "Merchant-Initiated Transactions", when processing Delayed Delivery Charges; and
- **viii.** Treat deposits on the Card no differently than deposits on all Other Payment Products.

2.5.7 Multicurrency (MCCY)

a. A Merchant transacting on the MCCY Platform must comply with the terms of the Agreement and these *Merchant Regulations*.

b. A Merchant shall be permitted to submit Charges and receive Settlements in one or more Alternative Currencies, provided that the Merchant shall not convert the currency of the original Transaction to another currency when requesting an Authorisation or submitting the Transaction (or both). A Merchant must submit and settle Charges in any Alternative Currency via the MCCY Platform using American Express' standard file format as set forth in the *Technical Specifications*. American Express reserves the right to modify the Merchant's access to the MCCY platform, currencies supported by the MCCY Platform, and the *Technical Specifications* in its sole discretion from time to time.

India: No Merchant shall submit via the MCCY Platform any Charge for Goods or Services provided in India on any Card issued in India.

c. For Internet Order Charges only, a Merchant shall be permitted to submit Charges and receive settlements in one or more Alternative Currencies, subject to the following:

   i. The Merchant shall require the Cardmember to use a Selected Currency. Once a Selected Currency is chosen, the Selected Currency must remain the same for that Transaction. In addition, the Merchant must disclose to the Cardmember any associated foreign exchange rate, mark-up, or fee, and indicate that the foreign exchange rate used by the Merchant may not be the same as foreign exchange rates available in the marketplace.

   ii. Once the Selected Currency is chosen, all prices displayed to the Cardmember, and the Transaction itself (if completed), shall be in the Selected Currency and the Selected Currency only.

   iii. The Merchant shall submit the Charge to the Network in the Selected Currency and for the amount agreed by the Cardmember.

d. Each Merchant is required to maintain one or more Bank Account(s) for settlement and agrees to provide American Express with the information it requests regarding any Bank Account. If a Bank Account does not meet American Express' requirements, or American Express is otherwise unable to verify the Bank Account, American Express may, in its sole discretion, immediately suspend the Merchant's use of the MCCY Platform, and shall have the immediate right to withhold payments without interest until the Merchant provides American Express with information needed to process payments. Each Bank Account must be maintained at a financial institution, and in a currency, approved by American Express.

e. The Discount Rate and any other fees and assessments applicable to any MCCY Transaction shall be determined based on the submission currency of such Transaction.

f. Any Transaction which the Merchant submits in a currency other than the settlement currency shall be converted by American Express into USD and then, if applicable, into the settlement currency on the date the Transaction is processed by American Express. American Express may charge a Conversion Fee on the gross amount of each such Transaction. Unless a specific rate is required by Applicable Law, American Express shall use conversion rates based on interbank rates selected from customary industry sources on the business day prior to the processing date.

2.5.8 Processing Travellers/Gift Cheques

a. American Express Travellers Cheques are no longer available for purchase. Support is available by phone and the American Express website for customers wishing to redeem Travellers Cheques. Travellers Cheques remain backed by American Express and have no expiration date. Details of how customers can redeem their Travellers Cheques can be found at https://americanexpress.com/travelerscheque.

b. For support, please contact Customer Service at 1.800.221.7282.

2.5.9 Split Shipment

a. 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.

b. The Merchant may obtain a single Authorisation and submit multiple Clearing 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 (see Section 3.2, "Authorisation Time Limit").

c. To accept the Card for Split Shipment Transactions, you must:

   i. State their full cancellation and refund policies;

   ii. Advise the Cardmember of the Authorisation amount that will be requested;

   iii. Disclose and obtain the Cardmember's consent that the items from the purchase will be delivered separately and billed as separate Charges;

   iv. Provide the estimated delivery date(s); and

   v. Submit a Charge Clearing Record only after each item has shipped.

2.6 Charge and Credit Clearing Records

a. This section details the requirements for creating, submitting, retaining, and maintaining accurate and compliant Charge Clearing Records and Credit Clearing Records within the Transaction processing framework.

2.6.1 Charge Transactions

2.6.1.1 Clearing Records

a. Merchants must create a Clearing Record for every Charge. For each Charge submitted electronically, Merchants must create an electronically reproducible Clearing Record that complies with the *Technical Specifications*. For each Charge submitted on paper, Merchants must comply with the Clearing Record requirements listed in Section 4.5, "Submitting Charges and Credits – Paper".

b. If the Cardmember wants to use different Cards for payment of a purchase, Merchants may create a separate Clearing Record for each Card used. However, if the Cardmember is using a single Card for payment of a purchase, the Merchant must not divide the purchase into more than one Charge, nor shall the Merchant create more than one Clearing Record except in the case of airline, cruise line, lodging, or Split Shipment Transactions. Refer to Subsection 2.5.9, "Split Shipment" for more information.

c. Merchants must ensure that all Clearing Records are kept for the full retention period as defined in Chapter 8, "Regulations for Specific Industries" from the date the Merchant submitted the corresponding Charge to American Express. If American Express sends a Merchant a request, the Merchant must provide a copy of the original or electronically stored Clearing Record and other supporting documents and data to American Express within the response timeframe from the date of American Express' request.

d. Charges must be submitted directly, or through the Merchant's Processor, to American Express for processing.

2.6.1.2 Transaction Receipts

a. The Merchant must complete a Transaction Receipt at time of purchase for every Charge. Examples include pre-printed forms supplied to the Merchant by the Acquirer, a Transaction receipt created by an electronic POS device (such as an Authorisation terminal with printer or a checkout register).

b. A Transaction Receipt must be provided to the Cardmember at the conclusion of the Transaction. A Merchant must provide a revised Transaction Receipt to the Cardmember if the Merchant changes the included information.

c. Merchants must:

   i. Truncate the PAN and not display the Expiration Date in accordance with the PCI DSS in place at the time of the Transaction or according to applicable Applicable Law.

   ii. Keep all Transaction Receipts for the timeframe listed in Section 8.1, "Country Specific Policies".

d. Merchants may truncate the PAN on their own copies in accordance with the PCI DSS in place at the time of the Transaction or according to Applicable Law. Refer to the Introduction to DSOP and Standards for Protection for more information.

e. A Transaction Receipt is not required at the time of the Transaction for Contactless Transactions using a Contactless-enabled Card originating at Transit Access Terminals (TATs). Refer to Section 2.6, "Charge and Credit Clearing Records".

f. Transaction Receipts, whether printed or electronic, must include the following:

   i. The PAN or Token truncated in accordance with requirements stated above. Truncated Card Account digits must be masked with replacement characters such as "x," " *," or "#," and not blank spaces or numbers. For manually imprinted Transaction Receipts provided to the Cardmember, the Card Account number and Expiration Date are required.

   ii. Cardmember name, if available.

   iii. Transaction date.

   iv. Amount of the Charge

      - The total purchase price of Goods and Services purchased, including applicable taxes, tips, postage and shipping fees.

- Any tip amount, when requested by the Merchant, should be filled in by the Cardmember before the total is entered in the form.

v. Description of the Goods and Services purchased.

vi. Merchant name (or DBA – "Doing Business As" Name) and address.

vii. Merchant number.

viii. Authorisation approval code number.

ix. The words "No Refund," if a no-refund policy is applicable, or other wording that conforms to Applicable Laws or regulations and describes the Merchant's return policy.

g. Merchants requesting a Cardmember signature must not require Cardmembers to sign the Transaction Receipt until the total amount is shown.

h. For Corporate Purchasing Card (CPC) Charges, Merchants must comply with the Clearing Record requirements above. In addition, Merchants are required to capture additional Card Data on the Clearing Record, and Transmission Data on the Transmissions, according to the *Technical Specifications*, including:

i. CPC reference information (e.g., purchase order number);

ii. The CPC Client Account information;

iii. The purchase price of the Goods with the actual amount of taxes charged shown separately, where taxes are applicable;

iv. Merchants must process CPC Charges under their CPC Establishment Number.

2.6.2 Credit Transactions

2.6.2.1 General Requirements

a. When a Cardmember returns merchandise purchased with a Card or for any reason is due Credit toward a submitted Charge made with a Card, the Merchant must comply with the following requirements and restrictions.

i. A Merchant must never issue a Credit unless that Merchant previously processed a corresponding Charge.

ii. A Merchant must only issue a Credit Transaction to the Card Account used in the original Charge. For Digital Wallet programme Transactions, the Credit can be processed using either the Mobile Device or the corresponding Card. The Payment Account Reference (PAR) can assist Merchants in verifying that the PAN or Token presented corresponds to the Card Account used in the original Charge.

iii. There is no requirement for the Merchant to obtain Authorisation for a Credit. Merchants may submit an Authorisation on Credit for refunds outlined in Subsection 3.3.6, "Authorisation on Credit".

iv. A Merchant must never refund Cash against a previously submitted Charge, except as follows:

- If Applicable Law requires a Merchant to refund cash to a Cardmember.
- If the refund is being requested by the recipient of a gift purchased by a Cardmember.
- The original Charge was processed on a Prepaid Card and that Prepaid Card is no longer available.

b. Merchants may apply their in-store return policy when Prepaid Cardmembers no longer have their Card.

c. Merchants must ensure that all Clearing Records are kept for the applicable Record Retention Period from the date the Merchant submitted the corresponding Transaction to American Express. If American Express sends a Merchant a request, the Merchant must provide a copy of the original or electronically stored Clearing Record and other supporting documents and data to American Express within the response timeframe from the date of American Express' request.

d. Credits must be submitted directly, or through the Merchant's Processor, to American Express for processing.

e. Merchants must follow these steps to issue a Credit:

i. Obtain an Authorisation, if the Merchant supports Authorisation on Credit.

ii. Create a Credit Clearing Record.

iii. Compare the last four (4) digits on the Charge Credit Clearing Record against the Card presented (when applicable).

iv. Have the Cardmember sign the Credit Record (optional).

v. Provide a copy of the Transaction Receipt to the Cardmember.

f. Merchants must submit Credits to American Express within seven (7) days of determining that a Credit is due, and create a Credit Clearing Record that complies with the following requirements.

g. Merchants must submit all Credits under the Merchant Number for the Establishment where the Charge originated.

h. A Credit must be issued in the currency in which the original Charge was submitted to American Express.

i. Merchants must issue Credits to the Card used to make the original purchase. If the Card is not available, Merchants may implement their in-store refund policy.

j. If a Merchant issues a Credit, American Express will not refund the Discount or any other fees or assessments previously applied on the corresponding Charge.

k. For all Credit Clearing Records, Merchants must:

i. Submit the Credit to American Express directly, or through the Merchant's Processor.

ii. Retain the original Credit Clearing Records (as applicable) and all documents evidencing the Transaction, or reproducible records thereof, for the timeframe listed in Section 8.1, "Country Specific Policies".

iii. Provide a copy of the Transaction Receipt to the Cardmember.

l. Pursuant to Applicable Law, truncate the Card Account and do not print the Card's Expiration Date on copies of Credit Transaction Receipts provided to the Cardmember.

2.6.2.2 Transaction Receipt Requirements

a. The Merchant must complete a Transaction Receipt for every Credit issued. Examples include pre-printed forms supplied to the Merchant by the Acquirer, a Transaction receipt created by an electronic POS device (such as an Authorisation terminal with printer, or a checkout register).

b. A Transaction Receipt must be provided to the Cardmember at the conclusion of the Transaction regardless of whether the Clearing Record is manually imprinted or electronically created. A Merchant must provide a revised Transaction Receipt to the Cardmember if the Merchant changes the included information.

c. Merchants must:

i. Truncate the PAN and not display the Expiration Date in accordance with the PCI DSS in place at the time of the Transaction or according to Applicable Law.

d. Transaction Receipts, whether paper or electronic, must include the following:

i. The PAN or Token truncated in accordance with requirements stated above. Truncated Card Account digits must be masked with replacement characters such as "x," " *," or "#," and not blank spaces or numbers. For manually imprinted Transaction Receipts provided to the Cardmember, the Card Account number is required.

ii. Credit date.

iii. Amount of the Credit.

iv. Merchant name (or DBA – "Doing Business As" Name) and address.

v. Merchant Number.

vi. The Cardmember signature, if required by law.

e. Merchants must ensure that all Transaction Receipts are kept for the applicable Record Retention Period from the date the Merchant submitted the corresponding Charge to American Express.

2.6.3 Substitute Transaction Receipt

a. In some cases, Merchants may provide a Substitute Transaction Receipt as supporting documentation in place of the original Transaction Receipt. Merchants must also provide any additional information requested in the Inquiry. Substitute Transaction Receipts may be used in response to the following Inquiry reasons:

i. 6003

ii. 6006

iii. 6016

b. Refer to Section 5.8, "Inquiry Types" for additional information regarding Inquiry reasons.

c. The Substitute Transaction Receipt must include the following:

i. Card Account
ii. Cardmember name
iii. Merchant name
iv. Merchant location
v. Transaction date/date Goods or Services were shipped or provided
vi. Transaction amount
vii. Authorisation Approval
viii. Description of Goods and/or Services

d. Additionally, the following optional information should be included, if available, on the Substitute Transaction Receipt:

i. Date Goods and/or Services were ordered
ii. The Merchant's website address
iii. The Merchant's customer service's telephone number/email address
iv. Shipped name and address
v. Automated Address Verification response code
vi. Order confirmation number
vii. Electronically captured Cardmember signature

2.7 Use of Service Providers

a. With American Express' prior approval, Merchants may retain, at their expense, a Service Provider; however, the Merchant remains financially and otherwise liable for all obligations, services, and functions such Service Providers perform under the Agreement for the Merchant, including confidentiality obligations and compliance with the *Technical Specifications* for Authorising and submitting Charge Data to American Express, as if the Merchant performed such obligations, services, and functions. Any omission or failure to perform by a Service Provider does not relieve the Merchant of their obligations under the Agreement. Merchants must ensure that their Service Providers cooperate with American Express to enable Card acceptance. Merchants, and not American Express, are responsible and liable for any problems, errors, omissions, delays, or expenses caused by their Service Provider including in relation to the handling of confidential Cardmember Information; any settlement payments misdirected to other parties because of misprogramming of POS systems by third parties; and for any fees that the Merchant's Service Provider charges American Express or it's Affiliates, or that American Express or it's Affiliates incur as a result of the Merchant's Service Provider. Merchants must ensure that their Service Provider has sufficient resources and security controls to comply with all standards, including, but not limited to, technical standards, guidelines, or rules including to prevent internet fraud and protect the personal data of the Cardmember, including data related to Transactions, under Applicable Law. American Express may bill the Merchant for any fees charged by their Service Provider or deduct them from American Express payments to the Merchant. Merchants must notify American Express promptly if Merchants change their Service Provider and provide American Express, on request, with all relevant information about the Service Provider. American Express needs not alter its conduct of business in respect of such Service Provider's performance and may rely upon that performance as if done by the Merchant. Any listing or certification by American Express of a Service Provider does not constitute a guarantee or warranty by American Express of their performance and does not relieve the Merchant of responsibility and liability for any such Service Provider that the Merchant elects to use.

AMERICAN EXPRESS

Authorisation

3

3.1 The Purpose of Authorisation

a. 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.

b. For every Charge, you are required to obtain an Authorisation Approval except for Charges under a Floor Limit (see Section 3.4, "Floor Limit"). For every Credit, we recommend that you obtain an Authorisation Approval for the full amount of the refund in accordance with Section 2.6, "Charge and Credit Clearing Records".

c. 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 Subsection 3.3.2, "Estimated Charge Amount".

d. 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) we will accept the Charge, (iv) you will be paid for the Charge, (v) you will not be subject to a Chargeback, or (vi) the Charge you submit will not be rejected.

3.2 Authorisation Time Limit

a. 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 us more than seven (7) days after the original Authorisation date.

b. 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.

c. 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.

d. The new Approval must be included in the Clearing 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.

e. Estimated Charge Amounts for Merchants in eligible industries are valid for the time periods listed in Table 3-1: Estimated Charge Amount in Subsection 3.3.2, "Estimated Charge Amount". You must obtain a new Authorisation if you do not submit the Charge to us within the Authorisation Validity timeframe.

3.3 Variable Authorisation

a. You must submit a single Authorisation for the full amount of a Charge, or you may utilise Variable Authorisations if the final Charge amount is not known at the time of the initial Authorisation.

b. Variable Authorisation is a suite of optional capabilities that allows Merchants to adjust the amount of a pending Authorisation before the Charge is submitted.

c. Refer to the *Technical Specifications* to determine if Variable Authorisation is available for your geographic region.

3.3.1 Estimated Authorisation

a. The following Estimated Authorisation procedures apply where the final Charge amount is not known at the time of Authorisation.

i. You may obtain an Estimated Authorisation for a good faith estimate of the final Charge amount. Do not overestimate the Authorisation amount. You must inform the Cardmember of any estimated amount for which Authorisation will be requested and must obtain the Cardmember's consent to the estimated amount before initiating the Authorisation request.

ii. Estimated Authorisation amounts must be greater than zero ($0.00).

iii. You must inform the Cardmember that the amount of the Estimated Authorisation is not final and may change.

iv. For travel industries (e.g., lodging, cruise line, and car rental), upon reservation or check-in, determine the estimated amounts of Charges based upon the daily rate and the expected number of days, plus taxes and any known incidental amounts. You must not include an amount for any possible damage to or

theft in the Estimated Authorisation. You may obtain Authorisation and submit intermittently (no less than daily) throughout the duration of travel.

v. For car rental periods exceeding four (4) months, you represent and warrant hereunder that your multi-month rental programme complies with Applicable Law.

vi. Regardless of the industry, you must submit the corresponding Charge as soon as you become aware of the amount to be charged. For any amount of the Charge that exceeds the amount for which you obtained an Authorisation, you must obtain the Cardmember's consent.

vii. You should indicate that the Authorisation amount is an estimated amount by placing the Estimated Authorisation indicator in the Authorisation message. Refer to the *Global Credit Authorization Guide* for additional information about Estimated Authorisation messages.

3.3.2 Estimated Charge Amount

a. If we classify or otherwise determine that you are in an industry that is eligible for Estimated Charge variance as listed in Table 3-1: Estimated Charge Amount, then the Authorisation Approval is valid for Charge amounts that are within the corresponding Estimated Charge variance percentage as listed in the table.

b. If the Estimated Charge Amount falls within the range listed in Table 3-1: Estimated Charge Amount, then no further Authorisation action is necessary.

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

d. Estimated Charge Variance percentages may not apply to Transactions in the EEA and/or UK.

Table 3-1: Estimated Charge Amount

Industry	MCC	Estimated Charge Variance +/-	Authorisation Validity
Eating Places, Restaurants	5812	30%[2]	7 days
Drinking Places	5813	30%[2]	7 days
Grocery Stores (CNP)	5411	15%[1]	7 days
Retail Stores (CNP)	All MCCs	15%[1]	7 days
Taxicabs & Limousines	4121	20%	7 days
Car Rental	7512	15%	30 days
Lodging	7011	15%	30 days
Motor Home & RV Rentals	7519	15%	7 days
Steamship & Cruise Lines	4411	15%	30 days
Truck Rental	7513	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 transactions

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

3.3.3 Incremental Authorisation

a. Incremental Authorisation allows a Merchant to request an increase in the amount of a previously approved Authorisation. Merchants may submit an Incremental Authorisation request if the following conditions are met:

- **i.** The original Authorisation request was submitted as an Estimated Authorisation, and contained the Estimated Authorisation indicator
- **ii.** The Estimated Authorisation request was Approved
- **iii.** The Charge has not been Submitted

b. If the final Charge amount is greater than the amount of the Estimated Authorisation Approval (plus any Estimated Charge variance in Table 3-1: Estimated Charge Amount) then you may request an Incremental Authorisation for the amount that is greater than the previously Approved amount.

c. In addition, if you perform an Incremental Authorisation the following will apply:

- **i.** If the Cardmember is not present at the time of Incremental Authorisation, refer to Subsection 2.5.3, "Credentials-on-File" and Subsection 2.5.4, "Merchant-Initiated Transactions" for additional information.
- **ii.** If the Incremental Authorisation request is declined or otherwise not Approved, then the original Estimated Authorisation approval will continue to be valid for the duration of the Authorisation validity period.

iii. The data elements required in our *Technical Specifications* (e.g., point of service data codes) from the initial Estimated Authorisation will apply to the final Charge. If the Card is no longer available at the time of the Incremental Authorisation request, you must request the Incremental Authorisation as a "Card-on-file" Charge in accordance with the *Technical Specifications*.

iv. An Incremental Authorisation Approval does not increase the Authorisation validity period.

v. Refer to the *Technical Specifications* (including the *Global Credit Authorization Guide*) for additional information about Incremental Authorisation messages.

3.3.4 Authorisation Reversal

a. You must reverse an Authorisation for an Approved Charge if you do not intend to send a Submission to American Express within the Authorisation time limit or Authorisation validity period. See Section 3.2, "Authorisation Time Limit" and Table 3-1: Estimated Charge Amount in Subsection 3.3.2, "Estimated Charge Amount".

b. If you determine that the final Charge amount is less than the amount of the Authorisation Approval minus any Estimated Charge variance listed on Table 3-1: Estimated Charge Amount, then you must reverse the difference between the final Charge amount and the amount of the Authorisation.

c. You must submit a full or partial Authorisation Reversal within twenty-four (24) hours of determining that the previously Approved amount will not be submitted, or that the amount to be submitted will be less than the previously Approved amount. Refer to the *Technical Specifications* (including the Global Credit Authorisation Guide) for additional information about Authorisation Reversal messages.

d. Multiple Authorisation requests within a single Charge can be reversed with a single Authorisation Reversal when the reversal and all previous Authorisation requests include the same Original Transaction Identifier. For example, an Estimated Authorisation for $100 plus an Incremental Authorisation for $50 may both be reversed by a single Authorisation Reversal for $150.

e. The reversed amount of the Charge must not be Submitted.

3.3.5 Partial Authorisation

a. Partial Authorisation is an optional functionality of Credit, 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.

b. Partial Authorisation approvals may not be available on all Transactions.

c. Partial Authorisation is not supported for the following Transaction types:

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

ii. Recurring Billing

3.3.6 Authorisation on Credit

a. Authorisation on Credit is a capability available in some areas that allows Merchants to send refund-specific Authorisation Request messages to Issuers.

b. An Authorisation on Credit may allow Issuers to display a pending credit to a Cardmember, thus improving the Cardmember experience during refunds.

c. The Authorisation on Credit allows Issuers to match a refund or credit Transaction to the original purchase Transaction and may be required in certain geographic regions.

d. Check with your Processor or Terminal Provider, or refer to the *Technical Specifications* to determine if Authorisation on Credit is available to you, and if it is required for your geographic region.

3.4 Floor Limit

a. We maintain a zero-dollar Floor Limit on all Charges regardless of the amount, unless we assign a Floor Limit to an Establishment. 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.

3.5 Possible Authorisation Responses

a. Responses to your requests for Authorisation are generated by Issuers and transmitted by us 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 Processor or Terminal Provider to determine what Authorisation responses will display on your equipment.

Table 3-2: Authorisation Response

Authorisation response	What it means
Approved	The Charge or Credit is approved.
Partially Approved (for use with Credit, 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 Credit, 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, we 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 refund 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. If your policies direct you to do so, you may initiate the pick up process by calling our Authorisation Department.

3.6 Obtaining an Authorisation

a. You must ensure that all Authorisation requests comply with the *Technical Specifications* (see Section 1.4, "Compliance with our Specifications"). If the Authorisation request does not comply with the *Technical Specifications*, the Authorisation was Declined, or for which no Approval code was obtained, we may reject the Submission or we may exercise a Chargeback.

b. 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.

c. If you use an electronic POS system to obtain Authorisation, the Approval must be printed automatically on the Clearing Record.

d. When obtaining an Authorisation is not possible due to POS system problems, system outages, or other disruptions of an electronic Charge, you must obtain a Voice Authorisation as follows:

- **i.** Call our Authorisation Department and provide: Card Account or Token, Merchant Number, and Charge amount. In some situations, you may be asked for additional information such as Expiration Date or CID Number.
- **ii.** A response will be provided. If the request for Authorisation is approved, capture the Approval code for Submission and enter the Approval code into your POS system.
- **iii.** For instructions on how to complete this type of Charge, contact your Terminal Provider, Processor, or if you have a direct link to American Express, your American Express representative.
- **iv.** We may assess a fee for each Charge for which you request a Voice Authorisation unless such a failure to obtain Authorisation electronically is due to the unavailability or inoperability of our computer authorisation system.

India: Voice Authorisation and the procedures described in clause 3.6.d are not applicable in India.

e. We acknowledge that you, at your own risk, may submit Transactions without Authorisation only in the event of a loss of connectivity resulting in your POS system being unable to connect to our systems for Authorisation. In relation to any such Charge for which you did not obtain Authorisation, we may reject the Charge if we have reasonable grounds to do so, or we may exercise any of our rights under this Agreement including, but not limited to, Chargeback, offsetting, and withholding amounts from payment we otherwise would make to you.

3.7 Card Identification (CID) Number

a. 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.

b. 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.

c. **Note:** CID Numbers must not be stored for any purpose. They are available for real time Charges only. See Introduction to DSOP and Standards for Protection.

AMERICAN EXPRESS

Submission

4

4.1 Submitting Charges and Credits

a. Establishments must submit Transactions, whether electronic or paper, in Local Currency, or in the case of an Establishment that we have approved for processing on the American Express multicurrency platform, in accordance with the Agreement, unless American Express otherwise agrees in writing or unless required by Applicable Law. You must submit all Charges and Credits under an Establishment Number of the Establishment where the Charge or Credit originated. A unique Establishment Number must be used for each Local Currency. Any currency conversions made by American Express pursuant to the Agreement shall be made as of the date of processing the Transaction by American Express or at such other date as American Express may provide notice. Unless a specific rate is required by Applicable Law, American Express will use conversion rates based on interbank rates that American Express selects from customary industry sources on the business day prior to the processing date.

b. If, after the effective date of the Agreement, an Establishment wishes to permit customers to make purchases or payments in a currency not listed in the *Technical Specifications* and not previously agreed to by American Express as an eligible currency on the American Express multicurrency platform, you shall immediately notify American Express in writing; and you may, after written notice from American Express of our agreement to your submission of Charges in that currency, submit Charges in that currency. If American Express does not agree to your submission of Charges in a currency not listed in the *Technical Specifications*, you must not submit Charges in such currency.

c. In all cases, submission and payment of Transactions will be subject to immediate review and amendment in the event that Applicable Law, regional volatility, or other unforeseen events inhibit the settlement operation for either party.

d. Transactions (including Charges and Credits) will be deemed accepted on a given business day if processed by us before our deadline for processing Charges and Credits for that day at the relevant location.

4.2 Submitting Charges

a. You must submit all Charges to us within seven (7) days of the date they are incurred, provided that you must wait to submit Charges until you have shipped the Goods or provided the Services to the Cardmember, after which you have seven (7) days to submit such Charges. Charges are deemed "incurred", for purposes of the preceding sentence, on the date that the Cardmember agrees to pay for the Goods or Services purchased with the Card.

b. The deposit element of a Delayed Delivery Charge and any Advance Payment Charges may be submitted before the Goods are shipped or Services provided. See Subsection 2.5.6, "Delayed Delivery" and Subsection 2.5.1, "Advance Payments".

c. If you are located in the EEA or UK, you must not submit Charges where the full exact amount is not specified when the Cardmember consents to the Transaction. Without prejudice to our Chargeback rights generally, if you do so, and the Card is issued in the EEA or UK, we will have Chargeback rights for the full amount of the Charge for a period of one hundred and twenty (120) days from the date of submission of the Charge, and thereafter for any disputed portion of the Charge (up to and including the full amount). If the Cardmember consents to an adjusted Charge amount, we may exercise our Chargeback rights accordingly. A Cardmember may provide consent, e.g., by completing a valid CVM, excluding Cardmember signature, in the course of your following the procedures set out for an In-Person Charge in Section 2.3, "In-Person Charges".

4.3 Submitting Credits

a. You must create a Credit Record for every Credit and submit Credits to us within seven (7) days of determining that a Credit is due. You must not issue a Credit when there is no corresponding Charge. You must submit a Credit only for the value of the corresponding Charge, excluding the Merchant Service Fee. We will deduct the full amount of the Credit from our payment to you (or, if you have signed a direct debit mandate, debit your Bank Account), but if we cannot, then you must pay us promptly upon receipt of our notification. If you issue a Credit, we will not refund the Discount or any other fees or assessments previously applied on the corresponding Charge and may charge you a fee for processing the Credit. A credit shall be issued in the currency in which the original Charge was submitted to us.

b. You must issue Credits to the Card Account used to make the original purchase, unless it was made with a Prepaid Card that is no longer available for the Cardmember's use, or unless the Credit is for a gift that is

being returned by someone other than the Cardmember that made the original purchase, in which case you may apply your refund policy.

c. You must not give cash refunds to Cardmembers for Goods or Services they purchase on the Card, unless required by Applicable Law. You must disclose your refund policy to Cardmembers at the time of purchase and in compliance with Applicable Law.

4.4 Submitting Charges and Credits – Electronically

a. If you have an electronic POS system, you must submit Charges and Credits electronically over communication links (Transmissions). Transmissions must comply with the *Technical Specifications*. We need not accept any non-compliant Transmissions or Charge Data. You must place additional, less, or reformatted information on Transmissions within thirty (30) days written notice from us. Even if you transmit Charge Data electronically, you must still complete and retain the Clearing Records.

b. If you upgrade your POS system for Chip Card acceptance for Other Payment Products, you agree to comply with *Technical Specifications* that we provide to you to enable Chip Card acceptance.

c. You must ensure your POS system meets all relevant mandates and certification requirements as required and in accordance with the compliance dates notified to you by American Express, including, but not limited to:

- POS systems need to be American Express Chip/American Express Integrated Circuit Card Payment Specifications (AEIPS) compliant
- Contactless reader POS systems need to be American Express Expresspay compliant

d. American Express may choose to notify you in writing or via its Merchant Specifications Website (www.americanexpress.com/merchantspecs) or its successor website.

e. Notwithstanding the foregoing, if commercially reasonable and not prohibited by any of your other agreements, you will work with us to configure your Card Authorisation, submission, and POS system equipment or systems to communicate directly with our systems for Authorisations and submissions of Charge Data.

4.5 Submitting Charges and Credits – Paper

a. If, due to extraordinary circumstances, you are required to submit Charges and Credits on paper, you must submit Charges and Credits in accordance with our instructions. We are not obliged to agree to paper submissions and we reserve the right to charge a fee for Charges and Credits submitted on paper. Such fee will be notified to you in advance.

4.6 Payments Errors and Adjustments

a. If we determine at any time that we have paid you in error or that there is an error in American Express' reconciliation of Charges (e.g., incorrect calculations, inclusion of another party's charge forms, inclusion of invalid Card Accounts, etc.) and monies are due to American Express, we may exercise the right to Chargeback such erroneous amount to you or the relevant Establishment, in American Express' discretion. If you receive any payment from us not owed to you under the Agreement, you must immediately notify us (by calling our telephone service centre) and your Service Provider (if applicable) and return such payment to us promptly. Whether or not we are notified, we have the right to withhold or deduct future payments to you or debit your Bank Account until we fully recover the amount.

b. You or your Establishments must notify American Express in writing of any error or omission in respect of the Discount or other fees or payments for Transactions or Chargebacks within ninety (90) days of the date of the statement containing such claimed error or omission. If you do not provide such notice within the required timeframe, American Express will consider the statement to be conclusively settled by you as complete and correct in respect of such amounts, except for any amounts owed to us. We have no obligation to pay any party other than you under the Agreement. This clause, 4.6.b, is not applicable for Merchants located in Australia and/or New Zealand.

c. The adjustments described in this subsection will be calculated in the currency in which the related Charges were submitted or payment was made (as applicable), with applicable conversions made in accordance with the procedures herein.

AMERICAN EXPRESS

Chargebacks and Inquiries

5

5.1 Introduction

a. This chapter describes how American Express processes Chargebacks and Inquiries.

b. Highlights of this chapter include:

- a discussion of the American Express Disputed Transaction process,
- a review of the ways to handle Disputed Transactions,
- examples of various Inquiry types and recommended supporting documentation,
- an overview of the American Express Chargeback policies, and
- tips for avoiding Inquiries and Chargebacks and preventing fraud.

5.2 Transaction Process

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

- Cardmember dissatisfaction with some aspect of the purchase (e.g., a failure to receive the merchandise, duplicate billing of a Transaction, incorrect billing amount),
- an unrecognised Transaction where the Cardmember requests additional information,
- Cardmember billed for Goods or Services not yet received, or
- actual or alleged fraudulent Transactions.

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

c. You must not suggest or require Cardmembers to waive their right to dispute any Transaction, as a condition to accepting the Card.

5.3 Disputed Transactions Rights

a. With respect to a Disputed Transaction, unless otherwise indicated by us:

i. we may send you an Inquiry prior to exercising Chargeback,

ii. if we determine we have sufficient information to resolve the Disputed Transaction in favour of the Cardmember, we will exercise our Chargeback rights; or

iii. for Transactions subject to the Fraud Full Recourse Programme we have Chargeback rights, where you do not have the right to request a reversal of our decision to exercise our Chargeback rights (Section 5.11, "Fraud Full Recourse Programme").

b. We have Chargeback rights:

i. whenever Cardmembers bring Disputed Transactions, as described in this chapter, or have rights under Applicable Law or contract to withhold payments,

ii. in cases of actual or alleged fraud relating to Transactions,

iii. if you do not comply with the Agreement (including sending incomplete or incorrect Transaction Data in Transaction Submissions), even if we had notice when we paid you for a Transaction that you did not so comply and even if you obtained Authorisation for the Transaction in question, or

iv. as provided elsewhere in the Agreement.

c. All judgements regarding resolution of Disputed Transactions are at our sole discretion.

d. We may reinvestigate a previously Disputed Transaction if a Cardmember provides new or additional information after we review the initial supporting documentation. In such case, you may be required to provide additional information to support the validity of the Transaction.

e. You must not resubmit a Disputed Transaction after it has been resolved in favour of the Cardmember. We will Chargeback all such Disputed Transactions that are resubmitted.

f. If you have established a process whereby your Service Provider will receive and manage Disputed Transactions on your behalf, you agree that we are not liable for your Service Provider's failure to perform its responsibilities to you, including responding to us within the dispute resolution timelines set out in the Agreement.

5.4 Disputed Transactions Process

a. The following describes the Disputed Transactions process:

Table 5-1: Disputed Transaction Process

Case is opened	We may take one of the following actions, based upon the information provided by you, the Cardmember, Issuer, or Network: • We may send you a Chargeback or, if we cannot resolve the Disputed Transaction without further information from you, an Inquiry. • We may resolve the Disputed Transaction in your favour and either take no further action (if we have not previously exercised Chargeback) or reverse our previous Chargeback. None of these actions affect procedures under the Fraud Full Recourse Programme (see Section 5.11, "Fraud Full Recourse Programme").
Merchant Receives a Chargeback or Inquiry	American Express tries to resolve a Disputed Transaction by first using information available to us. However, in instances where we cannot resolve a Disputed Transaction, we will send you a Chargeback or, if we cannot resolve the Disputed Transaction without further information from you, an Inquiry. The Chargeback or Inquiry that we will send to you includes information about the Transaction in question, required documentation that you must send us to support the Transaction, and a deadline by which your response must be received. Refer to the following sections for more information: • Section 5.5, "Chargebacks and Inquiries Response Timeframe" • Section 5.6, "Chargeback Reasons" • Section 5.8, "Inquiry Types" • Section 5.12, "Ways to Receive Chargebacks and Inquiries"
Merchant responds	You may respond to the Chargeback or Inquiry by: • providing the required documentation to support the validity of the Transaction, • advising that the Chargeback is invalid and the Incorrect Chargeback code was used and providing documentation including the specific details and supporting evidence, • authorising a Chargeback to your Merchant Account, • issuing a Credit to the Card Account, or • issuing a partial Credit to the Card Account and providing American Express with supporting documentation for the remainder of the Transaction and the reason for providing only a partial Credit. See Section 5.13, "Response Methods" for the process to follow when responding to a Chargeback or Inquiry. **Note:** If you choose not to respond to our Inquiry, we will debit your Merchant Account with a "No Reply" Chargeback (see Section 5.6, "Chargeback Reasons").
American Express reviews	American Express reviews your response to ensure it includes all the required and requested pieces of information about the Disputed Transaction. Upon receipt of the required information, we will determine whether to process, reverse, or uphold the Chargeback.

Table 5-1: Disputed Transaction Process (Continued)

Disputed Charge is resolved	When a Disputed Transaction is resolved, one of the following may occur: • We will notify the Cardmember and Issuer of the resolution, with consideration to any supporting documentation you provide. • We will notify you of a Chargeback and debit your Bank Account. See Section 5.10, "How We Chargeback" for details. We typically resolve Disputed Transactions within two (2) Cardmember billing cycles from the time the dispute is opened or as required by Applicable Law. The documentation you receive from us may provide a more exact timeframe.

5.5 Chargebacks and Inquiries Response Timeframe

a. You must respond in writing to our Chargeback and Inquiry within twenty (20) days.

b. Notwithstanding Section 5.5 a, if you are located in Argentina and a Disputed Transaction relates to a Card issued in Argentina, you must respond within five (5) days.

c. Notwithstanding Section 5.5 a, if you are located in India and a Disputed Transaction relates to a Card issued in India, you must respond within ten (10) days.

d. Notwithstanding Section 5.5 a, if a Disputed Transaction relates to a Card issued in the EEA or UK and involves a claim that the Cardmember was not advised of the full exact amount of the Transaction at the time the Cardmember consented to the Transaction, we reserve the right to reduce the response period to five (5) days from the date on which we contacted you requesting a written response.

5.6 Chargeback Reasons

a. When we process a Chargeback to you, we will provide information about the Chargeback. For each Chargeback reason, the following tables include:

- Description – brief description of the Chargeback reason,
- Information provided with Chargeback – type of information provided by the Cardmember or Issuer (or both) to support the Chargeback (documentation may not be provided with the Chargeback if it was preceded by an Inquiry),
- Support required to request a Chargeback Reversal – criteria of required documentation if you request a Chargeback Reversal. If the Chargeback is invalid and the incorrect Chargeback code was used, you must provide documentation including the specific details and supporting evidence.

b. The tables in the following subsections list the Chargeback reasons and information related to each Chargeback reason. The key below describes the applicable classification and code structure of Chargeback codes by country:

Table 5-2: Chargeback Reason Codes

Classification	Code structure	Country
International Standards Organization (ISO)	4 numeric digits	All countries outside of US and Canada
US/Canada Chargeback reason code	1 alpha followed by 2 numeric digits	US and Canada

5.6.1 Authorisation

Table 5-3: Invalid Authorisation (ISO 4521) / Transaction amount exceeds Authorisation amount (A01)

Invalid Authorisation (ISO 4521) / Transaction amount exceeds Authorisation amount (A01)	
Description	The amount of the Authorisation Approval was less than the Transaction amount you submitted. Certain exceptions apply, see Section 3.3, "Variable Authorisation" for industry clarifications.
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that a valid Authorisation Approval was obtained for the full Transaction amount in accordance with the Agreement unless exceptions apply, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-4: Invalid Authorisation (ISO 4521) / No valid authorisation (A02)

Invalid Authorisation (ISO 4521) / No valid authorisation (A02)	
Description	The Transaction you submitted did not receive a valid Authorisation Approval; it was declined or the Card was expired. Certain exceptions apply, see Section 3.3, "Variable Authorisation" for industry clarifications.
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that a valid Authorisation Approval was obtained in accordance with the Agreement, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed • For a Transit Contactless Transaction, proof that: ▪ An approved Account Status Check or Authorisation was obtained within the Authorisation Time Period, prior to the Submission of the corresponding Aggregated Transaction for an amount that does not exceed the Chargeback Protection Threshold, or ▪ Authorisation was obtained for an Aggregated Transaction that exceeded the Chargeback Protection Threshold or the Authorisation Time Period, or ▪ if the Account Status Check or Authorisation was declined, the Transaction amount was less than or equal to the Declined Authorisation Protection threshold For "expired or not yet valid Card", the following support is also acceptable: • Proof that the Transaction was incurred prior to the Card Expiration Date or within the Valid Dates on the Card

Table 5-5: Invalid Authorisation (ISO 4521) / Authorisation approval expired (A08)

Invalid Authorisation (ISO 4521) / Authorisation approval expired (A08)	
Description	The Transaction was submitted after the Authorisation Approval expired.
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that a valid Authorisation Approval was obtained in accordance with the Agreement, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

5.6.2 Cardmember Disputes

Table 5-6: Credit not processed (ISO 4513 / C02)

Credit not processed (ISO 4513 / C02)	
Description	We have not received the Credit (or partial Credit) you were to apply to the Card.
Information provided with the Chargeback	• Transaction Data, or • Copy of the Credit Record or details showing that you were to provide Credit to the Cardmember.
Support required to request a Chargeback Reversal	• If no Credit (or only partial Credit) is due, a written explanation of why credit is not due with appropriate documents to support your position • Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Proof that the Merchant refunded the Cardmember through an alternate method, along with Issuer validation that the Merchant attempted an Authorisation on a Credit Transaction that was declined.

Table 5-7: Credit not processed (ISO 4513) / Goods/Services returned or refused (C04)

Credit not processed (ISO 4513) / Goods/Services returned or refused (C04)	
Description	The Goods or Services were returned or refused but the Cardmember did not receive Credit.
Information provided with the Chargeback	• Transaction Data, and • If returned: Details of the return (e.g., returned date, shipping documentation, etc.), or • If refused: Date of the refusal and the method of refusal

Table 5-7: Credit not processed (ISO 4513) / Goods/Services returned or refused (C04) (Continued)

Credit not processed (ISO 4513) / Goods/Services returned or refused (C04)	
Support required to request a Chargeback Reversal	• If returned: A copy of your return policy, an explanation of your procedures for disclosing it to the Cardmember, and details explaining how the Cardmember either did not follow the return policy or did not return the Goods to your business, or • A copy of the Clearing Record indicating the terms and conditions of the purchase with details explaining how the Cardmember did not follow the policy, or • If Goods/Services refused: Proof that the Goods/Services were accepted (e.g., signed delivery slip if the Goods were delivered, screen print showing use of the Service if Service was provided via internet), or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Proof that the Merchant refunded the Cardmember through an alternate method, along with Issuer validation that the Merchant attempted an Authorisation on a Credit Transaction that was declined.

Table 5-8: Credit not processed (ISO 4513) / Goods/Services cancelled (C05)

Credit not processed (ISO 4513) / Goods/Services cancelled (C05)	
Description	The Cardmember claims that the Goods/Services ordered were cancelled.
Information provided with the Chargeback	• Transaction Data, and • Cancellation details (e.g., cancellation number, cancellation date, email notification, written documentation requesting cancellation, acknowledgement that cancellation request was received)
Support required to request a Chargeback Reversal	• A copy of your cancellation policy, an explanation of your procedures for disclosing it to the Cardmember, and details explaining how the Cardmember did not follow the cancellation policy, or • A copy of the Clearing Record indicating the terms and conditions of the purchase and details explaining how the Cardmember did not follow the policy, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Proof that the Merchant refunded the Cardmember through an alternate method, along with Issuer validation that the Merchant attempted an Authorisation on a Credit Transaction that was declined.

Table 5-9: Credit not processed (ISO 4513) / Guaranteed Reservations (C18)

Credit not processed (ISO 4513) / Guaranteed Reservations (C18)	
Description	The Cardmember claims to have cancelled a reservation yet was charged a Guaranteed Reservations Transaction.
Information provided with the Chargeback	• Transaction Data, and • Cancellation details (e.g., cancellation number, cancellation date, email notification, written documentation requesting cancellation, acknowledgement that cancellation request was received)
Support required to request a Chargeback Reversal	• Documentation that supports the validity of the Guaranteed Reservations, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Proof that the Merchant refunded the Cardmember through an alternate method, along with Issuer validation that the Merchant attempted an Authorisation on a Credit Transaction that was declined.

Table 5-10: Goods/Services not received or only partially received (ISO 4554 / C08)

Goods/Services not received or only partially received (ISO 4554 / C08)	
Description	The Cardmember claims to have not received (or only partially received) the Goods/Services.
Information provided with the Chargeback	• Transaction Data, and • Written description of the Goods/Services the Cardmember purchased, or • Documentation showing return, or attempt to return, the partially received Goods (e.g., pickup/delivery confirmation)
Support required to request a Chargeback Reversal	• Proof that the Goods or Services were received in their entirety by the Cardmember or the Cardmember's authorised representative, or • Proof that the Goods or Services were delivered to the address specified by the Cardmember, or • Completion of work order approved in writing by the Cardmember showing the Cardmember received the Services and dates that the Services were used/provided, or • Proof refuting Cardmember's claim that Services were cancelled or that the Goods were returned to the Merchant, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • For Instalment Payment Transactions and Bill Payment Provider Transactions, provide a copy of your terms and conditions agreed to by the Cardmember and details explaining how the Cardmember did not comply with the terms and conditions, or • Compelling Evidence as defined in Subsection 5.7.1, "Compelling Evidence for Goods/Services not received or only partially received (ISO 4554/C08)"

Table 5-11: Paid by other means (ISO 4515 / C14)

Paid by other means (ISO 4515 / C14)	
Description	The Cardmember has provided us with proof of payment by another method.
Information provided with the Chargeback	• Transaction Data, and • Documentation or written explanation describing how the Cardmember paid with another form of payment
Support required to request a Chargeback Reversal	• Documentation showing that the Cardmember's other form of payment was not related to the Disputed Transaction, or • Proof that the Cardmember provided consent to use the Card as a valid form of payment for the Disputed Transaction, or • Proof or an explanation that the other form of payment is not valid or that the Merchant did not receive payment from a third party for the same Goods or Services, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-12: Cancelled recurring billing (ISO 4544 / C28)

Cancelled recurring billing (ISO 4544 / C28)	
Description	Cardmember claims to have cancelled or attempted to cancel Recurring Billing Transactions for Goods or Services. Please discontinue all future billing for this Recurring Billing Transaction.
Information provided with the Chargeback	• Transaction Data, and • Cancellation or attempted cancellation details (e.g., cancellation number, cancellation date, email notification, written documentation requesting cancellation, acknowledgement that cancellation request was received)
Support required to request a Chargeback Reversal	• Proof that the Cardmember has not cancelled and continues to use the Service or receives the Goods, and a copy of your cancellation policy, an explanation of your procedures for disclosing it to the Cardmember, and details explaining how the Cardmember did not follow the cancellation policy. For Transactions in connection with an Introductory Offer, proof that you have fulfilled the requirements set forth in Subsection 2.5.5.1, "Introductory Offers"; or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-13: Goods/Services not as described (ISO 4553 / C31)

Goods/Services not as described (ISO 4553 / C31)	
Description	The Cardmember claims to have received Goods/Services that are different than the written description provided at the time of the Transaction.

Table 5-13: Goods/Services not as described (ISO 4553 / C31) (Continued)

Goods/Services not as described (ISO 4553 / C31)	
Information provided with the Chargeback	• Transaction Data, and • A description of the Cardmember's claim that the Goods/Services received differ from your written description provided at the time of Transaction, and • In the case of Goods: written description of the Cardmember's attempt to return the Goods
Support required to request a Chargeback Reversal	• Proof refuting the Cardmember's claim that the written description differs from the Goods/Services received, or • Proof that the Cardmember agreed to accept the Goods/Services as provided, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Proof that Goods and Services matched what was described at time of purchase (e.g., photographs, e-mails) or, • For Instalment Payment Transactions and Bill Payment Provider Transactions, provide a copy of your terms and conditions agreed to by the Cardmember and details explaining how the Cardmember did not comply with the terms and conditions. For Goods or Services purchased by the Cardmember that were received in a damaged or defective state, the Merchant must provide one (1) or more of the following items: • Show that an attempt was made by the Merchant to repair or replace damaged or defective Goods or to provide replacement Services • If returned, state how the Cardmember did not comply with the Merchant's clearly documented cancellation, return policy or applicable law and regulations • Show that the Cardmember agreed to accept the Goods or Services "as is"

Table 5-14: Goods/Services damaged or defective (ISO 4553 / C32)

Goods/Services damaged or defective (ISO 4553 / C32)	
Description	The Cardmember claims to have received damaged or defective Goods/Services.
Information provided with the Chargeback	• Transaction Data, and • Description of the damage or defective Goods/Services, date of receipt of the Goods/Services, extent of the damage to the Goods or how the Service was defective, and • Details of how you were notified or how the Cardmember attempted to notify you of the issue, and • If returned: Details of how the Cardmember returned, or attempted to return, the Goods to you

Table 5-14: Goods/Services damaged or defective (ISO 4553 / C32) (Continued)

Goods/Services damaged or defective (ISO 4553 / C32)	
Support required to request a Chargeback Reversal	• Proof refuting the Cardmember's claim that the Goods/Services were damaged or defective (provided that, in the case of Goods, they were not returned to you), or • Proof that an attempt was made to repair or replace damaged or defective Goods or to provide replacement Services, or • Proof that the Cardmember did not comply with your clearly documented cancellation and return policies or Applicable Law (provided that, in the case of Goods, they were returned to you), or • Proof that the Cardmember agreed to accept the Goods as delivered, or • Proof that the Goods/Services were not returned to you, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed or • For Instalment Payment Transactions and Bill Payment Provider Transactions, provide a copy of your terms and conditions agreed to by the Cardmember and details explaining how the Cardmember did not comply with the terms and conditions.

Table 5-15: Vehicle rental Transaction non qualified or unsubstantiated (ISO 4750) / Vehicle rental - Capital Damages, theft, or loss of use (M10)

Vehicle rental Transaction non qualified or unsubstantiated (ISO 4750) / Vehicle rental - Capital Damages, theft, or loss of use (M10)	
Description	The Cardmember claims to have been incorrectly billed for Capital Damages, theft, or loss of use. See Section 8.2.4, "Motor Vehicles".
Information provided with the Chargeback	• Transaction Data, and • If the Transaction amount exceeds the estimated amount by more than 15%, a copy of the specific estimate of the Capital Damages agreed to by the Cardmember • If the Cardmember purchased the Merchant's collision, loss, or theft insurance – documentation that proves the Cardmember purchased, and was charged for the car rental Merchant's collision, loss, or theft insurance • If the Cardmember was charged for theft or loss of use of the vehicle – documentation that proves the Cardmember was charged for theft or loss of use of the vehicle
Support required to request a Chargeback Reversal	• Proof that the Transaction submitted was within the specific estimate of the Capital Damages agreed in writing by the Cardmember, plus 15%. • Proof refuting Cardmember's claim that they were covered by the Merchant's insurance (i.e., rental agreement evidencing Cardmember's waiver of insurance or documentation that shows the Cardmember purchased insurance that was not sufficient to pay for the Capital Damages). • Proof that the Transaction was valid and not for theft or loss of use. • Proof that the Cardmember agreed in writing to accept liability for the Capital Damages. • Proof that a credit which directly offsets the Disputed Transaction has already been processed.

Table 5-16: Local Regulatory/Legal Dispute (ISO 4754)

Local Regulatory/Legal Dispute (ISO 4754)	
Description	Certain laws may provide Cardmembers with the right to be refunded by the Issuer. In such circumstances we will have Chargeback rights in respect to such Transactions. Where such laws are in effect and the Cardmember claims the rights provided, the Issuer may charge back for this reason, but only where no other Chargeback rights apply, the Transaction meets the defined requirements, and both the acquirer and Issuer have an obligation under the applicable law or regulation.
Information provided with the Chargeback	Transaction Data and applicable law or regulation
Support required to request a Chargeback Reversal	• Supporting documentation demonstrating that the alleged law/regulation does not exist (e.g., was repealed or expired), the Cardmember is not covered by it, or it does not apply to the facts of the Cardmember's dispute, or it does not establish an obligation of the acquirer. • Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed.

5.6.3 Fraud

Table 5-17: Missing imprint (ISO 4527 / F10)

Missing imprint (ISO 4527 / F10)	
Description	The Cardmember claims they did not participate in this Transaction that was not processed using Magnetic Stripe or Chip Card Data. **Note:** Not applicable to Card Not Present Transactions, and Digital Wallet Payments.
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that this was a Card Not Present Transaction, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Proof that the Card was present by providing an imprinted Transaction Receipt Record or showing capture of the Magnetic Stripe

Table 5-18: Multiple ROCs (ISO 4534 / F14)

Multiple ROCs (ISO 4534 / F14)	
Description	The Cardmember claims they participated in one valid transaction with your establishment, however, the Cardmember denies participation in the additional and subsequent transactions that were submitted by you.
Information provided with the Chargeback	• Transaction Data for each Transaction
Support required to request a Chargeback Reversal	• Proof that each of the Transactions are valid Transactions, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-19: No Valid Authorisation (ISO 4755) / No Cardmember Authorisation (F24)

No Valid Authorisation (ISO 4755) / No Cardmember Authorisation (F24)	
Description	The Cardmember claims they did not participate in this Transaction. You submitted the Transaction for payment, but the Transaction was not Authorised, was declined or was submitted with an expired Authorisation. Note: If prior Authorisation was provided for a lesser amount, the Chargeback amount is restricted to the difference of the Authorised amount and the submitted Transaction amount. For estimated Transaction amounts, the Chargeback amount is restricted to the difference of the Authorised amount plus the allowable percentage and the submitted Transaction amount. See Section 3.3, "Variable Authorisation".
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Proof that you received a valid Authorisation for the Transaction • For a Transit Contactless Transaction, proof that: ▪ An approved Account Status Check or Authorisation was obtained within the Authorisation Time Period, prior to the Submission of the corresponding Aggregated Transaction for an amount that does not exceed the Chargeback Protection Threshold, or ▪ Authorisation was obtained for an Aggregated Transaction that exceeded the Chargeback Protection Threshold or the Authorisation Time Period, or ▪ if the Account Status Check or Authorisation was declined, the Transaction amount was less than or equal to the Declined Authorisation Protection threshold.

Table 5-20: Card Not Present (ISO 4540 / F29)

Card Not Present (ISO 4540 / F29)	
Description	The Cardmember denies participation in a mail order, telephone order, application-initiated, or Internet Transaction.
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof of Delivery to the Cardmember's billing address, or • Proof that a valid authorisation Approval was obtained, and that you attempted to validate the CID, and the response received was: ▪ a "no match," ▪ an "unchecked," or • Proof that you validated the address via Authorisation and shipped Goods to the validated address, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Compelling Evidence as defined in Subsection 5.7.2, "Compelling Evidence for Card Not Present Fraud (ISO 4540/F29)"

Table 5-21: Fraud Liability Shift - Counterfeit (ISO 4798) / EMV counterfeit (F30)

Fraud Liability Shift - Counterfeit (ISO 4798) / EMV[1] counterfeit (F30)	
Description	The Cardmember denies participation in the Transaction and a counterfeit Chip Card was used at a POS system where the Transaction was not processed as a Chip Card Transaction because either the POS system was unable to process a Chip Card or the Transaction was manually keyed. Notes: • May not be applied unless the country's EMV status is designated as "counterfeit" as specified in Chapter 8, "Regulations for Specific Industries" • Not applicable to contactless Transactions and Digital Wallet Payments
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that this was a Card Not Present Transaction, • Proof that the POS system processed a Chip Card Transaction, or • Proof that a Credit, which directly offsets the Disputed Transaction, has already been processed

1. EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC, section 2.1.1.A.V.C.

Table 5-22: Fraud Liability Shift - Lost/Stolen/Non-Received (ISO 4799) / EMV Lost / Stolen / Non Received (F31)

Fraud Liability Shift - Lost/Stolen/Non-Received (ISO 4799) / EMV Lost / Stolen / Non-Received (F31)	
Description	The Cardmember denies participation in the Transaction and Chip Card with PIN capabilities was lost/stolen/non-received and was used at a POS system where the Transaction was not processed as a Chip Card Transaction with PIN validation because either the POS system is not an Enabled Chip and PIN POS system, or the Transaction was manually keyed. Notes: • May not be applied unless the country's EMV status is designated as "lost/stolen" as specified in Chapter 8, "Regulations for Specific Industries" • Not applicable to Contactless Transactions, Digital Wallet Payments, and Transactions that qualify under the No CVM Programme. (Section 2.3.2, "No Signature/No PIN Programme")
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that this was a Card Not Present Transaction, • Proof that the POS system processed a Chip Card Transaction with PIN validated, or • Proof that a Credit, which directly offsets the Disputed Transaction, has already been processed

5.6.4 Inquiry/Miscellaneous

Table 5-23: Insufficient reply (ISO 4517 / R03)

Insufficient reply (ISO 4517 / R03)	
Description	Complete support and/or documentation were not provided as requested in response to an Inquiry.
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that a Credit which directly offsets the Disputed Transaction has already been processed, or • Documentation requested with Chargeback

Table 5-24: No reply (ISO 4516 / R13)

No reply (ISO 4516 / R13)	
Description	We did not receive your response to our Inquiry within the specified timeframe. See Section 5.5, "Chargebacks and Inquiries Response Timeframe".
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof you responded to the original Inquiry within the specified timeframe, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

5.6.5 Processing Error

Table 5-25: Unassigned Card Account (ISO 4523 / P01)

Unassigned Card Account (ISO 4523 / P01)	
Description	You have submitted a Transaction using an invalid or otherwise incorrect Card Account. **Note:** You may resubmit the Transaction to us if you are able to verify and provide the correct Card Account.
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Copy of the imprint that confirms Card Account, or • Proof that you obtained an Authorisation Approval for such Card Account, or • Copy of the Clearing Record from the terminal that electronically read the Card Account, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-26: Credit/Debit Presentment Error (ISO 4752) / Credit processed as Charge (P03)

Credit/Debit Presentment Error (ISO 4752) / Credit processed as Charge (P03)	
Description	The Cardmember claims the Charge you submitted should have been submitted as a Credit.
Information provided with the Chargeback	• Transaction Data, and • Copy of the Credit Record or details showing you agreed to provide Credit to the Cardmember
Support required to request a Chargeback Reversal	• Proof that the Transaction was submitted correctly, or • Proof that a Credit which directly offsets the Transaction has already been processed

Table 5-27: Credit/Debit Presentment Error (ISO 4752) / Charge processed as Credit (P04)

Credit/Debit Presentment Error (ISO 4752) / Charge processed as Credit (P04)	
Description	The Cardmember claims the Credit you submitted should have been submitted as a Charge.
Information provided with the Chargeback	• Transaction Data, and • Copy of the Clearing Record or details of the Transaction
Support required to request a Chargeback Reversal	• Proof that the Credit was submitted correctly, or • Proof that a Transaction that directly offsets the Credit has already been processed

Table 5-28: Incorrect Transaction Amount or Primary Account Number (PAN) Presented (ISO 4507) / Incorrect Transaction amount (P05)

Incorrect Transaction Amount or Primary Account Number (PAN) Presented (ISO 4507) / Incorrect Transaction amount (P05)	
Description	The Transaction amount you submitted differs from the amount the Cardmember agreed to pay.
Information provided with the Chargeback	• Transaction Data, and • Details describing the discrepancy and a copy of the Clearing Record, if available
Support required to request a Chargeback Reversal	• Proof that the Cardmember agreed to the amount submitted, or • Proof that the Cardmember was advised of and agreed to pay for any additional or delayed Transactions using the Card the Transaction was submitted to, or • Itemised contract/documentation substantiating the Transaction amount submitted (e.g., copy of the itemised Record of Transaction or the Record of Transaction combined with itemised documentation showing the breakdown of charges), or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-29: Late Presentment (ISO 4536) / Late submission (P07)

Late Presentment (ISO 4536) / Late submission (P07)	
Description	The Transaction was not submitted within the required timeframe. See Section 4.2, "Submitting Charges"
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof the Transaction was submitted within the required timeframe, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-30: Multiple Processing (ISO 4512) / Duplicate Transaction (P08)

Multiple Processing (ISO 4512) / Duplicate Transaction (P08)	
Description	The individual Transaction was submitted more than once.
Information provided with the Chargeback	• Transaction Data for each Transaction
Support required to request a Chargeback Reversal	• Documentation showing that each Transaction is valid, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-31: Non-Matching Card Number (ISO 4507 / P22)

Non-Matching Card Number (ISO 4507 / P22)	
Description	The Card Account in the Submission does not match the Card Account in the original Transaction.
Information provided with the Chargeback	• Transaction Data, and • Supporting documentation showing the Card Account on the Clearing Record is different than on the Submission
Support required to request a Chargeback Reversal	• Copy of the Card imprint confirming the Card Account, or • Copy of the Transaction Receipt Record from the terminal that electronically read the Card Account, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

Table 5-32: Currency discrepancy (ISO 4530 / P23)

Currency discrepancy (ISO 4530 / P23)	
Description	The Transaction was incurred in an invalid currency. Section 4.1, "Submitting Charges and Credits"
Information provided with the Chargeback	• Transaction Data

Table 5-32: Currency discrepancy (ISO 4530 / P23) (Continued)

Currency discrepancy (ISO 4530 / P23)	
Support required to request a Chargeback Reversal	• Proof that a Credit which directly offsets the Disputed Transaction has already been processed

5.6.6 Fraud Full Recourse

Table 5-33: Fraud Full Recourse Programme (ISO 4763 / FR2)

Fraud Full Recourse Programme (ISO 4763 / FR2)	
Description	The Cardmember denies authorising the Transaction and your Establishment has been placed in the Fraud Full Recourse Programme.
Information provided with the Chargeback	• Transaction Data
Support required to request a Chargeback Reversal	• Proof that you had not been placed in the Fraud Full Recourse Programme at the time of the Chargeback, or • Proof that a Credit which directly offsets the Disputed Transaction has already been processed

5.7 Compelling Evidence

a. You may provide Compelling Evidence as support to demonstrate the Cardmember participated in the Transaction, received Goods or Services, or benefited from the Transaction. If we determine that the evidence satisfies the relevant section(s) of the Compelling Evidence policy, the Issuer will review the Compelling Evidence with the Cardmember prior to making a decision on the Chargeback reversal request. Merchants are expected to provide all available information, and to only submit Compelling Evidence when the Merchant strongly believes the Cardmember participated in the Transaction, received Goods or Services, or authorised the Transaction. Only Compelling Evidence that has been gathered in compliance with Applicable Law may be relied upon. For a list of Compelling Evidence items, see Subsection 5.7.1, "Compelling Evidence for Goods/Services not received or only partially received (ISO 4554/C08)", and Subsection 5.7.2, "Compelling Evidence for Card Not Present Fraud (ISO 4540/F29)".

5.7.1 Compelling Evidence for Goods/Services not received or only partially received (ISO 4554/C08)

Table 5-34: Compelling Evidence requirements for Goods/Services not received or only partially received (ISO 4554/C08)

Item #	Allowable Compelling Evidence for Goods/Services not received or only partially received (ISO 4554/C08) Chargeback Reversal request must include one (1) of the following items:
1	For Transactions involving Goods or Services, evidence to prove that there is a link between the person who received the Goods or Services and the Cardmember (e.g., photographs, emails), or

Table 5-34: Compelling Evidence requirements for Goods/Services not received or only partially received (ISO 4554/C08) (Continued)

Item #	Allowable Compelling Evidence for Goods/Services not received or only partially received (ISO 4554/C08) Chargeback Reversal request must include one (1) of the following items:
2	For Airline or other passenger transportation Transactions, one (1) of the following must be provided: • Evidence that the Cardmember or designated passenger participated in the flight or transportation (e.g., scanned boarding pass or passenger manifest), or • Credits of frequent flyer miles or loyalty point programme rewards for the flight or travel in question, showing a direct connection to the Cardmember, or • Proof flight in question was available during airline bankruptcy proceedings, or • Evidence of additional Transactions related to the original Transaction, such as seat upgrades, baggage payment, or purchases made on board the aircraft or passenger transport, or • Itemised invoice for associated Transactions, or Or,
3	For Card Not Present Transactions where the Goods are picked up at the Merchant's location: • The Merchant must provide the Cardmember or authorised third party signature on the pickup form as well as additional proof to demonstrate that the identity of the Cardmember or authorised third party was verified at the time of pickup Or,
4	For e-commerce Transactions representing the sale of Digital Goods or Services downloaded from a Merchant's website or application or accessed online, one (1) of the following must be provided: • Proof that the Cardmember's IP address at the time of purchase matches the IP address where the digital goods were downloaded, or • Proof the Cardmember's email address provided at the time of purchase matches the email address used to deliver the digital goods, or • Proof that the Merchant's website was accessed by the Cardmember for Digital Goods or Services after the Transaction Date. Note: In addition to the above, one (1) of the following may also be provided: • Description of the Digital Goods, or • Date and time the Digital Goods were downloaded or accessed.

5.7.2 Compelling Evidence for Card Not Present Fraud (ISO 4540/F29)

Table 5-35: Compelling Evidence Requirements for Card Not Present Fraud (ISO 4540/F29)

Item #	Allowable Compelling Evidence for Card Not Present fraud (ISO 4540/F29) Chargeback Reversal request must include one (1) of the following items:
1	For Transactions involving the shipment of Goods or Services, proof that the Transaction contains a shipping address that matches a previously used shipping address from an undisputed Transaction, or
2	For Airline or other passenger transportation Transactions, one (1) of the following must be provided: • Evidence that the Cardmember participated in the flight or transportation (e.g., scanned boarding pass, or passenger manifest), or • Credits of frequent flyer miles or loyalty point programme rewards earned or redeemed for the flight or travel in question, showing a direct connection to the Cardmember, or • Proof of receipt of the flight or transportation ticket at the Cardmember's billing address, or • Proof that the Transaction contains the designated passenger name that matches a previously used passenger name from an undisputed Transaction, Or,
3	For e-commerce Transactions involving the sale of Goods or Services, provide all of the following: a. Description of Goods or Services. b. Date and time the Goods or Services were purchased and when the Cardmember downloaded, accessed, or was provided the Goods or Services. c. Proof that the Cardmember participated in at least one prior undisputed E-Commerce Transaction at the Merchant using the same Payment Credential for the same unique account in the twelve (12) months preceding the Chargeback processing date, including the following information for the undisputed Transaction(s) and disputed Transaction: i. The customer name and login information linked to the Cardmember account at the Merchant. ii. Two or more of the following, which must be the same for the previous undisputed Transaction(s) and the disputed Transaction: a. Device ID b. The full IP address c. Email address used to receive confirmation of the Transaction from the Merchant d. Proof that the Merchant verified the Cardmember on the Merchant website or platform, in order to complete the Transaction. Examples include: i. Proof that the Cardmember password was captured by the Merchant in order to complete the Transaction ii. Proof of prior history with Device ID and IP address used for the disputed Transaction iii. Proof that Two Factor Authentication was performed in order for the Cardmember to complete the Transaction iv. Proof that the Merchant validated the Card and the Cardmember at the time of the Transaction using AAV (Automated Address Verification) verification response of "Y" or CID/CVV verification response of "Y" Or,

Table 5-35: Compelling Evidence Requirements for Card Not Present Fraud (ISO 4540/F29) (Continued)

Item #	Allowable Compelling Evidence for Card Not Present fraud (ISO 4540/F29) Chargeback Reversal request must include one (1) of the following items:
4	For Recurring Billing Transactions all of the following must be provided: a. Proof that the Cardmember agreed in writing to Authorise the Merchant to bill the Cardmember's Card Account on a periodic basis for the Goods or Services. b. Cardmember name and login information linked to the Cardmember account with the Merchant. c. Proof that the Cardmember participated in at least one prior undisputed Recurring Billing Transaction for the same Goods or Services at the Merchant using the same Payment Credential for the same unique Card Account, including: i. Description of Goods or Services for the previous, undisputed Transaction(s) and the disputed Transaction. ii. Date and time of purchase of the previous, undisputed Transaction(s) and disputed Transaction. d. Evidence showing how the Merchant notified the Cardmember of the Recurring Billing Transaction, including: i. The communication sent to the Cardmember after the first customer-initiated Recurring Billing Transaction for the same Goods or Services, ii. And, if the disputed Transaction was an annual or semi-annual Merchant-Initiated Transaction, provide details about how the Merchant obtained the Cardmember's express consent of the upcoming renewal. a. Date and time of the notification regarding the upcoming Recurring Billing [renewal / Transaction] b. Communication method and the Cardmember's contact information used for the notification (e.g., if the communication was sent by email, provide the Cardmember's email address)
5	For Transactions involving the sale of website search and/or advertising services to promote consumer products or services, all of the following must be provided: a. Proof of a legally binding contract held between the Merchant and the Cardmember, and b. Details of the initial ad-service setup, including at least two (2) of the following items: i. Purchaser's IP address and geographical location at the date and time of the initial ad-service setup ii. Email address of purchaser iii. Company name or purchaser name, and c. Proof the Cardmember has accessed the Merchant's website to establish services on or before the Transaction date, and d. Proof that the device and Card used for the disputed Transaction was used in a previous Transaction that was not disputed. In addition, provide the following information that is currently linked to the Cardmember account with the Merchant: i. Device ID ii. IP address and geographical location iii. Device name (if available) e. Proof that the Cardmember received the Goods or Services, and f. Description of the Goods or Services and the date they were provided.

5.8 Inquiry Types

a. American Express tries to resolve Disputed Transactions by first using information available to us. This includes, but is not limited to, replying with a Substitute Clearing Record (Subsection 2.6.3, "Substitute Transaction Receipt") on your behalf in attempts to resolve the Disputed Transaction. American Express relies on the information previously provided by the Merchant related to the disputed transaction when generating a Substitute Clearing Record. No warranty, express or implied, is made by American Express, nor do we accept any liability regarding the accuracy, adequacy, completeness, reliability, or usefulness of the information provided by the Merchant and used in creating a Substitute Clearing Record.

b. In instances where we cannot resolve a Disputed Transaction, we will send you an Inquiry. The form of Inquiry that we will send you includes information about the Transaction in question, explanations of the material you must send us to support the Transaction, and a deadline by which your response must be received. In response to Inquiries, we will accept Compelling Evidence items (Section 5.7, "Compelling Evidence") to show that the Cardmember participated in the Transaction, received the Goods or Services, or benefited from the Transaction. In addition, when providing Proof of Delivery, a signature from the Cardmember or an authorised signer of the Card is not required.

Table 5-36: Inquiry Types

Inquiry category, reason code, and definition	Industry and supporting documentation
(6014) Does Not Recognise/ Remember/No Knowledge *(6014)* *Cardmember does not recognise or remember the Transaction.* *(6014)* *Cardmember does not recognise or remember the Card Not Present Transaction.*	The Cardmember claims to not recognise the Transaction. Please perform one of the following: • provide support and itemisation; or, • issue Credit Optional support, if available: • If the Transaction relates to shipped Goods, please include shipping details with the full delivery address.
(6003/4513) Credit Not Processed *Cardmember claims Credit is due from Merchant, but has not received the Credit.*	The Cardmember has requested Credit for Goods that were returned to your Establishment. Please perform one of the following: • issue Credit or • explain why Credit is not due along with a copy of your return policy
(6003/4554) Non Receipt of Goods/Services *Cardmember did not receive the Goods or Services.*	The Cardmember requests delivery of Goods/Services ordered but not received. Please perform one of the following: • provide the Service or ship the Goods, • issue Credit, or • provide Proof of Delivery or proof that the Cardmember received the Services in full. For other recommended supporting documentation, please refer to Section 5.7, "Compelling Evidence". When providing Proof of Delivery, a signature from the Cardmember or an authorised signer of the Card is not required.
(6003/4507) Overcharge/ Incorrect Transaction Amount *Cardmember claims that the amount of the Transaction is incorrect.*	The Cardmember claims the Transaction amount you submitted differs from the amount the Cardmember agreed to pay. Please perform one of the following: • issue Credit, or • explain why Credit is not due and provide relevant documentation.

Table 5-36: Inquiry Types (Continued)

Inquiry category, reason code, and definition	Industry and supporting documentation
(6003/4553) Damaged or Defective Goods *Goods received from the Merchant were damaged or defective. Request for return Authorisation*	The Cardmember claims the Goods received are damaged or defective and requests return Authorisation. If a return is not permitted, please provide • a copy of your return or refund policy, and • information on your efforts to resolve the claim.
(6003/4553) Repair or Replacement of Defective Goods *Goods received from the Merchant were damaged or defective. Request for repair, replacement or return instructions*	The Cardmember requests repair or replacement of damaged or defective Goods received. Please perform one of the following: • issue Credit, or • return instructions and make the appropriate repairs, or • a copy of your return/replacement policy and explain why the Goods cannot be repaired/replaced.
(6003/4513 or 4544) Goods or Services Cancelled or Returned *The Cardmember recalls the purchase, but claims to have cancelled/returned it. This category includes billings for cancelled reservations, Guaranteed Reservations Transactions, cancelled lodging/cruise deposits, cancelled recurring/continuing billing and other deposits.*	The Cardmember claims the Goods / Services were cancelled / expired or the Cardmember has been unsuccessful in an attempt to cancel the Goods / Services. Please discontinue future billings and perform one of the following: • issue Credit, or • provide a copy of your cancellation or return policy provided to the Cardmember at the time of the purchase and an explanation regarding how the Cardmember did not follow your cancellation or return policy, or • if the Transaction is a Recurring Billing Transaction, provide evidence the Cardmember has not cancelled and continues to use the Service or receive the Goods.
(6003/4553) Not as Described or Dissatisfied with Goods or Services *Goods or Services do not conform to the documented description; or the Cardmember is not satisfied with the Goods or Services that were delivered or provided.*	The Cardmember claims the Goods / Services do not conform to the documented description or they are not satisfied with the Goods / Services that were delivered or provided. Please perform one of the following: • provide proof of repair or replacement for Goods or Services that were not as described by your Establishment, or • issue Credit, or • provide a copy of terms and conditions for all Goods or Services provided including warranty information, if applicable. • advise of efforts taken to resolve the issue and/or options available for resolution.
(6003/4554) Services Not Rendered *Cardmember has not received the Goods or Services that were purchased.*	The Cardmember has requested Credit for Goods / Services that were not received from your Establishment. Please perform one of the following: • issue Credit or • provide Proof of Delivery or proof that Services were provided in full. For other recommended supporting documentation, please refer to Section 5.7, "Compelling Evidence". When providing Proof of Delivery, a signature from the Cardmember or an authorised signer of the Card is not required.

Table 5-36: Inquiry Types (Continued)

Inquiry category, reason code, and definition	Industry and supporting documentation
(6006) Fraudulent Transactions *Cardmember claims Transaction is fraudulent.*	The Cardmember claims the Transaction incurred at your Establishment is fraudulent. For a Card Present Transaction, provide: • a copy of the Clearing Record and • if applicable, an imprint of the Card, if one was taken. For a Card Not Present Transaction, provide: • a copy of the Clearing Record, • any contracts or other details associated with the purchase, and • Proof of Delivery with the Cardmember's complete and valid billing address. For other recommended supporting documentation, please refer to Section 5.7, "Compelling Evidence". When providing Proof of Delivery, a signature from the Cardmember or an authorised signer of the Card is not required.
(6003/4752) Credit Presentment Error *The Transaction should have been submitted as a Credit.*	The Cardmember claims the referenced Transaction should have been submitted as a Credit. Please perform one of the following: • issue Credit, or • provide support and itemisation for the Transaction and an explanation of why Credit is not due.
(6003/4513) Cancelled or refused *The Goods or Services were cancelled or refused.*	The Cardmember claims the Goods / Services were cancelled and /or refused. Please perform one of the following: • issue Credit, or • provide your cancellation or refund policy provided to the Cardmember at the time of the purchase, and an explanation regarding how the Cardmember did not follow your cancellation policy.
(6003/4512) Duplicate Billing *Cardmember was Charged multiple times for the same Transaction.*	The Cardmember requests Credit from your Establishment for a duplicate billing. • If your records show this is correct, please issue Credit. • If Credit is not due, provide support and itemisation of both charges and explain fully in the space below.
(6003/4513) Credit Not Presented *Credit is due but does not appear.*	The Cardmember claims that a Credit is due but has not appeared on their account. Please perform one of the following: • issue Credit, or • provide support for the Transaction and an explanation of why Credit is not due.
(6003/4515) Paid by Other Means *Transaction was paid by another form of payment.*	The Cardmember claims the Transaction was paid by another form of payment. Please perform one of the following: • issue Credit, or • provide proof that the Cardmember's payment by other means was not related to the Disputed Transaction; or • provide an explanation that you have no record of the Cardmember's other payment.

Table 5-36: Inquiry Types (Continued)

Inquiry category, reason code, and definition	Industry and supporting documentation
(6016) Cardmember Requests Support *Cardmember only requesting supporting documentation.*	The Cardmember is not disputing the Transaction at this time, but is requesting support and itemisation. Please provide this requested documentation.
(6003/4750) Vehicle Rental and Capital Damages *Cardmember has questioned the Transaction for damages/ theft or loss.*	The Cardmember has questioned the Transaction for damages / theft or loss. Please perform one of the following: • issue credit; or • provide a copy of the following documentation: ▪ Itemised rental agreement, ▪ Itemised documentation to support the Transaction, ▪ proof that the Cardmember agreed in writing to accept responsibility for the Transaction, and ▪ proof that the Cardmember agreed in writing to select American Express as the payment method for the Transaction.

5.9 Chargeback and Inquiry Monitoring

a. We monitor the number of Inquiries and Chargebacks at all Merchants and Establishments on the Network. Your Inquiries and/or Chargebacks may be considered disproportionate if any of the following conditions are present:

i. You are unable to provide supporting documentation for Transactions made at your Establishment consistently.

ii. The number of No Reply and Insufficient Chargebacks at your Establishment is deemed to be excessive relative to your prior history or industry standards.

iii. We receive a disproportionately high number of Disputed Transactions, resulting in a Chargeback or an Inquiry.

b. If any of the preceding conditions are present, we may place you or a qualifying End Beneficiary in our Fraud Full Recourse Programme (see Section 5.11, "Fraud Full Recourse Programme").

5.10 How We Chargeback

a. We may Chargeback by (i) deducting, withholding, recouping from, or otherwise offsetting against our payments to you or debiting your Bank Account, or we may notify you of your obligation to pay us, which you must do promptly and fully; or (ii) reversing a Transaction for which we have not paid you. Our failure to demand payment does not waive our Chargeback rights.

b. Chargeback will be calculated in the currency in which the Transaction was submitted with applicable conversions made in accordance with the procedures herein.

c. In the event of a Chargeback, we will not refund the Discount or any other fees or assessments, or we will otherwise recoup such amounts from you, unless stated otherwise to you by us.

5.11 Fraud Full Recourse Programme

Table 5-37: Fraud Full Recourse Programme

Fraud Full Recourse Programme
The Fraud Full Recourse Programme allows us to Chargeback any time a Cardmember disputes a Transaction based on actual or alleged fraud without the right to request a reversal of our decision to exercise our Chargeback rights. In all countries in which we operate the Fraud Full Recourse Programme, you, and where applicable, a qualifying End Beneficiary, may be placed in this programme for one or more of the following reasons: • you are in an industry we consider high risk, • An Establishment's fraud performance levels meet or exceed either the Low Tier or High Tier Programme Thresholds set forth in Subsection 5.11.1, "Low Tier and High Tier Programme Thresholds". Or, • You engage or participate in fraudulent, deceptive or unfair business practices, illegal activities, or permit (or fail to take reasonable steps to prevent) prohibited uses of the Card, **Note:** We may place you, or a qualifying End Beneficiary, in a Fraud Full Recourse Programme upon signing, or any time during the term of the Agreement upon notice to you. The above reasons are not exhaustive and we may, at our sole discretion, place you, or a qualifying End Beneficiary, in the Programme for other reasons. Placement in the Fraud Full Recourse Programme binds you to the programme terms indicated above. In the event of a conflict between this programme and any other programme, e.g., fraud liability shift programmes, the terms of the Fraud Full Recourse Programme will prevail. We will have the rights set forth in this subsection, even if we had notice of such defect at the time of payment, you have received an Authorisation and/or have complied with all other provisions of the Agreement. For the avoidance of doubt, if you, or a qualifying End Beneficiary, have been placed on the Fraud Full Recourse Programme, the programme will apply to all fraud related Cardmember disputes, including disputed Transactions that precede the application date of the programme to you by up to one (1) year.

5.11.1 Low Tier and High Tier Programme Thresholds

a. You will be placed in the Fraud Full Recourse Programme if your Establishment's fraud performance levels meet or exceed either the Low Tier or High Tier Programme Thresholds set forth in the following table:

Table 5-38: FTG Performance Tiers

Programme Tier	Performance	Programme Actions
Low Tier Programme Threshold	• The monthly fraud to gross* Transactions ratio at an Establishment equals or exceeds **0.9% and** • An Establishment has a minimum fraud amount of **USD $25,000** in a one (1) month period	• If you do not reduce your fraud performance levels below the Low Tier Programme Threshold for three (3) consecutive calendar months following the date of our notice to you, you will be subject to Fraud Full Recourse (FFR) Chargebacks and will no longer qualify for SafeKey fraud liability shift (see Subsection 7.1.1, "American Express SafeKey Fraud Liability Shift"). • To exit the Fraud Full Recourse Programme, see Subsection 5.11.2, "Removing a Merchant from the Fraud Full Recourse Programme".
High Tier Programme Threshold	• The monthly fraud to gross* Transactions ratio at an Establishment equals or exceeds **1.8% and** • An Establishment has a minimum fraud amount of **USD $50,000** in a one (1) month period	• Following the date of our notice to you, you will be subject to Fraud Full Recourse (FFR) Chargebacks and will no longer qualify for SafeKey fraud liability shift (see Subsection 7.1.1, "American Express SafeKey Fraud Liability Shift"). • To exit the Fraud Full Recourse Programme, see Subsection 5.11.2, "Removing a Merchant from the Fraud Full Recourse Programme".

* For the purposes of this table only, Fraud to Gross (FTG) means the ratio of fraudulent Transactions as compared to total Transaction volume, provided that both volume amounts are in the same currency.

b. A Merchant will remain in the FFR Programme until their FTG ratio falls below the requirements. Refer to Subsection 5.11.2, "Removing a Merchant from the Fraud Full Recourse Programme" for more information.

5.11.2 Removing a Merchant from the Fraud Full Recourse Programme

a. A Merchant that is in the Fraud Full Recourse Programme because of its fraud performance levels will be removed from the Fraud Full Recourse Programme and the Merchant's SafeKey fraud liability shift will be reinstated (provided Merchant is enrolled in SafeKey Programme) if Merchant's fraud performance levels fall below either of the following thresholds:

i. The fraud to gross Transactions ratio at an Establishment is below 0.9% per month for three (3) consecutive months, or

ii. An Establishment's fraud amount is below USD $25,000 per month for three (3) consecutive months.

5.12 Ways to Receive Chargebacks and Inquiries

a. American Express has a variety of options for the exchange of Chargeback and Inquiry information with you. In addition to the traditional paper by mail method, you can access your Merchant Account online to receive and respond to Chargebacks and Inquiries.

b. Managing your Merchant Account online offers the following benefits:

- allows you to address Disputed Transactions and urgent Chargebacks and Inquiries,
- helps eliminate the risk of mail delays and shuffling through stacks of paper, and
- allows you to upload and send scanned supporting documentation.

c. If you prefer, you can receive and respond to Inquiries by paper via mail.

5.13 Response Methods

a. You may respond to Chargebacks and Inquiries through various channels depending on how you receive your Chargebacks and Inquiries.

Table 5-39: Response Methods

Online	Mail	Fax
You may respond to Chargebacks and Inquiries online at www.americanexpress.com/merchant: • Respond to Chargebacks and Inquiries directly without paperwork • Address Chargebacks and Inquiries Online is our preferred method for handling Chargebacks and Inquiries.	If you prefer to mail your responses, use the Disputed Transaction addresses listed in the Contact Information page of your Terms and Conditions.	You may fax replies directly to Customer Service Disputes. Fax numbers are typically found on the dispute notification, listed in the Contact Information page or the disputes fax number found on our website. For paper by mail Disputes, we prefer that you fax all responses and include the Inquiry cover sheet. This will ensure the timely receipt of your documentation.

b. For mail and fax responses, you must include the claim form with your response. The claim form must include the case number. Each page of the supporting documentation for the Disputed Transaction must also include the case number. If the documentation does not contain the case number, or you are unable to locate the correct case number, you must include a copy of the initial Chargeback or Inquiry letter with your response. Failure to provide the correct case number or the cover letter may result in a liability to you.

AMERICAN EXPRESS

Indirect Acceptors

6

6.1 Indirect Acceptors

a. This Chapter 6, "Indirect Acceptors", states additional requirements applicable to Indirect Acceptors.

b. Indirect Acceptors are bound by the terms of their Agreement and applicable provisions of the *Merchant Regulations*. American Express has the right, in our sole discretion, to approve and designate a Merchant as an Indirect Acceptor.

6.2 Indirect Acceptor Models

a. Indirect Acceptors may operate through one or more different models including, but not limited to, the following:

   i. Bill Payment Provider

   ii. Marketplaces

   iii. Digital Wallet Operators allowing Cardmembers to make purchases or transfer funds through one or more methods:

      a. Instalment Payment Transaction (sometimes called "Buy Now Pay Later")

      b. Peer to Peer (P2P) Transaction

      c. Staged Back-to-Back Transaction

      d. Stored Value Transaction (sometimes called "Top Up Wallet")

6.3 General Requirements for Indirect Acceptors

a. Indirect Acceptors are liable for all acts, omissions, and other adverse conditions caused by the End Beneficiaries.

b. Indirect Acceptors are fully responsible and financially liable for all Transactions and all other issues involving End Beneficiaries. In addition, we may place you in one of our Chargeback programmes. See Section 5.11, "Fraud Full Recourse Programme", to understand the Chargeback policies that apply to Indirect Acceptors.

c. Indirect Acceptors must comply with Applicable Law, including but not limited to, the Anti-Money Laundering (AML), Anti-Terrorist Financing (ATF), and sanction screening requirements that take into consideration the End Beneficiary of the Transaction.

d. For all Indirect Acceptor models except Digital Wallet Operators engaged in Stored Value Transactions and Marketplaces, Indirect Acceptors must screen End Beneficiaries as customers, applying reasonable measures to obtain and verify the customer identification information for each End Beneficiary in accordance with Applicable Law.

e. Indirect Acceptors that fail to comply with the requirements of this section may be subject to non-compliance fees as stated in Subsection 8.4.3, "Payment Facilitators and Indirect Acceptor Fees".

f. Indirect Acceptors are classified as a restricted industry and must comply with the requirements set out in Subsection 8.2.1, "Prohibited or Restricted Industries".

g. In addition to the requirements set forth above, Indirect Acceptors must:

   i. Comply with Section 2.4, "Card Not Present Charges".

   ii. Comply with Subsection 2.5.4, "Merchant-Initiated Transactions" when processing non-Cardmember-Initiated-Transactions.

   iii. Monitor End Beneficiaries for potentially suspicious or unusual activity, and ensure requisite reports are filed in accordance with Applicable Law.

   iv. Obtain and maintain all required licenses and approvals necessary to conduct business, including Stored Value Transaction requirements to hold funds in reserve.

   v. Not facilitate payments to End Beneficiaries in prohibited or restricted industries. See Subsection 8.2.1, "Prohibited or Restricted Industries".

   vi. Accept the Card only to facilitate payments to eligible End Beneficiaries. Other Indirect Acceptors are not eligible End Beneficiaries, with the exception of Marketplaces.

vii. Perform verification checks, credit checks, "Know Your Customer," and AML checks of End Beneficiaries in accordance with all Applicable Laws and otherwise as we may require, providing American Express, on request, copies of your policies governing these checks and otherwise responding to American Express' request about the performance of these checks.

viii. Provide the mandatory data elements as required in the *Technical Specifications*, see Subsection 1.4, "Compliance with our Specifications") with each Authorisation request and Submission.

ix. Submit accurate data and conduct periodic checks to ensure accuracy.

x. Include an indicator identifying the Indirect Acceptor model, a separate Merchant number for each Transaction type, and the Card Acceptor name. See the *Technical Specifications* for more information.

xi. Provide the MCC field in both the Authorisation request and Submission as listed in Table 6-1: Indirect Acceptors MCCs

h. American Express may request additional information about End Beneficiaries when needed to validate compliance. Merchants must provide American Express with the information about their End Beneficiaries as specified.

Table 6-1: Indirect Acceptors MCCs

Indirect Acceptor/Transaction Type	Merchant Category Code (MCC)
Bill Payment Provider	The appropriate MCC for each End Beneficiary
Instalment Payment Transaction	The appropriate MCC for each End Beneficiary
Marketplaces	The appropriate MCC that best describes the majority of the Goods and Services throughout the Marketplace
Peer to Peer (P2P) Transaction	MCC 6538 (P2P payment transfer of funds)
Staged Back-to-Back Transaction	The appropriate MCC for each End Beneficiary
Stored Value Transaction	MCC 6540 (Stored Value/Gift Card Purchase/Load)

i. Refer to the *Codes Reference Guide* for more information.

6.3.1 Additional Requirements for Bill Payment Providers

a. Bill Payment Providers must comply with the following:

i. Each Transaction must be individually Authorised and Submitted. Do not aggregate Transactions.

ii. Do not make payments to individuals. Only pay End Beneficiaries who are registered businesses, with the exception of rental payments.

iii. Disclose to the Cardmember that the Bill Payment Provider is the Merchant, is providing a financial service to the Cardmember by paying the End Beneficiary on the Cardmember's behalf, and that the Bill Payment Provider is not the seller of the Goods and Services.

iv. Facilitate payments only to End Beneficiaries that are located in the same country as the Bill Payment Provider, and, in all cases, only in a country where you are authorised to accept Cards, except for EEA & UK Bill Payment Providers which may facilitate payments to End Beneficiaries that are located in other EEA & UK countries.

v. When facilitating payments on behalf of consumers, only pay End Beneficiaries that are in the industries listed in Table 6-2: Permitted Industries for Bill Payment Providers Facilitating Consumer Payments.

vi. When facilitating payments on behalf of businesses, in addition to the prohibited and restricted industries set forth in Section 8.1, "Country Specific Policies", you must not pay End beneficiaries that are listed in the Table 6-3: Excluded Industries for Bill Payment Providers Facilitating Business Payments.

Table 6-2: Permitted Industries for Bill Payment Providers Facilitating Consumer Payments

MCC	Description
4814	Telecommunications Services, including Local and Long Distance Calls, Credit Card Calls, Calls Through Use of Magnetic-Stripe-Reading Telephones, and Fax Services
4899	Cable and Other Pay Television Services
4900	Utilities – Electric, Gas, Water, and Sanitary
6300	Insurance Sales, Underwriting, and Premiums
6513	Real Estate Agents and Managers – Rentals
7523	Parking Lots and Garages
7911	Dance Halls, Studios, and Schools
7997	Membership Clubs (Sports, Recreation, Athletic), Country Clubs, and Private Golf Courses
8011	Doctors and Physicians – Not Elsewhere Classified
8062	Hospitals
8099	Medical Services and Health Practitioners – Not Elsewhere Classified
8211	Elementary and Secondary Schools
8220	Colleges, Universities, Professional Schools, and Junior Colleges
8241	Correspondence Schools
8244	Business and Secretarial Schools
8249	Trade and Vocational Schools
8299	Schools and Educational Services – Not Elsewhere Classified
8351	Child Care Services
9211	Court Costs, including Alimony and Child Support
9222	Fines
9311	Tax Payments
9399	Government Services – Not Elsewhere Classified

Note: MCC 9311 (Tax Payments) is not allowed for consumer payments in Australia.

Table 6-3: Excluded Industries for Bill Payment Providers Facilitating Business Payments

MCC	Description
3000-3350, 4511	Airline/Charter/Air Carrier

Table 6-3: Excluded Industries for Bill Payment Providers Facilitating Business Payments (Continued)

MCC	Description
3351-3500, 7512	Car Rental Agencies
3501-3999, 7011	Lodging (Hotels, Motels, Resorts, Central Reservations)
4411	Cruise Lines (including onboard shops)
7012	Timeshares

6.3.2 Additional Requirements for Instalment Payment Transactions

a. Digital Wallet Operators that provide Instalment Payment Transactions must comply with the following:

i. Do not charge the Cardmember interest or any other finance charges, other than late payment fees.

ii. Disclose all material terms of the instalment agreement to the Cardmember including, but not limited to, the amount and frequency of the Instalment Payment Transactions, and any late payment fees.

iii. Provide Transaction details to Cardmembers via mobile application or website about each instalment Transaction, including:

a. Description of each individual purchase, including the name of the End Beneficiary

b. Date and amount of each individual purchase

c. Date and amount of each instalment charge for that individual purchase

d. Number of instalments paid by the Cardmember and number of instalments remaining in the series (e.g., "1 of 4")

iv. Submit an Authorisation request for each individual Instalment Payment Transaction at the time the instalment is due, for the amount of the instalment, not the full purchase amount.

v. Do not submit an Authorisation request nor submit any related future instalments if a purchase is disputed, and only resume instalments if the Chargeback or Disputed Charge is resolved in the Instalments Payment Provider's favour.

vi. Have a direct contract with the End Beneficiary except in the limited circumstance where a third-party facilitates payments to the End Beneficiaries, in such instances the following requirements apply to the Instalment Payment Provider, the third-party agent, or both:

a. Instalment Payment Provider must have a direct contract with your third-party agent.

b. Instalment Payment Provider or the third-party agent must provide End Beneficiary data elements in accordance the *Technical Specifications*. The Instalment Payment Provider remains responsible and otherwise liable for the third-party agent's compliance with this requirement and any omission or failure to perform does not relieve the Instalment Payment Provider of their obligations to comply with the requirements in this section.

c. Notwithstanding the foregoing, American Express reserves the right to revoke this exception at any time at our sole discretion.

vii. Facilitate payments only to End Beneficiaries that are located in the same country as the Instalment Payment Provider except for EEA & UK Instalment Payment Providers which may facilitate payments to End Beneficiaries that are located in other EEA & UK countries.

viii. In addition to prohibited and restricted industries set forth in Subsection 8.2.1, "Prohibited or Restricted Industries", do not accept the Card to facilitate payments for End Beneficiaries in industries listed in Table 6-4: Excluded Industries for Instalment Payment Transactions.

Note: Instalment Payment Transactions charged by Digital Wallet Operators are not considered Recurring Billing Transactions or Delayed Delivery Charges.

Table 6-4: Excluded Industries for Instalment Payment Transactions

MCC	Description
0742	Veterinary Services
3000-3350, 4511	Airline and Air Carriers
3351-3500, 7512	Car Rental Agencies
3501-3999, 7011	Lodging (Hotels, Motels, and Resorts)
4119	Ambulance Services
4411	Cruise Lines (including onboard shops)
4722	Travel Agencies and Tour Operators
4814	Telecommunications Services
4900	Utilities
5122	Drugs, Drug Proprietaries, and Druggists' Sundries
5813	Nightclubs
5968	Long-term Subscriptions
5976	Orthopedic Goods and Prosthetic Devices
6010, 6011	Cash-like Transactions
6300, 6381, 6399	Insurance
6513	Real Estate Agents and Managers – Rentals
6538	P2P Payments
7012	Timeshares
7280, 8062	Hospitals and Private Hospitals
7997	Lifetime Memberships
8050	Nursing and Personal Care Facilities
8071	Medical Dental Laboratories
8099	Medical Services and Health Practitioners – Not Elsewhere Classified
9222	Fines
9311	Tax Payments

6.3.3 Additional Requirements for Marketplaces

a. Marketplaces must comply with the following:

i. Have an agreement with the End Beneficiary binding the End Beneficiary to the Marketplace's terms of service for participating in the Marketplace platform.

ii. Provide Transaction details to Cardmembers for each purchase, including:
   a. A description of each individual purchase, including the name of the End Beneficiary
   b. Date and amount of each individual purchase
iii. Display the Marketplace's name or brand more prominently than the End Beneficiaries on your website or mobile application.

b. In addition to prohibited and restricted industries set forth in Section 8.2.1, "Prohibited or Restricted Industries", do not accept the Card to facilitate payments for End Beneficiaries in industries listed in Table 6-5: Excluded Industries for Indirect Acceptors.

6.3.4 Excluded Industries for Indirect Acceptors

a. In addition to prohibited and restricted industries set forth in Section 8.2.1, "Prohibited or Restricted Industries", do not accept the Card to facilitate payments for End Beneficiaries in industries listed in Table 6-5: Excluded Industries for Indirect Acceptors

i. Marketplaces
ii. Staged Back-to- Back (DWO)
iii. Stored Value Transactions (DWO)

Table 6-5: Excluded Industries for Indirect Acceptors

MCC	Description
3000-3350, 4511	Airline/Charter/Air Carrier
3351-3500, 7512	Car Rental Agencies
3501-3999, 7011	Lodging (Hotels, Motels, Resorts, Central Reservations)
4411	Cruise Lines (including onboard shops)
7012	Timeshares

American Express may modify the excluded industries listed in Table 6-5: Excluded Industries for Indirect Acceptors, Table 6-4: Excluded Industries for Instalment Payment Transactions, and Table 6-5: Excluded Industries for Indirect Acceptors at any time at our sole discretion, in accordance with Section 1.2, "Changes in the Merchant Regulations". If an Indirect Acceptor accepts the Card to facilitate payments to End Beneficiaries in an excluded industry, we may exercise Chargebacks, suspend acceptance of Cards by you, and/or terminate the Agreement.

AMERICAN EXPRESS

Fraud Prevention

7

7.1 American Express SafeKey Programme

a. The American Express SafeKey Programme ("SafeKey Programme") enables Merchants to verify Cardmembers during the online Authentication process in order to help reduce the likelihood of American Express Card fraud.

b. The SafeKey Programme does not eliminate online fraud, especially where no authentication occurs. You must continue to employ other reasonable fraud mitigation practices and continue to perform fraud screening to mitigate fraud.

c. American Express offers different versions of the SafeKey Programme, supporting different types of Transactions. Your Establishments must use the version of SafeKey that supports the types of Transactions you process. For additional information about the American Express SafeKey Programme, please refer to the relevant *SafeKey Implementation Guide*, *SafeKey Protocol Guide*, and *Technical Specifications* which are available at www.americanexpress.com/merchantspecs.

d. To participate in the SafeKey Programme, your Establishments must:

   i. complete the required SafeKey technical integration with your SafeKey Service Provider;

   ii. comply with the relevant *SafeKey Implementation Guide* and the *SafeKey Protocol Guide*, as may be updated from time to time, which are available at www.americanexpress.com/merchantspecs;

   iii. provide complete and accurate data for SafeKey Charges, as specified in the relevant *SafeKey Implementation Guide* and the *SafeKey Protocol Guide* and Specifications; and

   iv. comply with the SafeKey branding requirements detailed in the *American Express SafeKey Logo Guidelines*, available at www.americanexpress.com/merchantspecs.

e. We may suspend, terminate, amend, or prevent access to the SafeKey Programme at any time, with or without notice to you. We shall not be liable and shall have no obligation to you in the event we suspend, terminate, amend, or prevent access to the SafeKey Programme. If you do not agree with the modified or current SafeKey Programme, you must cease participation.

7.1.1 American Express SafeKey Fraud Liability Shift

a. Under the SafeKey Programme, we will not exercise our Chargeback rights for certain types of fraudulent Transactions, including Card Not Present Chargebacks ("SafeKey Fraud Liability Shift"). The SafeKey Fraud Liability Shift does not apply to Disputed Charges involving dispute reasons other than fraud (e.g., the SafeKey Fraud Liability Shift does not apply to Goods or Services disputes).

b. To qualify for the SafeKey Fraud Liability Shift, in addition to the requirements in Section 7.1, "American Express SafeKey Programme" above, you must comply with the additional requirements below:

   i. The SafeKey Charge was SafeKey Authenticated and received Electronic Commerce Indicator (ECI) 5, or SafeKey Attempted and received an ECI 6;

   ii. Do not exceed a fraud ratio of 0.9% and fraud Charges of USD $25,000 calculated monthly, based on all Charges as determined by American Express. If at any time you exceed the Fraud to Sales Ratio you must work with us to reduce the number of Disputed Charges at your Establishment;

   iii. If your Establishment is located outside of Japan, the SafeKey Electronic Commerce Indicator was provided in both the Authorisation request and the Charge submission; and

   iv. For Establishments located within Japan, the SafeKey Electronic Commerce Indicator was provided in the Authorisation request.

c. For the avoidance of doubt, we reserve the right, in our sole discretion, to revoke, modify, or terminate your Establishment's eligibility for the SafeKey Fraud Liability Shift where:

   i. You do not meet any of the requirements listed above (e.g., you exceed the Fraud to Sales Ratio, or where you do not provide clear and accurate data for SafeKey Charges);

   ii. You submit SafeKey authentication data to us that is different from the authentication data used during the SafeKey authentication process; or

   iii. You submit authentication data that is invalid or reused authentication data from a different SafeKey Charge.

d. **Note:** Some American Express Cards, such as Gift Cards, where available, are not eligible for the SafeKey Programme, as they cannot be fully authenticated by the Issuer at the time of the Charge.

7.2 Fraud Prevention Tools

a. As available, you should use our Automated Address Verification (AAV), Address Verification Service (AVS), Enhanced Authorisation, and CID services (or any other similar fraud prevention tools that we may make available to you from time to time). These are methods to help you mitigate the risk of fraud but are not guarantees that a Charge will not be subject to Chargeback. You must be certified for AAV, AVS, and Enhanced Authorisation in order to use these fraud prevention tools. We may suspend, terminate, amend or prevent access to the fraud prevent tools at any time, with or without notice to you. We will not be liable and will have no obligation to you in the event we suspend, terminate, amend, or prevent access to the fraud prevention tools.

7.3 Strong Customer Authentication

a. If you have Establishments in the EEA or UK, those Establishments must support solutions allowing us to perform Strong Customer Authentication of the Cardmember for Charges made by Digital Orders. If you fail to allow us to perform Strong Customer Authentication, Charges made by Digital Orders may be declined.

b. If your Establishments in the EEA or UK accept Charges made by Digital Orders, they should participate in our American Express SafeKey Programme.

AMERICAN EXPRESS

Regulations for Specific Industries

8.1 Country Specific Policies

a. The tables below define the applicable requirements and thresholds in each Country.

- **i.** Contact Limit: Maximum Amount for a Contact Transaction with No CVM. See Subsection 2.3.2, "No Signature/No PIN Programme".
- **ii.** Contactless Limit: Maximum Amount for a Contactless Transaction with No CVM. See Subsection 2.3.5, "Contactless Chip Cards"
- **iii.** Aggregated Limit: Aggregated Charge Limit. See Subsection 2.5.2, "Aggregated Transactions"
- **iv.** Retention: Record Retention Period
- **v.** EMV FLS: Transactions in these countries are subject to the following Chargebacks: EMV counterfeit (ISO 4798) listed as "Counterfeit" and/or EMV Lost/Stolen/Non Received (ISO 4799) listed as "Lost/Stolen". See Subsection 5.6.3, "Fraud".
- **vi.** POS Capability: POS Terminals must be capable and Cards must be accepted in accordance with Chip and/or PIN requirements listed in Section 2.3, "In-Person Charges".

b. Refer to the tables listed below to find a specific country.

- Table 8-1: Americas/Latin America and the Caribbean (LAC)
- Table 8-2: Asia Pacific (APAC)
- Table 8-3: Europe/Middle East/Africa (EMEA)

Table 8-1: Americas/Latin America and the Caribbean (LAC)

Country	Contact Limit	Contactless Limit	Aggregated Limit	Retention	EMV FLS	POS Capability
Argentina	ARS 80,000	ARS 80,000	USD 15	36 months	Counterfeit	Chip Only Country
Canada	CAD 50	CAD 250	USD 15	24 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Mexico	MXN 250	MXN 1,500	USD 15	12 months	Counterfeit, Lost/Stolen	Chip and PIN Country
United States	USD 200	USD 200	USD 15	24 months	Counterfeit, Lost/Stolen	Chip and PIN Country

Table 8-2: Asia Pacific (APAC)

Country	Contact Limit	Contactless Limit	Aggregated Limit	Retention	EMV FLS	POS Capability
Australia	AUD 35	AUD 200	AUD 15	12 months	Counterfeit	Chip and PIN Country
Hong Kong (Special Administrative Region of China)	HKD 1,000	HKD 1,000	USD 15	12 months	Counterfeit	Chip Only Country
India	INR 0	INR 5,000	USD 15	12 months	Counterfeit	Chip and PIN Country
Japan	JPY 15,000	JPY 15,000	JPY 1,200	12 months	Counterfeit	Chip Only Country
New Zealand	NZD 100	NZD 200	USD 15	12 months	Counterfeit	Chip and PIN Country
Singapore	SGD 200	SGD 200	USD 15	12 months	Counterfeit	Chip Only Country

Table 8-2: Asia Pacific (APAC) (Continued)

Country	Contact Limit	Contactless Limit	Aggregated Limit	Retention	EMV FLS	POS Capability
Taiwan (Province of China)	TWD 3,000	TWD 3,000	USD 15	12 months	Counterfeit	Chip Only Country

Table 8-3: Europe/Middle East/Africa (EMEA)

Country	Contact Limit	Contactless Limit	Aggregated Limit	Retention	EMV FLS	POS Capability
Austria	EUR 0[1]	EUR 50	EUR 15	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Belgium	EUR 0[1]	EUR 50	EUR 15	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Denmark	DDK 0[1]	DDK 350	DDK 100	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Finland	EUR 0[1]	EUR 50	EUR 10	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
France	EUR 0[1]	EUR 50	EUR 15	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Germany	EUR 0[1]	EUR 50	EUR 15	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Iceland	ISK 0[1]	ISK 7,500	10 GBP	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Italy	EUR 0[1]	EUR 50	EUR 15	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Luxembourg	EUR 0[1]	EUR 50	EUR 15	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Netherlands	EUR 0[1]	EUR 50	EUR 15	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Norway	EUR 0[1]	NOK 500	NOK 100	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Spain	EUR 0[1]	EUR 50	EUR 15	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
Sweden	SEK 0[1]	SEK 400	SEK 100	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country
United Kingdom	GBP 0[1]	GBP 100	GBP 10	18 months	Counterfeit, Lost/Stolen	Chip and PIN Country

[1] Unless it is a Transaction conducted at an unattended terminal for transport fares and parking fees only. The limit for such Transactions will be the corresponding Maximum Amount for a Contactless Transaction with No CVM.

8.2 Industry Specific Policies

8.2.1 Prohibited or Restricted Industries

a. Some Merchants are not eligible (or may become ineligible) to accept the Card. We may suspend acceptance of Cards by you or any of your Establishments or terminate the Agreement immediately without prior notice if we determine or have reason to believe, in our sole discretion, that you meet any of the following conditions:

- **i.** 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.
- **ii.** You do not have a verifiable physical address and can only be reached by telephone.
- **iii.** You or any of your Establishments are involved in (or knowingly participate in or have participated in) fraudulent or illegal activities.
- **iv.** You or any of your Establishments are identified as sponsors of international terrorism, as warranting special measures due to money laundering concerns, or as noncooperative with international AML principles or procedures.
- **v.** You are listed on the List of Names made subject to the Regulations Establishing a List of Entities pursuant to subsection 83.05(1) of the Criminal Code of Canada or the United Nations Suppression of Terrorism Regulations or any other such list or regulation that may exist now or in the future.
- **vi.** You are listed on the U.S. Department of Treasury, Office of Foreign Assets Control, Specially Designated Nationals and Blocked Persons List.
- **vii.** You are listed on the U.S. Department of State's Terrorist Exclusion List.
- **viii.** You are located in or operating under a 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 AML principles or procedures by an intergovernmental group or organisation of which the United States is a member.
- **ix.** Your verifiable physical address is not located in an authorised jurisdiction.
- **x.** You or any of your Establishments fall into one of the categories and/or accept Transactions for the prohibited activities displayed in Table 8-4: Prohibited/Restricted Industries.

b. In order to accept the Card in an industry classified as restricted, you must obtain written permission from us to accept Transactions in these industries. We may, at our full discretion, approve or deny such requests. We may suspend acceptance of Cards by you or any of your Establishments or terminate the Agreement immediately without prior notice if we determine or have reason to believe, that you or any of your Establishments are performing a restricted activity or operating in a Restricted Industry without our written permission.

Table 8-4: Prohibited/Restricted Industries

Industry Category	Description	Prohibited Regions	Restricted Regions	MCC
Air Charters	A company that provides on demand aircraft.	–	All Regions	–
Airlines	A company that provides scheduled Air transport for travelling passengers and freight. Airlines are recognised with an air operating certificate or license issued by a governmental aviation body. Airlines have an assigned ARC / IATA / ICAO callsign.	–	All Regions	–
Auction Houses	A company that runs auctions.	–	All Regions	–
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.	EEA/UK	All Other Regions	9223

Table 8-4: Prohibited/Restricted Industries (Continued)

Industry Category	Description	Prohibited Regions	Restricted Regions	MCC
Bankruptcy Services	A company or agency that is in the business of recovering money owed on delinquent accounts or supporting the bankruptcy process.	All Regions	–	–
Bullion	Bulk metal in bars or ingots. Examples include: • Gold, silver, platinum, or palladium bullion • Gold, silver, platinum, or palladium bars • Precious metals	–	All Regions	–
Cash at point of sale from a Non-Financial Institution / Cash on Card	A cash-like Transaction from a non-financial Institution. Examples include: • Money Orders • Post Office • Peer to Peer (P2P) • Funding source for payroll	–	All Regions	6051
Charity	A non-profit, non-political organisation that collects donations, including fundraising. This category also includes donation crowdfunding merchants that accept donations on behalf of individuals raising money for various causes without any expectation of repayment and without any additional perceived or actual financial or tangible benefit.	–	All Regions	8398
Cheque cashing / guarantee	A business that provides customers with a way to turn a cheque into cash without having to rely on a bank account.	All Regions	–	–
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.	All Regions	—	—
Collection Agencies	A company that lenders use to recover funds that are past due. Examples include: debt collection agencies, factoring companies, and liquidators.	EEA/UK	All Other Regions	7322
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 – Rental (MCC 6513).**	EEA/UK	All Other Regions	—
Credit Financing	A merchant that provides financing to customers, earning revenue on that financing via fees and interest. Examples include: credit cards, personal loans, student loans, Buy Now Pay Later (BNPL) wallets, car loans, mortgage payments, and loan crowdfunding.	EEA/UK	All Other Regions	6010 6011 6012 6051
Credit Restoration	A service aimed at improving credit ratings by disputing errors and outdated claims with credit bureaus.	All Regions	—	—

Table 8-4: Prohibited/Restricted Industries (Continued)

Industry Category	Description	Prohibited Regions	Restricted Regions	MCC
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.	All Regions	—	6051
Debt Repayment (past due or defaulted)	A company collecting payment of overdue debt. Examples include: a payment to a collection agency, factoring company, liquidator, or insolvency practitioner/ lawyer.	All Regions	—	—
Digital File Hosting (Cyberlockers)	Online data hosting services that provide remote storage space within a secure storage architecture; they can be accessed globally over the internet; Cyberlockers are also referred to as online storage or cloud storage.	—	All Regions	4816
Door-to-Door Sales	Unsolicited individual (who may go from door to door) selling Goods and/or Services with immediate payment expected.	—	All Regions	5963
Escort Services	A business, agency or person who, for a fee, provides or offers to provide a companion.	EEA/UK	All Other Regions	7273
Foreign Exchange	A business or financial institution that has the legal right to exchange one currency for another currency.	—	All Regions	6051
Gambling and Gaming for Value	The wagering or payment of money or something of value on an event with an uncertain outcome, with the primary intent of winning money or material Goods (excluding traditional and temporary retail promotions). Examples include: • Regulated (real money) betting, including casino, poker, sports betting, lottery tickets • Advance-deposit wagering, including horse/dog racing • Fantasy sports, pay-to-play games that award monetary prizes • Skill-based, pay-to-play games that award monetary prizes • Games of chance that are not free to enter and award monetary prizes • Social casinos that involve at least some payment (such as "freemium" models) and include prizes of monetary value • Government-owned and other lotteries • Gambling chips • Gambling credits	EEA/UK	All Other Regions	7800 7801 7802 7995 9406
Indirect Acceptors	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.	—	All Regions	—

Table 8-4: Prohibited/Restricted Industries (Continued)

Industry Category	Description	Prohibited Regions	Restricted Regions	MCC
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, mutual funds) • Investment on futures, contracts, and commodities trading • Equity crowdfunding	EEA/UK	All Other Regions	—
Licensed Insolvency Practitioners	Licensed insolvency practitioners	EEA/UK	All Other Regions	—
Marijuana/cannabis-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.*	EEA/UK, U.S.	All Other Regions	—
Multi-level Marketing / Pyramid Selling	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.	—	All Regions	5966 5967
Non-Travel Related Memberships	Subscriptions where the Goods or Services are paid more than one month in advance.	—	All Regions	—
Online Adult Entertainment	A business or Entity that provides internet adult digital content.	All Regions	—	—
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.	All Regions	—	—
Payment Facilitators	An entity whose business model provides that it accepts the Card on behalf of third parties (Sponsored Merchants). Formerly referred to as "Payment Aggregators", "Payment Service Provider" or "PSP" in our materials.	—	All Regions	—
Pharmacies (Card Not Present)	Online pharmacies selling prescription drugs / products.	—	All Regions	5122 5912
Political Party Donations	Contributions, funds, Goods, or Services raised to promote the interests for a national, state, or local political party, candidate or campaign.	—	All Regions	8651

Table 8-4: Prohibited/Restricted Industries (Continued)

Industry Category	Description	Prohibited Regions	Restricted Regions	MCC
Prostitution	A person or business providing sexual services in return for payment.	EEA/UK	All Other Regions	—
Real Estate Down Payments	An initial payment when the real estate is purchased on the Card.	EEA/UK	All Other Regions	6012 6051
Telemarketing -Travel Related	A business that telemarkets travel related products or services or other travel arrangements.	—	All Regions	5962
Timeshares	The selling of part ownership of a property for use as a holiday home whereby a card member can buy the right to use the property for the same fixed period annually.	—	All Regions	—
Tobacco and Smokeless Tobacco Retailers (Card Not Present)	A business that sells tobacco, smokeless tobacco, and e-cigarettes online.	—	All Regions**	5993
Top-up wallet managed by Merchants not Intermediaries	Functionality that provides a Stored Value, a feature that allows funds to be loaded into a digital wallet for subsequent payments, including purchases of Goods and Services, at single or multiple payment acceptors.	—	All Regions	—
Travel Agencies & Tour Operators	A business that provides travel information and booking services.	—	All Regions	4722
Unregulated massage parlours	A massage parlour that is not registered with a governing body.	EEA/UK	All Other Regions	7297
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.	EEA/UK	All Other Regions	6051
Wine Futures (En Primeur)***	The selling of wine whereby the Cardmember commits to purchasing the wine still maturing in the barrel, which is then bottled and shipped at a later date. This category excludes investment in wine for commodities trading.	—	EEA/UK	—
Wire Transfers In-Person (not online)	A business that specialises in the transfer of money from one location to another.	All Regions	—	4829

* For the EEA/UK, this excludes products manufactured using marijuana derivatives within legal limits to the extent permissible by Applicable Law, for example, cannabidiol (CBD) drinks and oils.

**Vaping products are prohibited in Australia for retail sales, but permitted in pharmacies. All other tobacco related products are restricted.

***In countries outside the EEA and UK, this category is incorporated into the description of investments.

We have the right, in our sole discretion, whether or not to approve you as an eligible Merchant in a restricted industry.

Contact your American Express representative or Merchant Services if you have any questions about any of the industries in Table 8-4: Prohibited/Restricted Industries.

8.2.2 Charitable Donations

a. If you accept the Card for charitable donations, you represent and warrant that you are a non-profit organisation and are registered as a charity in the country.You may accept the Card only for charitable donations that are either 100% tax-deductible to the Cardmember, or in payment of Goods or Services

where at least 75% of the Charge is tax-deductible to the Cardmember. Notwithstanding the foregoing, charitable donations may be non-tax deductible if required under Applicable Law.

8.2.3 Insurance

a. If any of your Goods or Services are sold or billed by Independent Agencies, then you must provide to us a list of such Independent Agencies and notify us of any subsequent changes in the list. We may use this list to conduct mailings that encourage such Independent Agencies to accept the Card. We may mention your name in such mailings, and you will provide us with a letter of endorsement or assistance as we may require.

b. You will use your best efforts to encourage Independent Agencies to accept the Card. We acknowledge that you have no control over such Independent Agencies.

c. From time to time we may establish marketing campaigns that promote Card acceptance specifically at your Establishments or, generally, at insurance companies. You acknowledge that a necessary purpose for which you submit Cardmember Information that is responsive to such marketing campaigns includes our use of that information to perform back-end analyses to determine the success of such marketing campaigns. The Agreement does not authorise either party to enter into any marketing or cross-selling arrangements for insurance products.

d. We undertake no responsibility on your behalf for the collection or timely remittance of premiums.

e. You will indemnify, defend, and hold harmless us and our Affiliates, successors, and assigns from and against all damages, liabilities, losses, costs, and expenses, including legal fees, to Cardmembers (or former Cardmembers) which we or our Affiliates, successors, or assigns do or will suffer or incur and which arise or are alleged to have arisen from your termination or other action regarding their insurance coverage.

f. This Section 8.2.3, "Insurance", applies to you and your Agencies that conduct business in the same industry as you. Agency means any entity or line of business that uses your Marks or holds itself out to the public as a member of your group of companies. Independent Agency means an entity or line of business that sells your and other's Goods or Services for which it may receive either payment or commission from you or an Agency.

8.2.4 Motor Vehicles

8.2.4.1 Vehicle Rental

a. Merchants must ensure that the Cardmember has executed a standard rental agreement.

b. On the first day of the rental, the vehicle rental Merchant shall obtain Authorisation for the full estimated amount of the Charge. The estimated Charge shall be determined by multiplying the applicable rental rate, tax and/or mileage rates, and any ancillary charges by the rental period reserved by the Cardmember. The Merchant shall not overestimate this amount and under no circumstances shall the estimated Transaction amount include ancillary Charges that represent either an amount for any possible damage to or theft of the vehicle or the insurance deductible amount when the Cardmember waives the insurance coverage at the time of rental.

c. The final submitted Transaction amount must not exceed the Authorisation amount by more than 15%.

d. Merchants may include costs for additional Goods and Services provided to the Cardmember (e.g., child seats) and the exact amount of any other cost that the Cardmember may be liable for and that is within the Cardmember's control to avoid (e.g., a "no show" fee or a charge for failing to return the vehicle with a full fuel tank). The rental agreement must include the Cardmember's consent to include these costs in the Charge submitted for the vehicle rental.

e. The Authorisation will be valid for the life of the rental agreement, provided the final submitted Transaction amount does not exceed more than 15% of the Authorised amount.

f. Refer to Subsection 3.3.2, "Estimated Charge Amount" for more information about processing estimated Charges.

g. Cardmembers may reserve, and Merchants must honour, vehicle rentals via Guaranteed Reservations. Upon providing the appropriate Card credentials, Cardmembers may have the rental Merchant hold a rental reservation for one (1) day's rental or the relevant incremental equivalent (such as hourly) of the rate agreed.

h. In addition to cars and trucks, vehicle rentals include:

i. Aircraft

ii. Bicycles
iii. Boats
iv. Equipment
v. Motor homes
vi. Motorcycles

i. To process Guaranteed Reservations, The Merchant must:
   i. Inform the Cardmember of the rental rate,
   ii. Provide the Cardmember with a reservation confirmation code, and
   iii. Provide the Cardmember the Merchant's cancellation policy including the cancellation deadline to avoid a "no show" charge as well as the "no show" charge amount.

j. If a Cardmember decides to cancel a Guaranteed Reservation Transaction in accordance with the Merchant's agreed-upon cancellation policy, the Merchant must provide the Cardmember a cancellation number and maintain a record of such cancellation.

k. If the rental services are not cancelled in compliance with the Merchant's cancellation policy, the Merchant may submit a Guaranteed Reservation Transaction equivalent to one (1) day's rental charge, or the relevant incremental equivalent (such as hourly) of the rate agreed.

l. To charge a Cardmember's account, the Merchant must either:
   i. Print the words "No Show" on the signature line of the Transaction Receipt, or
   ii. Transmit to American Express the appropriate Additional Amount Type Code "Guaranteed Reservations."

m. Failure to do so may result in an ISO 4513 – Credit Not Processed / Guaranteed Reservations (C18).

n. Refer to the *Technical Specifications* for more information.

o. If a Merchant cannot fulfil a rental reservation on the specified date and time, the Merchant must provide comparable accommodations, and/or Services, when reasonably available, at no additional cost to the Cardmember in accordance with the Merchant's rental agreement and/or Applicable Laws and regulations.

p. Upon rental of the vehicle:
   i. Ensure that the Cardmember has provided a valid driving license;
   ii. Ensure that the vehicle rental is commenced on or subsequent to the beginning date and on or prior to the expiration date shown on the face of the Card;
   iii. Ensure that the Cardmember has and met such other qualifications as the Establishment normally requires in the case of vehicle rentals; and
   iv. Ensure that a Clearing Record is completed.

q. If upon return of a rental vehicle, the car rental Merchant discovers that the vehicle has been damaged and the Cardmember has not purchased the car rental Merchant's collision or loss insurance, the car rental Merchant may submit a Charge, which will be submitted separately from any Charge for a specific amount estimate of the Capital Damages incurred.

r. The Charge which shall be submitted separately from any Charge submitted for the cost of the car rental, may be submitted, provided the following conditions are met:
   i. Prior to billing, the car rental Merchant has obtained the Cardmember's agreement in writing to:
      - A specific estimate of the Capital Damages, including an itemised lost and description of the specific damage occurred,
      - Accept responsibility for the capital damages, and
      - Select American Express as thew payment method for the Capital Damages.
   ii. The car rental Merchant has obtained a separate and additional Authorisation for the specific estimate of the capital damages to which the Cardmember has agreed in condition i above.
   iii. The original Charge for the car rental was made on an American Express Card of the Cardmember who agreed to the details referred to in condition i above. A car rental Merchant must never include the following in an Authorisation Request or in a Charge Submission:

- Losses due to theft of the vehicle, or
- Loss of revenue incurred by the car rental Merchant due to loss of use of the rental vehicle in question.

iv. The Charge submitted for Capital Damages may not exceed the following:

- 15% above the amount established in the specific amounts estimate of the Capital Damages, or
- The replacement cost of the vehicle, in the case of a total loss, due to damages caused by the Cardmember.

s. Merchants must not include an amount in any Charge for any damages, penalties, fines, charges, costs, or fees in addition to the Estimated Authorisation whether or not such amounts are set out in the rental agreement unless such itemised amounts are expressly permitted to be charged under the Agreement and expressly requested by the Cardmember to be charged to the Card. If the Merchant includes such amounts in any Charge without the Cardmember's express request, we will have Chargeback rights for the amount of the Charge in excess of the Estimated Authorisation.

t. In addition to the other Chargeback rights contained in the Agreement, American Express will exercise Chargeback rights if any Charge for Capital Damages is not submitted in accordance with all the procedures contained within these *Merchant Regulations*.

u. The Merchant must comply with requests from the Cardmember or the Cardmember's insurance adjustor to supply documentation related to the Capital Damages incident.

v. Merchants should adhere to the requirements in Subsection 2.5.4, "Merchant-Initiated Transactions" when processing Charges for damages.

w. American Express may monitor the Merchant's compliance with the preceding special Authorisation procedures. If we notify you that an Establishment is not complying with these Authorisation procedures, you must cure such non-compliance within thirty (30) days. If, after thirty (30) days from the date of such notice, the Merchant continues not to comply with these procedures, then American Express will have Chargeback rights for the full amount of any Charges made at that Establishment during such continued non-compliance. For purposes of this provision, "noncompliance" occurs when more than five percent (5%) of either your total or any one Establishment's Authorisations do not comply with the preceding procedures.

x. Notwithstanding the Authorisation procedures set out above, you must still obtain the Cardmember's consent to the full exact amount of the Charge. Any additional amount may only be submitted if you treat it as a separate Charge and obtain the Cardmember's consent to the full exact amount of the Charge.

8.2.4.2 Vehicle Sales

a. We will accept Charges for the deposit payment or the entire purchase price of new and used motor vehicles only if:

i. the amount of the Charge does not exceed the total price of the motor vehicle after deduction of applicable discounts, rebates, cash down payments, and trade-in values; and

ii. you obtain Authorisation for the entire amount of the Charge.

b. 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, we will have Chargeback rights for such Charge.

8.2.5 Oil, Petroleum, and Electric Vehicles

a. In some countries, additional policies and procedures are applicable to Merchants classified in the oil/petroleum and electric vehicle charging industries. For information about CATs, see Subsection 2.3.4, "Customer Activated Terminals".

8.2.5.1 Requirements

a. You must:

i. Obtain unique Merchant Number(s) for your CAT gas pump and electric vehicle charging sales. If you conduct any other business at your Establishment (e.g., convenience store sales, car washing services), you must obtain a unique Merchant Number for those lines of your business.

ii. Submit dealer location data along with each Authorisation request and each Submission file. Dealer location data consists of your business's:

- dealer number (store number)
- name
- street address
- city
- postal code

8.2.5.2 Automated Fuel Pumps

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

b. If you allow customers to initiate Transactions at CATs, you must:

i. Set a Pre-Authorisation request at your CAT gas pumps based on a good faith estimate of the final charge amount.

ii. For higher Charges such as diesel, adjust the pre-Authorisation amount to accommodate the higher Charges.

iii. Set your CAT gas pumps to shut off when they reach the pre-Authorisation amount.

iv. Upon completion of the sale, submit an Authorisation Adjustment Advice for the final sale amount, which must not be greater than the pre-Authorisation amount.

v. Request a separate Authorisation for purchases that exceed the original pre-Authorisation amount.

8.2.5.3 Electric Vehicle Charging

a. If you allow customers to initiate transactions at CATs, use one of these options:

- **Option 1: Pre-Authorisation**
  - **a.** Set a pre-Authorisation request at your electric vehicle charging stations based on a good faith estimate of the maximum charge amount.
  - **b.** Upon completion of the sale, submit an Authorisation Adjustment Advice for the final sale amount, which must not be greater than the pre-Authorisation amount.
  - **c.** Set your charging stations to shut off when they reach the pre-Authorisation amount.
- **Option 2: Estimated with Incremental Authorisation (where available)**
  - **a.** Using Variable Authorisation capabilities, obtain an Estimated Authorisation based on a good faith estimate of the final charge amount.
  - **b.** If the final sale amount is greater than the Estimated Authorisation, obtain an Incremental Authorisation for the additional amount.
  - **c.** If the final sale amount is less than the Estimated Authorisation plus any Incremental amounts, submit a Partial Authorisation Reversal for the excess Authorisation amount.
  - **d.** Refer to Section 3.3, "Variable Authorisation" for additional information and requirements.
  - **e.** Variable Authorisations, including Estimated Authorisations and Incremental Authorisations, may not be available in all areas. Refer to the *Technical Specifications* for details.

8.2.6 Payment Facilitators

a. If your business model requires you to accept the Card on behalf of third parties (Sponsored Merchants), and your Agreement allows it, you are a Payment Facilitator for the purposes of your Agreement with us. We have the right, in our sole discretion, whether or not to approve and/or designate you as a Payment Facilitator on the American Express network. As a Payment Facilitator, you must comply with any additional requirements, policies, or procedures of which we notify you from time to time.

b. At a minimum, you must:

i. submit to American Express the mandatory, conditional, and optional Sponsored Merchant Data elements in the Sponsored Merchant Information Interface as outlined in the *American Express Technical Specifications*.

ii. obtain Authorisation for all Sponsored Merchant charges and submit each Sponsored Merchant charge according to the mandatory data element requirements specified in the *Technical Specifications* or local network specifications.

c. If you are a Payment Facilitator located outside the EEA or UK, you cannot recruit Sponsored Merchant Prospects that fall into and/or engage in a line of business appearing within any of the following:

i. Any of the categories listed in Subsection 8.2.1, "Prohibited or Restricted Industries".

ii. Travel industry, including, but not limited to:

- Airlines and air carriers (MCC 3000-3350, 4511)
- Car rental agencies (MCC 3351-3500, 7512)
- Lodging, including hotels, motels, resorts, including "branded" central reservation services (MCC 3501-3999, 7011)
- Steamships and cruise lines including onboard cruise shops (MCC 4411)
- Timeshares (MCC 7012)
- Travel agencies and tour operators (MCC 4722)

iii. Telecommunications Services, including wireless, cable, satellite, wire line, ISP (MCC 4814, 4816, 4899).

iv. Other Entities acting as Payment Facilitators, including, but not limited to:

- Integrated Software Vendors (ISVs)
- Software as a Service Providers (SaaSs)
- Any other Entities that act as Payment Facilitators to Merchants. Notwithstanding the foregoing, while Payment Facilitators may not sign another Payment Facilitator as a Sponsored Merchant, they may contract with ISVs, SaaSs, and other third parties to offer additional services to Sponsored Merchants, so long as the Payment Facilitator enters into a Sponsored Merchant Agreement directly with each of its Sponsored Merchants and pays Charges to the applicable Sponsored Merchants.

v. Indirect Acceptors with the exception of Marketplaces.

d. If you are a Payment Facilitator located in the EEA or UK, you cannot, without prior written consent, recruit Sponsored Merchant Prospects that fall into and/or engage in a line of business appearing within any of the categories listed in Subsection 8.2.1, "Prohibited or Restricted Industries". Certain categories will require Payment Facilitators and/or their Sponsored Merchants to follow additional policies and procedures.

e. Please contact your American Express representative to understand all your obligations as a Payment Facilitator. Failure to comply with your obligations may result in non-compliance fees as set out in your Agreement or as otherwise disclosed to you.

8.2.7 Transit Contactless Transactions

8.2.7.1 Card Acceptance Requirements for Transit Contactless Transactions

a. When accepting and processing Transit Contactless Transactions you must:

i. Be classified in one of the following MCCs: 4111, 4112, 4131, 4784, 7523 and pass that MCC in the Authorisation and Submission.

ii. Not accept the following Cards:

a. expired Cards

b. Cards within the specified BIN ranges provided by us

c. Cards that are on the Deny List at the time the Cardmember attempts to access the transit system

iii. Flag all requests for Authorisation and Submission with a transit indicator and meet additional transit technical requirements (see Section 1.4, "Compliance with our Specifications").

8.2.7.2 Authorisation and Submission Requirements

a. When accepting a Transit Contactless Transaction, you must obtain an Account Status Check for a nominal amount or any amount up to the Chargeback Protection Threshold (as set forth in Subsection 8.2.7.3, "Transit Thresholds") or an Authorisation. The following sets out how to proceed based on the response you receive to the Account Status Check or Authorisation.

Table 8-5: Contactless Transit Authorisation and Submission Requirements

If	Then
The Account Status Check or Authorisation is approved	Continue to accept taps and submit the Aggregated Transit Charge up to the Chargeback Protection Threshold within the Authorisation Time Period since the most recent Approved Authorisation (as set forth in Subsection 8.2.7.3, "Transit Thresholds"). Authorisations for partial fares cannot be submitted. If the Card is on the Deny List and an Account Status Check or an Authorisation is approved, remove the Card from the Deny List.
The Account Status Check or Authorisation is declined	You must place the Card on the Deny List. If the final fare amount is less than or equal to the Declined Authorisation Protection threshold (as defined in Subsection 8.2.7.3, "Transit Thresholds"), submit the Transaction. If the final fare amount is greater than the Declined Authorisation Protection threshold, you must not submit the Transaction. You may request a new Authorisation as outlined in Subsection 8.2.7.5, "Transit Debt Recovery". **Note:** Authorisations for partial fares cannot be submitted. You must not split a Transaction with the intent of avoiding a single Authorisation for the final fare amount.
The combined taps are within the Chargeback Protection Threshold and Authorisation Time Period	You may submit the Transaction. You may obtain a new Account Status Check or Authorisation for future taps. **Note:** You must submit the Transaction according to the Submission Frequency (as set forth in Subsection 8.2.7.3, "Transit Thresholds").
The combined taps exceed the Chargeback Protection Threshold or the Authorisation Time Period is exceeded	You may submit the Transaction, provided that you obtain Authorisation at the time of submission. You may be subject to the "Invalid Authorisation (ISO 4521) / No Valid Authorisation (A02) or No Valid Authorisation (ISO 4755) / No Cardmember Authorisation (F24)" Chargeback should you submit a Transaction for a value above the Chargeback Protection Threshold.

8.2.7.3 Transit Thresholds

a. The following thresholds will apply and be provided to you in writing:

- **i.** Chargeback Protection Threshold
- **ii.** Authorisation Time Period
- **iii.** Submission Frequency
- **iv.** Declined Authorisation Protection

8.2.7.4 Transit Charge Information

a. You must ensure the Cardmember has access to the following information for a minimum of one hundred and twenty (120) days:

- **i.** Name associated with the Merchant Number

ii. Total Transaction amount
iii. Date of travel
iv. Start time of each individual journey, if available
v. End time of each individual journey, if available
vi. Final Transaction date

8.2.7.5 Transit Debt Recovery

a. If an Authorisation is declined, you may attempt to recover any outstanding debt, providing all the following conditions are met:
   i. The value of the debt is greater than the Declined Authorisation Protection Threshold (as set forth in Subsection 8.2.7.3, "Transit Thresholds").
   ii. You obtain an approved Authorisation for the full value of the debt owed.
   iii. You do not attempt more than six (6) Authorisations after the initial Authorisation was declined.
   iv. No more than thirty (30) days have elapsed since the initial Authorisation was declined.
   v. You should adhere to the requirements in Subsection 2.5.4, "Merchant-Initiated Transactions", when processing Merchant-Initiated Transactions for Debt Recovery.

8.2.7.6 Management of the Deny List

a. You must maintain a Deny List by adding or removing Card Accounts based on any new Authorisation approval or decline. You must not add a Card Account to the Deny List for any reason other than in exceptional circumstances where you reasonably suspect travel irregularities associated with the use of the relevant Card. The Deny List must be updated at least once daily. We recommend that you update the Deny List more frequently when possible.
b. When a Card is tapped, you must immediately check the Deny List and refuse entry to any Cardmember when the Card Account of the Card used appears on the Deny List.
c. You must not submit Transit Contactless Transactions when the Card Account appears on the Deny List at the time of submission attempt. A Card Account must be removed from the Deny List if an Account Status Check or Authorisation request is subsequently approved.
d. We may issue Chargebacks if you fail to comply with these requirements or the provisions of this Section 8.2.7, "Transit Contactless Transactions".

8.2.7.7 Pay-In-Advance Transit Passes

a. You may offer a pay-in-advance fare programme, which allows Cardmembers to use their Card, Contactless Card or Mobile Device to purchase, in advance of travel:
   i. time-based, unlimited travel passes, which allow the Cardmember to use their Contactless Card or Mobile Device to enter and/or use the transit system until the time limit for such pass expires, or
   ii. passes are available for a defined value or defined number of trips, which allow the Cardmember to use their Contactless Card or Mobile Device to enter and/or use the transit system until the balance is used. Balances on these passes are reduced as the Cardmember uses the transit system, either in terms of value or number of trips, depending on the type of pass purchased.
b. If the Cardmember uses a Pay-In-Advance Transit pass, you must:
   i. Limit the system functions to account identification and fare validation only, and
   ii. Not process taps as Transit Contactless Transactions.

8.2.8 Travel Industries

a. Additional terms and procedures are applicable to Merchants classified in the airline, cruise line, lodging, and vehicle rental industries. For the below listed industries, where applicable, follow the requirements for estimated Charge amounts in Subsection 3.3.2, "Estimated Charge Amount", when the final amount of the Charge is not known.
b. Prepaid Cards must not be accepted at check-in for lodging or embarkation of a cruise for onboard purchases, nor for any other Charges that are not "real time" purchases (i.e., for which Authorisation is obtained at the same time as the purchase.

8.2.8.1 Airline Merchants

8.2.8.1.1 Affiliate Carriers

a. The Merchant shall cause the Affiliate Carriers to accept Cards in accordance and in compliance with the Agreement and will be responsible for the Affiliate Carriers compliance thereof.

8.2.8.1.2 Clearing Records

a. The Merchant must follow the requirements for Clearing Records as detailed in Section 2.6, "Charge and Credit Clearing Records" and the Clearing Record must clearly state:

i. Cardmember's name and passenger name (if not the Cardmember);

ii. The ticket number, the origin, and destination of each flight, and the class code or, if not a ticket, a description of the Goods or Services being purchased;

iii. Airline merchant's and, if an Agent is involved, Agent's name and the location where Charge is being made; and

iv. If applicable, the election by Cardmember of Extended Payment.

8.2.8.1.3 Extended Payment

a. Certain Cardmembers who have an Extended Payment arrangement with American Express may request to use it when making a purchase for air transport. Related services may not be purchased with Extended Payment. Merchants will have no liability if, without knowledge, a Cardmember incorrectly identifies as having Extended Payment with American Express. Merchants should not ask a Cardmember if they wish to elect Extended Payment, but if the Cardmember indicates that Cardmember does, you will record the Cardmember's election by an entry on the Clearing Record and on the Transmission, if you submit electronically.

8.2.8.1.4 In-Flight Charges

a. Until American Express offers satellite or other in-flight Authorisation capability, Merchants do not need prior Authorisation for in-flight Charges permitted under the Agreement. However, within 24 hours after termination of a flight on which Charges have been made, Merchants must get Authorisation as described above for each such Charge.

8.2.8.1.5 Private Charter Charges

a. For Charges for private charters (where all or most of the charter is being paid with the Card), Merchants must obtain Authorisation at the time the request to pay with the Card is made and, if any such Authorisation is obtained more than seven (7) days prior to the flight, then Authorisation must be obtained again within seven (7) days prior to the flight. Charges for private charters (i.e., where the Card is being used to pay for all or most of the charter) may not be submitted until the service has been fully completed (e.g., if the Charge covers a round trip, the Charge must be submitted immediately after the completion of the return flight and not before).

8.2.8.1.6 Submitting Transactions

a. Agents in the U.S. will submit electronically through the Airline Reporting Corporation (ARC) or its successor, and Agents outside the U.S. will do the same through the appropriate International Air Transport Association (IATA) or Billing and Settlement Plan (BSP) process. Merchants must submit Transactions to American Express in the country where the Transactions were made, or as agreed between American Express and the Merchant. Transactions from Affiliate Carriers must be submitted to American Express by the Merchant or the Merchant's Agents. Merchants are solely responsible for settlement with each Affiliate Carrier and Agents and you are jointly and severally liable for their obligations under the Agreement.

b. Where American Express does not offer electronic submission, or is not available due to technical difficulties, or where American Express agrees otherwise in advance in writing, Merchants may submit Transactions to American Express using magnetic tape or on paper. Magnetic tapes must conform to American Express' requirements. Paper submissions must be batched as described in this section and sent to such address as American Express notifies you, along with a summary form as provided by American Express, as often as possible, but at least weekly. In case of sales by Agents, paper submissions must be sent to such address as airline merchant instructs them or to the appropriate central processing facility (ARC in the U.S. or an IATA or BSP outside the U.S.). Charges submitted on paper must be sorted, batched, summarised, and submitted separately to American Express as follows:

i. By currency;
ii. Charges incurred in any other currency (American Express is not obliged to accept such Charges but to the extent American Express does it is fully at American Express' discretion and will not create any obligation to accept such Charges in the future);
iii. All Charges on Extended Payment;
iv. All Charges for related services as agreed upon by American Express;
v. Each batch may contain no more than 150 Clearing Records; and
vi. Each batch must be accompanied by a summary form on which must be prominently indicated the gross amount and number of Charges, the currency, airline merchant's name, and airline merchant's assigned Establishment Number.

8.2.8.2 Cruise Lines

a. Cruise line Merchants may obtain an Authorisation at embarkation based on the estimated charge that will be incurred during the Cardmember's intended length of stay. The Authorisation should include:
   i. The room rate, including applicable tax and/or service charge rates
   ii. The Merchant's procedure for estimating additional ancillary Charges
b. The final submitted Transaction amount must not exceed the Authorisation amount by more than 15%.

8.2.8.3 Lodging

a. Lodging Merchant must obtain an Authorisation at check-in based on the estimated charge that will be incurred during the Authorisation Validity Period. The Authorisation should include:
   i. The Cardmember's intended length of stay.
   ii. The room rate, including tax and/or service charge rates.
   iii. The Merchant's procedure for estimating additional ancillary Charges.
b. The final submitted Transaction amount must not exceed the Authorisation amount by more than 15%.

8.2.8.3.1 Advance Payments

a. Advance Payments will hold a lodging reservation for the intended length of stay. Merchants may not present an Advance Payment Transaction for an amount that exceeds the cost of a fourteen (14) night stay plus applicable taxes.
b. When taking an Advance Payment from a Cardmember, the Merchant must inform the Cardmember of the Advance Payment requirements and the cancellation policy for such reservations. Refer to Subsection 2.5.1, "Advance Payments" for more information. The Merchant is required to provide the Cardmember with written confirmation of the following:
   i. Arrival and departure dates
   ii. Amount of the Advance Payment
   iii. Confirmation number
   iv. Merchant's cancellation policy
c. The Merchant must complete a Clearing Record with the following information for each Advance Payment:
   i. The words "Advance Payment (or Advance Deposit)" written on the signature line of the Transaction Receipt or transmit the appropriate Advance Payment description with the Charge data
   ii. The scheduled arrival date
d. Upon cancellation of the reservation, the Merchant must send written cancellation notice including the cancellation number to the Cardmember within three (3) Business Days. If a refund is due, the Merchant must submit a Credit Clearing Record with the words "Advance Deposit Cancellation" on the signature line or transmit the appropriate Advance Deposit indicator on the Credit Transaction.
e. If the arrival date of an Advance Deposit is changed, the Merchant is required to send the Cardmember a written confirmation of the change within three (3) Business Days.
f. If the Merchant is unable to honour the reserved accommodations and the reservation was not cancelled by the Cardmember, the Merchant must:

i. Submit a Credit Clearing Record for the Advance Payment made by the Cardmember.

ii. Pay for accommodations at a comparable location nearby until the duration of the original reservation expires (up to fourteen (14) nights), or until accommodation become available at the original location, whichever occurs first.

iii. Pay for transportation to the alternate establishment and for a return to the original location once per day until the original accommodations are available.

iv. Provide up to two (2) three (3)-minute telephone calls for the Cardmember's alternate accommodations.

8.2.8.3.2 Guaranteed Reservations

a. Guaranteed Reservations allow Cardmembers to guarantee their reservation for one (1) night's stay at a lodging, trailer park, or campground Merchant. Merchants should adhere to the requirements in Subsection 2.5.4, "Merchant-Initiated Transactions" when processing Reservation Guaranteed Reservations Transactions.

b. A Cardmember may contact a lodging Merchant and provide their Card Account number and Expiration Date to hold a reservation for one (1) night's stay. The Merchant must inform the Cardmember of the rate for the room accommodation for one (1) night. At the time of the reservation, the Merchant must provide the Cardmember with a confirmation code and cancellation policy. The Merchant must reserve accommodations until the published check-out time the following day.

c. Upon a Cardmember cancellation, the Merchant must provide the Cardmember with a cancellation number and maintain a record of such cancellation number.

d. If the Guaranteed Reservation is not claimed or cancelled in accordance with the Merchant's cancellation policy, the Merchant may charge the Cardmember's Account for a "no show" Charge equal to one (1) night's lodging. To charge a Cardmember's Account, either the words "No Show" must appear on the signature line of the Clearing Record, or the Merchant must transmit the appropriate indicator in the Charge Transaction data. Failure to do so may subject the Merchant to an ISO 4513 – Credit Not Presented Chargeback. See Table 5-9: Credit not processed (ISO 4513) / Guaranteed Reservations (C18).

e. If American Express receives disproportionate numbers of Disputed "no show" Charges, the Merchant must work with American Express to reduce the number of disputes. If such efforts fail to reduce the number of disputes, American Express may place the Merchant in any of American Express' Chargeback programmes. See Section 5.11, "Fraud Full Recourse Programme".

f. The Merchant must arrange and pay for alternate accommodations if the reserved accommodations are not available on the specified date and time and the reservation was not cancelled by the Cardmember. The Merchant will provide the Cardmember with the following services at no additional charge:

i. Comparable accommodations for one (1) night at another establishment;

ii. If requested, a three (3) minute phone call;

iii. Transportation to the alternate establishment's location; and

iv. Use good faith efforts to forward all communications to the Cardmember at the alternate Establishment's location.

8.2.8.3.3 Emergency Check-In

a. If a Cardmember whose Card is lost or stolen requests check-in, you must call the Authorisation telephone number, ask for an American Express representative, request Authorisation for an "Emergency Check-In", and follow the representative's instructions.

8.2.9 Travel Services

a. If you are in the business of supplying land, sea, or air transportation, accommodation, sightseeing tours or other arrangements, or other travel services and you use Agents to sell your services, your Agents may accept the Card as payment for your services and you may submit the resulting Charges to us for payment as if each Agent were one of your Establishments. You will cause your Agents to comply with the Agreement, and you will be responsible for their compliance. Because we will pay you and not your Agents for any Charges submitted to us in this manner, you will be responsible for paying your Agents and otherwise settling with them for those Charges.

b. American Express will assign you unique Establishment Numbers which you and your Agents must use as instructed by American Express for submissions of Transactions. You are solely responsible for financial arrangements and for settlement with Agents and you are jointly and severally liable for their obligations under the Agreement.

8.3 Japan Credit Bureau

a. American Express has an established relationship with Japan Credit Bureau (JCB), a Card Issuer based in Japan, whereby we act as JCB's merchant acquirer in Canada, Australia, and New Zealand. Merchants in Canada, Australia, and New Zealand can accept and process JCB cards with 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 using the same terminal on which they accept the American Express Card.

b. 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.

c. Complimentary American Express and JCB decals and signage are available for Merchants in Canada, Australia, and New Zealand. Contact your American Express representative for more information.

8.4 Merchant Fees

8.4.1 Introduction

a. You must pay us the Discount and you may be subject to various other fees and assessments. Some fees or assessments are for special products or services, while others may be applied because of your non-compliance with our policies and procedures. Many non-compliance fees and assessments can be avoided by correcting the actions that are causing you not to be in compliance.

8.4.2 Card Acceptance Discount Fees

Table 8-6: Card Acceptance Discount Fees

Fee	Description	Amount
Discount Rate	A Discount is one of the amounts we charge you for accepting the Card. To determine the Discount that you pay, contact your American Express representative.	Varies

8.4.3 Payment Facilitators and Indirect Acceptor Fees

a. The Agreement provides for various fees and assessments, as described in the following table.

Table 8-7: Payment Facilitator and Indirect Acceptor Fees

Fee	Description	Amount
Payment Facilitator or Indirect Acceptor general non-compliance fee	A fee applied in the event Payment Facilitator or Indirect Acceptor fails to comply with the policy and requirements documented in Subsection 8.2.6, "Payment Facilitators" or Chapter 6, "Indirect Acceptors". These fees may be assessed where a non-compliance fee has not been specified for a specific policy violation or when non-compliance fees have been assessed, but the Payment Facilitator or Indirect Acceptor has not taken action to correct the policy violation.	• Up to USD $10,000 for second violation of the same regulation within a 12-month period after notification of the first violation. • Up to USD $20,000 for third and subsequent violations of the same regulation within a 12-month period after notification of the first violation.
Sponsored Merchant or End Beneficiary reporting non-Compliance fee	A fee applied in the event a Payment Facilitator fails to provide the required Sponsored Merchant Data elements. This fee shall apply to Indirect Acceptors that may be required to submit End Beneficiary data.	• Up to USD $10,000 for second violation of the same regulation within a 12-month period after notification of the first violation. • Up to USD $20,000 for third and subsequent violations of the same regulation within a 12-month period after notification of the first violation.

AMERICAN EXPRESS

Glossary

In these *Merchant Regulations*, and throughout the Agreement, the following defined terms apply. Other defined terms appear in *italics* in the body of the Agreement and will apply for the whole of this document, not just the provision in which they appear.

Account Status Check

A type of Authorisation request that is used to ask an Issuer to indicate if the Card Account represented by the Card Account on the message is valid. The Account Status Check is used, for example, by transit authorities to check the status of a Card Account associated with a Transit Contactless Transaction at transit operator's terminal.

Advance Payment

A Charge for which full payment is made in advance of your providing the Goods and/or rendering the Services to the Cardmember.

Affiliate

Any legal entity that controls, is controlled by, or is under common control with the relevant party, including its subsidiaries.

Affiliate Carriers

Licensed passenger air transport carriers with which an airline merchant has shared designator code agreements and written franchise or similar agreements whereby such carriers (a) operate under a trade name and logo owned by the airline merchant; (b) hold themselves out to the public as being affiliated with the airline merchant; (c) utilise ticket stock bearing the airline merchant's name and identifying number; and (d) are required to comply with operational and customer service standards prescribed by the airline merchant. The Affiliate Carriers of an airline Merchant will be referred to collectively as a Carrier Affiliate Group and it is understood and agreed that the Affiliate Carriers are regional or small carriers.

Agent

A ticket, travel or generated sales agent or other agent, not an employee of Merchant, who sells Merchant's Goods and/or Services.

Aggregated Transaction

The combining of two (2) or more individual purchases, refunds, or both, incurred on the same Card Account Number and Merchant Account Number into one (1), larger Transaction. American Express also uses the following term in the Agreement to refer to Aggregated Transaction: Aggregated Charge.

Aggregated Transit Charge

An Aggregated Charge that combines multiple small Transit Contactless Transactions incurred on a Card into a single, larger Charge before submitting the Charge for payment.

Agreement

The agreement pursuant to which you accept American Express Cards and these *Merchant Regulations*, collectively.

Alternative Currency

A currency other than Local Currency, as such Currency or Currencies are approved by American Express.

American Express Card or Cards

Any card, electronic account access device, other virtual, electronic or physical payment instrument, or service issued or provided by American Express Company, any of its Affiliates or any authorised licensees thereof and bearing any Mark(s) of American Express Company or any of its Affiliates. Card also includes any card or other account access device issued by a Third Party Issuer. The use of the terms "charge" and "credit" in relation to Cards are interchangeable in the Agreement.

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.

American Express SafeKey Programme (AESK Programme)

An industry standard authentication tool that is designed to provide greater security for online Transactions.

Applicable Law

(i) Any law, statute, regulation, ordinance, or subordinate legislation in force from time to time to which you or we or an Affiliate of either 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 Charge

A Charge which is made via your application designed specifically for navigation on mobile or tablet devices.

Approval/Approved

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

Authorisation

The process for obtaining approval for a Charge, as described in the Agreement, in the form of an approval code number given by us or a third party designated and approved by us from time to time.

Authorisation Adjustment

The Authorisation Adjustment message allows Acquirers and their Merchants to adjust the Transaction amount when the final Transaction amount is lower than the amount previously authorised. This allows the Issuer to release any hold on available funds on a Cardmember's Card Account for excess amounts authorised without waiting to receive the Presentment message containing the final Transaction amount.

Authorisation Reversal

Authorisation message used by a Merchant to cancel or reduce the amount of a previously approved Authorisation once the final Charge amount is known.

Authorisation Time Period

The number of days an approved Authorisation is valid for a transit purchase, before another Account Status Check or Authorisation is required.

Bank Account

An account that you or your Affiliate holds at a bank or other financial institution.

Bank Identification Number (BIN)

A 6-digit number used on Cards to identify the Issuer of the Card and which serves as the first six digits of the Card Account number or Token.

Bill Payment Provider

An Indirect Acceptor that is engaged by Cardmembers to pay a bill on their behalf. Bill Pay Providers (BPPs) charge the Cardmembers' Card Account and pay eligible End Beneficiaries identified on the bill.

Business Day

A day on which all parties to a Transaction and/or an event are open to do business.

Buyer Initiated Payment (BIP) Transactions

A payment Transaction enabled via a payment instruction file processed through BIP.

Capital Damages

Damages done to a vehicle while rented to a Cardmember.

Card Account

An account established by an Issuer with a Person upon the issuance of one (1) or more Cards.

Card Identification Number (CID)

Any of several values printed on the face of the Card.

Card Not Present Charge

A Charge for which the Card is not presented to you at the point of purchase (e.g., Charges by mail, telephone, over the internet or digitally, including a Digital Wallet Application-initiated Transaction but excluding Digital Wallet Contactless-initiated Transactions).

Card Not Present Chargeback

A Chargeback on a Card Not Present Charge that was disputed as fraudulent.

Card Present Charge

A Charge for which the Card is presented at the point of purchase, including In-Person Charges and Charges made at CATs.

Cardholder Data

Has the meaning given in the then current Glossary of Terms for the PCI DSS.

Cardholder Verification Method (CVM)

The method by which Cardmember verification is performed to ensure that the person presenting the Card or Mobile Device is the person to whom the application was issued.

Cardmember

The carrier or holder of a Card (whose name may or may not be embossed or otherwise printed on the face of the Card) provided that, where a name is embossed on a Card, the person whose name appears on the Card is the Cardmember.

Cardmember-Initiated Transaction (CIT)

A Transaction which involves direct participation of the Cardmember.

Cardmember Information

Any information about Cardmembers and Card Transactions, including the names, addresses, account numbers, and card identification numbers (CIDs).

Charge

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

Charge Data / Credit Data

One or more of the data elements listed in Section 2.6, "Charge and Credit Clearing Records".

Chargeback

When used as a verb, means our right to: (i) our reimbursement from you for the amount of a Charge, or other amount, which we have paid to you whether by deducting, withholding, recouping from, or otherwise offsetting such amount against our payments hereunder (or debiting your Bank Account), or by notifying you or an Establishment of the obligation to pay us, which must be done promptly and fully; or (ii) our reversal of a Charge for which we have not paid you. When used as a noun, means the amount of a Charge subject to reimbursement from you or reversal. Sometimes called "full recourse" in our materials.

Chargeback Protection Threshold

The maximum value of one or more aggregated transit Transactions that can be settled against an approved Authorisation and protected from Chargebacks.

Chip

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

Chip and PIN Country

A Country where the POS system must be capable of processing Chip and PIN Transactions. See Chapter 8, "Regulations for Specific Industries".

Chip and PIN Transaction

A Chip Card Charge authenticated by a PIN.

Chip Card

A Card that contains an integrated Chip on which data is stored (including Cardmember Information), which an enabled POS system can read in order to facilitate the processing of the Charge. Sometimes called a "smart card", an "EMV Card", or an "ICC" or "integrated circuit card" in our materials.

Chip Card Data

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

Chip Only Country

A country where the POS system must be capable of processing Chip Card Transactions that are not required to be authenticated by a PIN.

Clearing Record

Previously referred as Charge Record. The record submitted for Clearing for a Cardmember's Charge or Credit Transaction containing the details of any Transaction carried out at an ATM or at the POS. American Express also uses the following terms in these *Merchant Regulations* and/or the Agreement to refer to a Clearing Record: Charge Records, Original Clearing Record, Substitute Clearing Record, Transaction Log, and Copy.

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.

Consumer Device Cardmember Verification Method (CDCVM)

An American Express approved and recognised Cardmember verification method whereby the Cardmember's credentials are verified on a Mobile Device and provided to an American Express issuer in the Charge Authorisation.

Consumer-Presented Quick Response (CPQR)

A Transaction where a Cardmember uses the Issuer application on a Mobile Device to generate a QR Code that is scanned at a POS device.

Contactless

A Transaction environment in which a Card or Mobile Device is enabled with a radio frequency component to communicate with a radio frequency-enabled POS device to initiate a Transaction.

Contactless Technology

Any technology which allows the transfer of Charge Data from a Chip Card or Mobile Device to a POS system on a Contactless basis in respect of an In-Person Charge.

Covered Parties

Any or all of your employees, agents, representatives, subcontractors, Processors, Service Providers, providers of your point-of-sale equipment (POS) or POS 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. Sometimes called "Vendors" in our materials.

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 you refund to Cardmembers for purchases or payments made using a Card.

Credit Record

A record of a Credit that contains Charge Data and complies with our 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 denominated in the digital Token.

Customer Activated Terminal (CAT)

An unattended POS system (e.g., a 'pay at pump' fuel dispenser, electric vehicle charging station, or a vending machine). Sometimes called "Self-Service Terminals" or "unattended terminals" in our materials.

Data Security Operating Policy (DSOP)

The American Express data security policy, as described in the Introduction to DSOP and Standards for Protection, of the *International Merchant Regulations*.

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.

Declined Authorisation Protection Threshold

The maximum amount that can be settled following a declined Authorisation for a Transit Contactless Transaction.

Delayed Delivery Charge

A single purchase for which you must create and submit two separate Clearing Records. The first Clearing Record is for the deposit or down payment, and the second Clearing Record is for the balance of the purchase.

Deny List

A list of Card Accounts that have received a declined Account Status Check or Authorisation without a subsequent approved one that removes it from the list.

Digital Delivery Transaction

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). Sometimes called "Internet Electronic Delivery Transaction" in our materials.

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 Order

Charge Data that is taken via a website payment page, over the internet, email, intranet, extranet, EDI, or other digital network in payment for Goods or Services. This includes Internet Charges and Application-initiated Charges. Sometimes called "Internet Order" in our materials.

Digital Wallet Application-initiated Transaction

A Transaction initiated by a digital wallet utilising a browser or merchant application within the Mobile Device, and not via Contactless Technology.

Digital Wallet Contactless-initiated Transaction

A Contactless Transaction initiated by a digital wallet within a Mobile Device via the Contactless interface at an Expresspay-enabled point of sale device.

Digital Wallet Operator

A Digital Wallet Operator (DWO) is an Indirect Acceptor that operates a payment application allowing Cardmembers to make purchases or transfer funds through one or more of the transaction types set forth in Section 6.2, "Indirect Acceptor Models".

Discount

An amount that we charge for accepting the Card as set out in your Application or elsewhere in the Agreement, the amount of which is: (i) a percentage of the face amount of the Charge (Discount Rate); (ii) a flat per-transaction fee; (iii) an annual fee; or (iv) any combination of (i) to (iii). Sometimes called "Discount Rate", "Merchant Fee", "Merchant Service Fee", or "Service Fee" in our materials.

Disputed Charge

Any Charge (or part thereof) 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, the Internet Transactions or Digital Wallet Application-initiated Transactions.

Electronic Commerce Indicator (ECI)

A data element related to a SafeKey Charge indicating the outcome of the SafeKey Authentication.

EMV Specifications

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

End Beneficiary

A third-party entity that receives payments from an Indirect Acceptor. The End Beneficiary does not receive Card information from the Indirect Acceptor. An End Beneficiary may also separately be a Merchant that directly accepts the Card.

Establishment

Each of your and your Affiliates' locations, shops, outlets, websites, digital networks, and all other points of sale using any methods for selling Goods and Services, including methods that you adopt in the future. Sometimes also referred to as a "Merchant", "SE" or "Service Establishment" in our materials.

Establishment Number

The unique number we assign to each Establishment. If you have more than one Establishment, we may assign to each a separate Establishment Number. Sometimes called "Merchant Number" or "SE Number" in our materials.

Estimated Authorisation

An Authorisation for an estimated amount that differs when the final Charge amount is not known at the time of the Authorisation from the final submission amount.

Expiration Date

The year and month in which a Card expires.

Expresspay

A programme within American Express for facilitating Contactless Transactions between a Chip Card or Mobile Device containing an Expresspay Application and an Expresspay-enabled POS device.

Floor Limit

A Charge amount above which you must obtain an Authorisation.

Fraudulent, Fictitious, and/or Collusive Merchant

A Merchant that provides fraudulent information during the set-up process, or processes transactions with the intent of defrauding American Express, an Acquirer, a Cardmember, or an Issuer; or a Merchant whose Charge volume is comprised of Confirmed Fraud, including, but not limited to Merchants involved in:

- Billing Cardmembers for unauthorised Charges (i.e., Charges the Cardmember did not authorise);
- Imprinting, swiping, or keying additional Transactions for unauthorised Charges before returning the Card to the Cardmember, or using stolen Card Account information while the Cardmember retains possession of their Card; and
- Keying in an unauthorised Transaction after being given a stolen Card Account number by a collusive Participant.

Fraud Full Recourse Programme

A programme that allows us to exercise our Chargeback rights without first sending an inquiry any time a Cardmember disputes a Charge for any reason based on actual or alleged fraud without the right to request a reversal of our decision to exercise our Chargeback rights.

Fraud to Sales Ratio

Calculation of total fraud as compared to your total charge volume for a specified period of time, as determined by American Express according to the parameters contained in the relevant *SafeKey Implementation Guide*.

Goods

Tangible commodities manufactured or produced for sale (e.g., wares, merchandise).

Guaranteed Reservations

Previously referred to as No Show Reservation Programme or Assured Reservations. Allows Cardmembers to guarantee their reservation at participating properties or rental agencies through the use of their Card, and also guarantees payment to hotel Merchants of one (1) night's rate should the Cardmember either not utilise the reservation or cancel within the proper timeframe.

Imprint

Cardmember data transferred from a Card to a Transaction receipt to complete a Transaction. An Imprint may be an electronic Imprint or a manual Imprint. A manual Imprint is the imprint of the embossed data taken with a manual imprinter. A pencil rubbing or photocopy of the Card is not considered proof of a valid Imprint.

In-Person Charge

A Charge for which the physical Card or, in the case of Digital Wallet Contactless-initiated Transactions, Mobile Device is presented at the point of sale, including Charges made at CATs. Sometimes called a "Card Present Charge" in our materials.

Incremental Authorisation

Authorisation message used by a Merchant to request an increase to the amount of a previously approved Estimated Authorisation request.

Indirect Acceptor

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, check/cheque, or wire.

Instalment Payment Transaction
A Transaction that represents a single instalment payment in a series of instalments over a fixed period (sometimes called "Buy Now Pay Later" in our materials).

Internet Charge
A charge which is made through your website or the relevant website of your Establishments over the Internet via a web browser. This excludes Application-initiated Charges.

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.

Local Currency
The currency of the Country in which a Charge is incurred, or Credit is made.

Marketplace
A Merchant that offers Cardmembers the ability to purchase from multiple End Beneficiaries on their prominently branded platform (i.e., website or mobile application) and pay for such purchases on the same platform.

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

Maximum Amount for a Contactless Transaction with No CVM
The maximum amount of the Charge that may be processed using Contactless Technology.

Merchant Account
An account established with us upon entering into the Agreement.

Merchant Category Code (MCC)
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 Credentials-on-File.

Merchant-Presented Quick Response (MPQR) Transaction
A Transaction initiated by a Cardmember using the Issuer application on a Mobile Device to capture a Merchant-Presented QR Code.

Mobile Device
An electronic device recognised by American Express that is enabled to initiate a Digital Wallet Payment. This includes, but is not limited to, mobile telephones, tablet computers, and wearable electronic devices.

Mobile Point of Sale (MPOS)
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.

Multicurrency (MCCY) Establishment
An Establishment processing on the MCCY platform under the Agreement.

Network – see American Express Network or Network

No CVM Programme
A programme that allows an Establishment to not request a CVM from Cardmembers.

Non-Chip Card
A card that does not have an integrated microchip embedded on containing Cardmember and account information.

Non-Chip Country
A country where a Chip or Chip and PIN Transaction is not required.

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 Agreement
Any agreement, other than the Agreement, between (i) you or any of your Affiliates and (ii) us or any of our Affiliates.

Other Payment Products
Any other charge, credit, debit, deferred debit, stored value, smart cards, other payment cards, other foreign currency accounts, account access devices, or any other payment instruments, services or products other than the Card.

Payment Account Reference
Non-financial reference generated by American Express that is associated with a Primary Account Number (PAN). PAR can be utilised by Acquirers and their Merchants to link the PAN and associated Tokens.

Payment Application
Has the meaning given to it in the then current Glossary of Terms for PCI DSS, which is available at www.pcisecuritystandards.org.

Payment Facilitator
An entity whose business model provides that it accepts the Card on behalf of third parties (Sponsored Merchants). Formerly referred to as "Payment Aggregators", "Payment Service Provider" or "PSP" in our materials.

Payment Services
The provision of payment services in connection with Transactions between Cardmembers and Sponsored Merchants whereby you, the Entity providing such services (and not the Sponsored Merchant), are the Merchant of record, submit Transactions under your Merchant Number and receive payment from us for Charges (among other things).

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 PIN Security Requirements

The Payment Card Industry PIN Security Requirements, which is available at www.pcisecuritystandards.org.

Peer to Peer (P2P) Transaction

A Transaction that transfers funds to and from its registered users of a payment application.

Personal Information

Information about an individual that is collected or held by you in the course of performing the Agreement and has the meaning given to it under the Privacy Laws. Personal Information includes but is not limited to information you receive or access about American Express Cardmembers or information we receive or access about you (if you are a person) and any individual employed by you whose details are provided to us as part of the Application or in the course of your acceptance of the Card.

PIN

Personal Identification Number.

PIN Entry Device

Has the meaning given to it in the then current Glossary of Terms for the Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI), 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, Mobile Point of Sale (MPOS), or payment engine or process, used by a Merchant, to obtain authorisations or to collect Transaction data, or both.

Pre-Authorisation

An Authorisation obtained at the beginning of a Transaction for a good faith estimate of the maximum Transaction amount, when an Incremental Authorisation will not be subsequently utilised.

Prepaid Card

Any Card marked or denoted as "prepaid" or bearing such other identifier as we may notify you from time to time.

Primary Account Number (PAN)

A series of digits used to identify a customer relationship. The assigned number identifies both the Card issuer and Cardmember.

Privacy Laws

The Act on the protection of Personal Information and any legal or regulatory requirement in Japan or elsewhere which relates to privacy or the protection of Personal Information and which American Express or you must observe.

Processor or Processing Agent

A third party intermediary retained by you that we have approved for obtaining Authorisations from and submitting Charges and Credits to us.

Quick Response (QR) Code

A two-dimensional static or dynamic machine-readable barcode containing data that can be extracted and used for a specific purpose, such as enabling a digital payment.

Record Retention Period

The amount of time you are required to retain the original or electronically stored Clearing Record or Credit Record, and all documents and data evidencing a Transaction, as notified from time to time.

Recurring Billing Charges

An option offered to Cardmembers to make recurring Charges automatically for a series of separate purchases or payments.

Response Timeframe

The amount of time you are required to provide a response containing the information we require after we contact you, as notified from time to time.

Risk-Mitigating Technology

Technology solutions that improve the security of American Express Cardholder Data and Sensitive Authentication Data, as determined by American Express. To qualify as a Risk Mitigating Technology, you must demonstrate effective utilisation of the technology in accordance with its design and intended purpose. Examples include: EMV, Point-to-Point Encryption, and tokenisation.

SafeKey Attempted

The Merchant requested authentication of the Cardmember in accordance with the AESK Programme and received proof of attempt, i.e., ECI 6, from either the Issuer or American Express Network. For the purposes of this definition, a response indicating "unable to authenticate", i.e., ECI 7, is not considered proof of attempt.

SafeKey Authentication

The Merchant requested authentication of the Cardmember in accordance with the AESK Programme and received proof of authentication, i.e., ECI 5, from either the Issuer or American Express Network.

SafeKey Charge

A Charge that has been authenticated via the SafeKey Programme.

Selected Currency

The currency selected by a Cardmember immediately upon the first point of interaction between the Merchant and the Cardmember.

Service Providers

Authorised Processors, third party processors, gateway providers, integrators of POS systems, and any other providers to Merchants of POS systems, or other payment processing solutions or services.

Services

Useful labour that does not provide a tangible commodity and which satisfies some customer demand (e.g., telephone service, airline tickets/travel, meals, professional services).

Split Shipment

A Split Shipment Transaction occurs when a Cardmember makes a single purchase of multiple Goods and the Goods are delivered to the Cardmember in multiple shipments.

Sponsored Merchant

Any third-party Entity (or seller of Goods) appointed by you and who has executed a Sponsored Merchant Agreement.

Sponsored Merchant Data

The mandatory, conditional, and optional requirements including, but not limited to names, postal and email addresses, tax ID numbers, names and social security numbers of the authorised signer of Sponsored Merchants, and similar identifying information about Sponsored Merchants, as set forth in the *American Express Technical Specifications*. For clarification, Sponsored Merchant Data does not include Transaction Data.

Sponsored Merchant Information Interface

Any format (including, but not limited to data files transmitted by secure file transfer protocol (SFTP), application programming interfaces (APIs), or through other methods) containing the Sponsored Merchant Data requirements set forth in the *American Express Technical Specifications*. The *Global Sponsored Merchant File* and Sponsored Merchant Acquisition API are examples of Sponsored Merchant Information Interface formats.

Sponsored Merchant Prospect

A seller of Goods and Services that wishes to accept the Card at the point-of-sale via a third party authorised to accept the Card on its behalf.

Staged Back-to-Back Transaction

A Transaction (i.e., website or mobile application) that allows Cardmembers to use a Card to fund a payment application for a specific purchase in real time to an End Beneficiary.

Stored Value Transaction

A Transaction that loads funds into a payment application for subsequent payments. This includes purchases of Goods and Services at single or multiple End Beneficiaries. Sometimes called "Top-Up Wallet" in our materials.

Strong Customer Authentication (SCA)

Authentication based on the use of two or more elements that are independent, in that the breach of one element does not compromise the reliability of any other element, with the elements falling into two or more of the following categories: (i) something known only by the Cardmember, (ii) something held only by the Cardmember, and (iii) something inherent to the Cardmember.

Submission

The collection of Transaction Data that you send to us.

Submission Frequency

The maximum number of days that transit Transactions can be aggregated before Submission is required.

Substitute Transaction Receipt

A document created from original Transaction data.

Technical Specifications

The set of mandatory, conditional, and optional requirements, including but not limited to guides, specifications, interfaces, bulletins, mandates, and notifications, which we may update form time to time, related to (i) connectivity to the American Express network and (ii) electronic Transaction processing, including Authorisation and submission of Transactions. These are either available at www.americanexpress.com/merchantspecs or upon request from your American Express representative. Sometimes called "American Express Technical Specifications" or "Specifications".

Third Party Issuer

Any other third party card issuer whose card you agree to accept under the Agreement.

Token

A surrogate value that replaces the PAN.

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.

Transaction Receipt

Previously referred to as Charge. An electronic or paper record of a Transaction generated by the Merchant and provided to a Cardmember.

Transit Access Terminal (TAT)

A Contactless-enabled POS Device that, when "tapped" by an authenticated Contactless Card, allows the Cardmember access to the transit system.

Transit Contactless Transaction

A Contactless (see also "Expresspay") Transaction for entry into and/or use of a transit system.

Transmission Data

The same as Cardholder 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.

Virtual Currency

A financial currency unit not issued by a national monetary union. Virtual Currencies may be accepted as a medium of exchange or monetary value transfer between two (2) or more individuals or Entities but may not have all the attributes of a real currency.

Voice Authorisation

The Authorisation of a Charge obtained by calling the American Express Authorisation Department.

we, our, and us

The American Express corporate entity applicable for your country as defined in the Agreement.

you and your

The company, partnership, sole trader or other legal entity accepting Cards under the Agreement and its Affiliates conducting business in the same industry and their respective Establishments.

AMERICAN EXPRESS

Data Security Operating Policy

AMERICAN EXPRESS

DSOP Summary of Changes

Icons

Important updates are listed in the Summary of Changes Table and also indicated in the *DSOP* with a change bar. A change bar is a vertical line, usually in the left margin, that identifies added or revised text. Only substantial changes in the *DSOP* with potential impacts to a Merchant's operational procedures are indicated with a change bar as shown in the left margin.

Removed text is highlighted with a trash can icon placed in the margin next to any significant deletion of text, including sections, tables, paragraphs, notes, and bullet points. Removed text is referenced in this Summary of Changes using the section numbering from the previous publication to avoid confusion.

Blue lines bordering paragraphs indicate region-specific information.

Summary of Changes Table

Important updates are listed in the following table and are also indicated in the *DSOP* with a change bar.

Section/Subsection	Description of Change
There are no changes for this release.	

Section 1 Introduction to DSOP and Standards for Protection

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, Service Providers, and card 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 our Merchants and Service Providers (collectively, you) share our concern and requires, as part of your responsibilities, that **you** comply with the data security provisions in your agreement to accept (in the case of Merchants) or process (in the case of Service Providers) the American Express® Card (each, respectively, the **Agreement**) and this Data Security Operating Policy (DSOP), which we may amend from time to time. 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 those) are stored, processed, or transmitted.

Capitalised terms used but not defined herein have the meanings ascribed to them in the glossary at the end of this policy.

The Data Security Operating Policy (DSOP) is a set of comprehensive policy requirements designed to protect Account Data whenever such data is stored, processed, or transmitted.

American Express requires all Merchants and Service Providers to be Payment Card Industry Data Security Standard (PCI DSS) compliant. As part of that requirement, 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 Security Standards Council (PCI-SSC) Requirements applicable to your processing, storing, or transmitting of Encryption Keys, Cardholder Data, or Sensitive Authentication Data, no later than the effective date for implementing that version of the applicable requirement.
- Ensure PCI-approved products are used when deploying or replacing technology to store, process, or transmit data.

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 American Express for ensuring your Covered Parties' compliance with these data security provisions (other than for demonstrating your Covered Parties' compliance with this policy under Section 2, "PCI DSS Compliance Program (Important Periodic Validation of your Systems)", except as otherwise provided in that section). Details regarding the PCI standards and how to comply with their requirements can be found at www.pcisecuritystandards.org.

Section 2 PCI DSS Compliance Program (Important Periodic Validation of your Systems)

You must take the following actions to validate under PCI DSS annually and every 90 days as described below, the status of your and your Franchisees' equipment, systems, and/or networks (and their components) on which Cardholder Data or Sensitive Authentication Data 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/Service Provider Level and Validation Documentation Requirements.
- Action 3: Complete the Validation Documentation that you must send to American Express.
- Action 4: Send the Validation Documentation to American Express within the prescribed timelines.

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

Level 1 Merchants, Level 2 Merchants, and all Service Providers, as described below, must participate in the Programme under this policy. American Express may designate, at our sole discretion, specific Level 3 and Level 4 Merchants to participate in the Programme under this policy.

Merchant and Service Providers required to participate in the Programme must enrol in the Portal provided by the Programme Administrator selected by American Express within the prescribed timelines.

- You must accept all reasonable terms and conditions associated with the use of the Portal.
- You must assign and provide accurate information for at least one data security contact within the Portal. The required information includes:
  - Full name
  - Email address
  - Telephone number
  - Physical mailing address
- You must provide updated or new contact information for the assigned data security contact within the Portal when the information changes.
- You must ensure your systems are updated to allow service communications from the Portal's designated domain.

Your failure to provide or maintain current data security contact information or enable email communications will not affect our rights to assess fees.

Action 2: Understand your Merchant/Service Provider Level and Validation Documentation Requirements

There are four Merchant Levels applicable to Merchants and two Levels applicable to Service Providers based on your volume of American Express Card Transactions.

- For Merchants, this is the volume submitted by their Establishments that roll up to the highest American Express Merchant account level.*
- For Service Providers, this is the sum of volume submitted by the Service Provider and Entities Service Provider to whom you provide services.

Buyer Initiated Payments (BIP) Transactions are not included in the volume of American Express Card Transactions to determine Merchant Level and validation requirements. You will fall into one of the Merchant Levels specified in Table A-1: Merchant and Service Provider Levels.

* In the case of Franchisors, this includes volume from their Franchisee Establishments. Franchisors who mandate that their Franchisees use a specified Point of Sale (POS) System or Service Provider also must provide validation documentation for the affected Franchisees.

Table A-1: Merchant and Service Provider Levels

Merchant Provider Level	Annual American Express Transactions
Level 1 Merchant	2.5 million American Express Card Transactions or more per year; or any Merchant that American Express otherwise, in its discretion, assigns a Level 1.
Level 2 Merchant	50,000 to fewer than 2.5 million American Express Card Transactions per year.
Level 3 Merchant	10,000 to fewer than 50,000 American Express Card Transactions per year.
Level 4 Merchant	Fewer than 10,000 American Express Card Transactions per year.
Service Provider Level	**Annual American Express Transactions**
Level 1 Service Provider	2.5 million American Express Card Transactions or more per year; or any Service Provider that American Express otherwise deems a Level 1.
Level 2 Service Provider	fewer than 2.5 million American Express Card Transactions per year; or any Service Provider not deemed Level 1 by American Express.

Merchant Validation Documentation Requirements

Merchants (not Service Providers) have four possible Merchant Level classifications. After determining the Merchant level from Table A-1: Merchant and Service Provider Levels (above), see the Table A-2: Merchant Validation Documentation to determine validation documentation requirements.

Table A-2: Merchant Validation Documentation

Merchant Level/ Annual American Express Transactions	Report on Compliance Attestation of Compliance (ROC AOC)	Self-Assessment Questionnaire Attestation of Compliance (SAQ AOC) AND Quarterly External Network Vulnerability Scan (Scan)	Security Technology Enhancement Program (STEP) Attestation for eligible Merchants
Level 1/ 2.5 million or more	Mandatory	Not applicable	Optional with approval from American Express (replaces ROC)
Level 2/ 50,000 to fewer than 2.5 million	Optional	SAQ AOC mandatory (unless submitting a ROC AOC); scan mandatory with certain SAQ types	Optional with approval from American Express* (replaces SAQ and network scan or ROC)
Level 3**/ 10,000 to fewer than 50,000	Optional	SAQ AOC optional (mandatory if required by American Express); scan mandatory with certain SAQ types	Optional with approval from American Express* (replaces SAQ and network scan or ROC)
Level 4**/ Fewer than 10,000	Optional	SAQ AOC optional (mandatory if required by American Express); scan mandatory with certain SAQ types	Optional with approval from American Express* (replaces SAQ and network scan or ROC)

* **Note:** American Express PCI Team will review the request and eligibility and confirm if you qualify for the STEP Program. Please reach out to your Client Manager and/or AXPPCICompliceProgram@aexp.com to check eligibility.

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

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 PCI Security Standards Council approved Qualified Security Assessor (QSA) or PCI Forensic Investigator (PFI).

Service Provider Validation Documentation Requirements

Service Providers (not Merchants) have two possible Level classifications. After determining the Service Provider Level from Table A-1: Merchant and Service Provider Levels (above), see Table A-3: Service Provider Validation Documentation to determine validation documentation requirements.

Service Providers are not eligible for STEP.

Table A-3: Service Provider Validation Documentation

Level	Validation Documentation	Requirement
1	Annual Report on Compliance Attestation of Compliance (ROC AOC)	Mandatory
2	Annual SAQ D (Service Provider) and Quarterly Network Scan or Annual Report on Compliance Attestation of Compliance (ROC AOC), if preferred	Mandatory

It is recommended that Service Providers also comply with the PCI Designated Entities Supplemental Validation.

Security Technology Enhancement Programme (STEP)

Merchants that are compliant with PCI DSS may, at American Express' discretion, qualify for American Express' STEP if they deploy certain additional security technologies throughout their Card processing environments. STEP applies only if the Merchant has not experienced a Data Incident in the previous 12 months and if 75% of all Merchant Card Transactions are performed using a combination of the following enhanced security options:

- **EMV, EMV Contactless or Digital Wallet** – on an active Chip-Enabled Device having a valid and current EMVCo (www.emvco.com) approval/certification and capable of processing AEIPS compliant Chip Card Transactions. (U.S. Merchants must include Contactless)
- **Point-to-Point Encryption (P2PE)** – communicated to the Merchant's processor using a PCI-SSC-approved or QSA-approved Point-to-Point Encryption system
- **Tokenised** – the implemented tokenisation solution must:
  - meet EMVCo specifications,
  - be secured, processed, stored, transmitted, and wholly managed by a PCI compliant third-party service provider, and
  - the Token cannot be reversed to reveal unmasked Primary Account Numbers (PANs) to the Merchant.

Merchants eligible for STEP have reduced PCI Validation Documentation requirements, as further described in Action 3: "Complete the Validation Documentation that you must send to American Express" below.

Action 3: Complete the Validation Documentation that you must send to American Express

The following documents are required for different levels of Merchants and Service Providers as listed in Table A-2: Merchant Validation Documentation and Table A-3: Service Provider Validation Documentation above.

You must provide the Attestation of Compliance (AOC) for the applicable assessment type. The AOC is a declaration of your compliance status and, as such, must be signed and dated by the appropriate level of leadership within your organisation.

In addition to the AOC, American Express may require you to provide a copy of the full assessment and, at our discretion, additional supporting documents demonstrating compliance with the PCI DSS requirements. This Validation Documentation is completed at your expense.

Report on Compliance Attestation of Compliance (ROC AOC) - (Annual 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. There are two versions: one for Merchants and another for Service Providers. The Report on Compliance must be performed by:

- a QSA, or
- an Internal security assessor (ISA) and attested to by your chief executive officer, chief financial officer, chief information security officer, or principal

The ROC AOC must be signed and dated by a QSA or ISA and the authorised level of leadership within your organisation and provided to American Express at least once per year.

Self-Assessment Questionnaire Attestation of Compliance (SAQ AOC) - (Annual Requirement) – 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 SAQ AOC must be signed and dated by the authorised level of leadership within your organisation and provided to American Express at least once per year.

Approved Scanning Vendor External Network Vulnerability Scan Summary (ASV Scan) - (90 Day Requirement) – 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 American Express at least once every 90 days.

If submitting a ROC AOC or STEP, you 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.

STEP Attestation Validation Documentation (STEP) - (Annual Requirement) – STEP is only available to Merchants who meet the criteria listed in Action 2: "Understand your Merchant/Service Provider Level and Validation Documentation Requirements" above. If your company qualifies, you must complete and submit the STEP Attestation form annually to American Express. The Annual STEP Attestation form is available to download from the Portal. You may also reach out to your Client Manager or write to American Express at AXPPCIComplianceProgram@aexp.com.

Non Compliance with PCI DSS - (Annual, 90 Day and/or Ad Hoc Requirement) – If you are not compliant with the PCI DSS, then you must submit a PCI Prioritised Approach Tool (PAT) Summary (available for download via the PCI Security Standards Council website).

The PAT Summary must designate a remediation date, not to exceed twelve (12) months following the document completion date in order to achieve compliance. You shall provide American Express with periodic updates of your progress toward remediation of your Non-Compliant Status (Level 1, Level 2, Level 3, and Level 4 Merchants; all Service Providers). Remediation actions necessary to achieve compliance with PCI DSS are to be completed at your expense.

American Express will not impose non-compliance fees prior to the remediation date. Per Table A-4: Non-Compliance Fee, you remain liable to American Express for all indemnity obligations for a Data Incident and are subject to all other provisions of this policy.

American Express, at its sole discretion, retains the right to impose non-compliance fees if:

- a PCI Prioritised Approach Template has not been submitted in accordance with the requirements stated in this section,
- the remediation steps outlined in the PCI Prioritised Approach Template for Non-Compliant Status were not met,

- any of the requirements of the PCI Prioritised Approach Template for Non-Compliant Status were not fulfilled, or
- the mandatory compliance documentation was not provided to American Express by the applicable deadline or upon request.

Merchants/Service Providers that do not comply with the requirements detailed in Action 2: Understand your Merchant/Service Provider Level and Validation Documentation Requirements, may be subject to fees as stated in Action 4: Send the Validation Documentation to American Express.

For the avoidance of all doubt, Merchants that are not compliant with PCI DSS are not eligible for STEP.

Action 4: Send the Validation Documentation to American Express

All Merchants and Service Providers required to participate in the Programme must submit the Validation Documentation marked "mandatory" in the tables in Action 2: "Understand your Merchant/Service Provider Level and Validation Documentation Requirements" to American Express by the applicable deadlines.

You must submit your Validation Documentation to American Express using the Portal provided by the Programme Administrator selected by American Express. By submitting Validation Documentation, you represent and warrant to American Express that the following is true (to the best of your ability):

- Your evaluation was complete and thorough;
- The PCI DSS status is accurately represented at the time of completion, whether submitting the Attestation of Compliance (AOC) or a PCI Prioritised Approach Tool (PAT) Summary for non-compliance;
- You are authorised to disclose the information contained therein and are providing the Validation Documentation to American Express without violating any other party's rights.

Non-Compliance Fees and Termination of Agreement

American Express has the right to impose non-compliance fees on you and terminate the Agreement if you do not fulfil these requirements or fail to provide the mandatory validation documentation to American Express by the applicable deadline. American Express will attempt to notify the data security contact of the applicable deadline for each annual and quarterly reporting period.

Table A-4: Non-Compliance Fee

Description*	Level 1 Merchant or Level 1 Service Provider	Level 2 Merchant or Level 2 Service Provider	Level 3 or Level 4 Merchant
A non-compliance fee will be assessed if the validation documentation is not received by the first deadline.	USD $25,000	USD $5,000	USD $50
An additional non-compliance fee will be assessed if the validation documentation is not received by the second deadline.	USD $35,000	USD $10,000	USD $100
An additional non-compliance fee will be assessed if the validation documentation is not received by the third deadline. **NOTE:** Non-compliance fees will continue to be applied until the validation documentation is submitted.	USD $45,000	USD $15,000	USD $250

* Non-Compliance Fees will be assessed in Local Currency equivalents.

* Not applicable in Argentina.

If your PCI DSS compliance documentation obligations are not satisfied, then American Express has the right to impose the non-compliance fees cumulatively, withhold payments, and/or terminate the Agreement.

Section 3 Data Incident Management Obligations

You must notify American Express immediately and in no case later than seventy-two (72) hours after discovery of a Data Incident.

To notify American Express, contact the American Express Enterprise Incident Response Programme (*EIRP*) toll free at 1.888.732.3750, or at 1.602.537.3021, or email at EIRP@aexp.com. You must designate an individual as your contact regarding such Data Incident. In addition:

- You must conduct a thorough investigation of each Data Incident and promptly provide to American Express all Compromised Card Numbers. American Express reserves the right to conduct its own internal analysis to identify data involved in the Data Incident.

For Data Incidents involving fewer than 10,000 unique Card Numbers, an investigation summary must be provided to American Express within ten (10) business days of its completion.

- Investigation summaries should contain the following information: incident summary, description of the affected environment(s), timeline of events, key dates, impact and data exposure details, containment and remediation actions, and attestation there is no indication additional American Express data is at-risk.

For Data Incidents involving 10,000 or more unique Card Numbers, you must engage a PCI PFI to conduct this investigation within five (5) days following discovery of a Data Incident.

- The unedited forensic investigation report must be provided to American Express within ten (10) business days of its completion.
- 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 program (as described below). Upon American Express' request, you shall provide validation by a Qualified Security Assessor (QSA) that the deficiencies have been remediated.

Notwithstanding the foregoing paragraphs of this Section 3, "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 fewer than 10,000 unique Card Numbers or where multiple incidents have occurred within a 12-month period. Any such investigation must comply with the requirements set forth above in this Section 3, "Data Incident Management Obligations" and must be completed within the timeframe 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 assess the Data Incident under applicable data breach notification laws globally and, where deemed necessary, notify applicable regulators and impacted Cardmembers in accordance with such data breach notification laws. If you have determined that your Service Provider or another entity is responsible for reporting the Data Incident, you shall advise such Service Provider or entity of its duty to assess its reporting obligations under applicable data breach notification laws. You agree to obtain written approval from American Express prior to referencing or naming American Express in any communications to Cardmembers about the Data Incident. You agree to work with American Express to provide details and rectify any issues arising from the Data Incident, including providing (and obtaining any waivers necessary to provide) to American Express 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 American Express 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.

What to do if you have a Data Incident?

Please follow these steps if you have identified a Data Incident at your business.

Step 1:
Fill out the Merchant Data Incident Initial Notice Form and email to EIRP@aexp.com within 72 hours after the Data Incident is discovered.

Step 2:
Conduct a thorough investigation; this may require you to hire a Payment Card Industry (PCI) Forensic Investigator.

Step 3:
Promptly provide us with all compromised American Express® Card numbers.

Step 4:
Work with us to help resolve any issues arising from the Data Incident.

View Section 3, "Data Incident Management Obligations" for more details on Data Incident Management Obligations.

Have more questions?

US: (888) 732-3750 (toll free)

International: +1 (602) 537-3021

EIRP@aexp.com

Section 4 Indemnity Obligations for a Data Incident

Your indemnity obligations to American Express under the Agreement for Data Incidents shall be determined, without waiving any of American Express' other rights and remedies, under this Section 4, "Indemnity Obligations for a Data Incident". In addition to your indemnity obligations (if any), you may be subject to a Data Incident non-compliance fee as described below in this Section 4, "Indemnity Obligations for a Data Incident".

You shall compensate American Express at the rate of $5 USD per account number, for Data Incidents that involve:

- 10,000 or more American Express Card Numbers with either of the following:
  - Sensitive Authentication Data, or
  - Expiration Date

However, American Express will not seek indemnification from you for a Data Incident that involves:

- fewer than 10,000 American Express Card Numbers, or
- more than 10,000 American Express Card Numbers, if you meet the following conditions:
  - you notified American Express of the Data Incident pursuant to Section 3, "Data Incident Management Obligations",
  - you were in compliance at the time of the Data Incident with the PCI DSS (as determined by the PFI's investigation of the Data Incident), and
  - the Data Incident was not caused by your wrongful conduct or that of your Covered Parties.

Notwithstanding the foregoing paragraphs of this Section 4, "Indemnity Obligations for a Data Incident", for any Data Incident, regardless of the number of American Express Card Numbers, you shall pay American Express a Data Incident non-compliance fee not to exceed USD $100,000 per Data Incident (as determined by American Express in its sole discretion) in the event that you fail to comply with any of your obligations set forth in

Section 3, "Data Incident Management Obligations". For the avoidance of doubt, the total Data Incident non-compliance fee assessed for any single Data Incident shall not exceed USD $100,000.

American Express will exclude from its calculation any American Express Card Account Number that was involved in a prior Data Incident indemnity claim made within the twelve (12) months prior to the Notification Date. All calculations made by American Express under this methodology are final.

American Express may bill you for the full amount of your indemnity obligations for Data Incidents or deduct the amount from American Express' payments to you (or debit your Bank Account accordingly) pursuant to the Agreement.

Your indemnity obligations for Data Incidents hereunder shall not be considered incidental, indirect, speculative, consequential, special, punitive, or exemplary damages under the Agreement; provided that such obligations do not include damages related to or in the nature of lost profits or revenues, loss of goodwill, or loss of business opportunities.

In its sole discretion, American Express may reduce the indemnity obligation for Merchants solely for Data Incidents that meet each of the following criteria:

- Applicable Risk-Mitigating Technologies were used prior to the Data Incident and were in use during the entire Data Incident Event Window,
- A thorough investigation in accordance with the PFI programme was completed (unless otherwise previously agreed in writing),
- Forensic report clearly states the Risk-Mitigating Technologies were used to process, store, and/or transmit the data at the time of the Data Incident, and
- You do not store (and did not store throughout the Data Incident Event Window) Sensitive Authentication Data or any Cardholder Data that has not been made unreadable.

Where an indemnity reduction is available, the reduction to your indemnity obligation (excluding any non-compliance fees payable), is determined as follows:

Table A-5: Criteria for Indemnity Obligation Reduction

Indemnity Obligation Reduction	Required Criteria
Standard Reduction: 50%	>75% of total Transactions processed on Chip Enabled Devices[1] OR
	Risk-Mitigating Technology in use at >75% of Merchant locations[2]
Enhanced Reduction: 75% to 100%	>75% of all Transactions processed on Chip Enabled Devices[1] AND another Risk-Mitigating Technology in use at >75% of Merchant locations[2]

[1] As determined by American Express internal analysis

[2] As determined by PFI investigation

- The Enhanced Reduction (75% to 100%) shall be determined based on the lesser of the percentage of Transactions using Chip Enabled Devices AND Merchant locations using another Risk-Mitigating Technology. The examples in Table A-6: Enhanced Indemnity Obligation Reduction illustrate the calculation of the indemnity reduction.
- To qualify as using a Risk-Mitigating Technology, you must demonstrate effective utilisation of the technology in accordance with its design and intended purpose.
- The percentage of locations that use a Risk-Mitigating Technology is determined by PFI investigation.
- The reduction in the indemnity obligation does not apply to any non-compliance fees payable in relation to the Data Incident.

Table A-6: Enhanced Indemnity Obligation Reduction

Ex.	Risk- Mitigating Technologies in use	Eligible	Reduction
1	• 80% of Transactions on Chip Enabled Devices • 0% of locations use other Risk-Mitigating Technology	No	50%: Standard Reduction (less than 75% use of Risk-Mitigating Technology does not qualify for Enhanced Reduction)[1]
2	• 80% of Transactions on Chip Enabled Devices • 77% of locations use other Risk-Mitigating Technology	Yes	77%: Enhanced Reduction (based on 77% use of Risk-Mitigating Technology)
3	• 93% of Transactions on Chip Enabled Devices • 100% of locations use other Risk-Mitigating Technology	Yes	93%: Enhanced Reduction (based on 93% of Transactions on Chip Enabled Devices)
4	• 40% of Transactions on Chip Enabled Devices • 90% of locations use other Risk-Mitigating Technology	No	50%: Standard Reduction (less than 75% of Transactions on Chip Enabled Devices does not qualify for Enhanced Reduction)

[1] A Data Incident involving 10,000 American Express Card Accounts, at a rate of USD $5.00 per account number (10,000 x $5 = USD $50,000) may be eligible for a reduction of 50%, reducing the Indemnity Obligations from USD $50,000 to USD $25,000, excluding any non-compliance fees.

Section 5 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 you are 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, 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.
- You must provide updated PCI DSS validation documents in accordance with Section 2, "PCI DSS Compliance Program (Important Periodic Validation of your Systems)".
- As applicable, you must engage a qualified PCI 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 3, "Data Incident Management Obligations".

Table A-7: TAP Non-Compliance Fee

Description	Level 1 Merchant or Level 1 Service Provider	Level 2 Merchant or Level 2 Service Provider	Level 3 or Level 4 Merchant
Non-compliance fee may be assessed when TAP obligations are not satisfied by the first deadline.	USD $25,000	USD $5,000	USD $1,000
Non-compliance fee may be assessed when TAP obligations are not satisfied by the second deadline.	USD $35,000	USD $10,000	USD $2,500
Non-compliance fee may be assessed when TAP obligations are not satisfied by the third deadline. **NOTE:** *Non-compliance fees may continue to be applied until the obligations are met or TAP is resolved.*	USD $45,000	USD $15,000	USD $5,000

If your TAP obligations are not satisfied, then American Express has the right to impose the Non-compliance fees cumulatively, withhold payments, and/or terminate the Agreement.

Section 6 Confidentiality

American Express shall take reasonable measures to keep (and cause its agents and subcontractors, including the Portal provider, to keep) your reports on compliance, including the Validation Documentation in confidence and not disclose the Validation Documentation to any third party (other than American Express' Affiliates, agents, representatives, Service Providers, and subcontractors) for a period of three years from the date of receipt, except that this confidentiality obligation does not apply to Validation Documentation that:

a. is already known to American Express prior to disclosure;

b. is or becomes available to the public through no breach of this paragraph by American Express;

c. is rightfully received from a third party by American Express without a duty of confidentiality;

d. is independently developed by American Express; or

e. is required to be disclosed by an order of a court, administrative agency or governmental authority, or by any law, rule or regulation, or by subpoena, discovery request, summons, or other administrative or legal process, or by any formal or informal inquiry or investigation by any government agency or authority (including any regulator, inspector, examiner, or law enforcement agency).

Section 7 Disclaimer

AMERICAN EXPRESS HEREBY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND LIABILITIES WITH RESPECT TO THIS DATA SECURITY OPERATING POLICY, 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. AMERICAN EXPRESS CARD ISSUERS ARE NOT THIRD PARTY BENEFICIARIES UNDER THIS POLICY.

Section 8 Glossary

For purposes of this *Data Security Operating Policy* only, the following definitions apply and control in the event of a conflict with the terms found in the *Merchant Regulations:*

Account Data consists of Cardholder Data and/or sensitive authentication data. See Cardholder Data and Sensitive Authentication Data.

Agreement means the General Provisions, the Merchant Regulations, and any accompanying schedules and exhibits, collectively (sometimes referred to as the Card Acceptance Agreement in our materials).

American Express Card, or **Card**, means 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, included on PCI SSC list of validated solutions or validated by a PCI SSC Qualified Security Assessor P2PE Company.

Approved Scanning Vendor (ASV) means 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.

Attestation of Compliance (AOC) means 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) means 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.

Buyer Initiated Payment (BIP) Transactions means a digital payment solution that lets buyers quickly and efficiently schedule payments to suppliers (linked to corporate cards).

Cardholder means a customer to which payment card is issued, or any individual authorised to use the payment card.

Cardholder Data means at a minimum, the full Primary Account Number (PAN) by itself or full PAN plus any of the following: cardholder name, expiration date, and/or service code. See Sensitive Authentication Data for additional data elements that might be transmitted or processed (but not stored) as part of a payment transaction.

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

Cardmember means an individual or entity (i) that has entered into an agreement establishing a Card account with an issuer or (ii) whose name appears on the Card.

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

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

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

Charge means a payment or purchase made on a Card.

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

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

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

Chip-Enabled Device means 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.

Compromised Card Number means an American Express Card account number related to a Data Incident.

Consumer is defined as a cardholder purchasing goods, services, or both.

Covered Parties means 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.

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

Credit Record means a record of Credit that complies with our requirements.

Data Incident means 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 means the window of intrusion (or similarly determined period of time) set forth in the final forensic report (e.g., 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.

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

EMV Transaction means 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 (American Express encryption key) means 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 Key (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.

Franchisee means an independently owned and operated third party (including a franchisee, licensee, or chapter) other than an Affiliate that is licensed by a Franchisor to operate a franchise and that has entered into a written agreement with the Franchisor whereby it consistently displays external identification prominently identifying itself with the Franchisor's Marks or holds itself out to the public as a member of the Franchisor's group of companies.

Franchisor means the operator of a business that licenses persons or Entities (Franchisees) to distribute Goods and/or Services under, or operate using the operator's Mark; provides assistance to Franchisees in operating their business or influences the Franchisee's method of operation; and requires payment of a fee by Franchisees.

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

Level 2 Merchant means a Merchant with 50,000 to fewer than 2.5 million American Express Card Transactions per year.

Level 3 Merchant means a Merchant with 10,000 to fewer than 50,000 American Express Card Transactions per year.

Level 4 Merchant means a Merchant with fewer than 10,000 American Express Card Transactions per year.

Level 1 Service Provider means a Service Provider with 2.5 million American Express Card Transactions or more per year; or any Service Provider that American Express otherwise deems a Level 1.

Level 2 Service Provider means a Service Provider with fewer than 2.5 million American Express Card Transactions per year; or any Service Provider not deemed Level 1 by American Express.

Merchant means the Merchant and all of its affiliates that accept American Express Cards under an Agreement with American Express or its affiliates.

Merchant Level means the designation we assign Merchants related to their PCI DSS compliance validation obligations, as described in Section 2, "PCI DSS Compliance Program (Important Periodic Validation of your Systems)".

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

Payment Application has the meaning given to it in the then current Glossary of Terms for Secure Software Standard and Secure Software Life Cycle Standard, which is available at www.pcisecuritystandards.org.

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

Payment Card Industry Security Standards Council (PCI SSC) Requirements means 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 means that a PIN Entry Device or a Payment Application (or both) 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 means Payment Card Industry Data Security Standard, which is available at www.pcisecuritystandards.org.

PCI Forensic Investigator (PFI) means 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 means the Payment Card Industry PIN Security Requirements which is 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 (PTS) Point of Interaction (POI), Modular Security Requirements, which is available at www.pcisecuritystandards.org.

Point of Sale (POS) System means 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.

Point-to-Point Encryption (P2PE) means a solution that cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption.

Portal, The means the reporting system provided by the American Express PCI Programme administrator selected by American Express. Merchants and Service Providers are required to use The Portal to submit PCI validation documentation to American Express.

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

Processor means a service provider to Merchants who facilitate authorisation and submission processing to the American Express network.

Programme, The means the American Express PCI Compliance Programme.

Qualified Security Assessor (QSA) means an entity that has been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to the PCI DSS.

Risk-Mitigating Technology means technology solutions that improve the security of American Express Cardholder Data and Sensitive Authentication Data, as determined by American Express. To qualify as a Risk-Mitigating Technology, you must demonstrate effective utilisation of the technology in accordance with its design and intended purpose. Examples include, but may not be limited to: EMV, Point-to-Point Encryption, and tokenisation.

Security Technology Enhancement Programme (STEP) means the American Express programme in which Merchants are encouraged to deploy technologies that improve data security.

Self-Assessment Questionnaire (SAQ) means 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 means security-related information used to authenticate cardholders and/or authorise payment card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.

Service Providers means authorised processors, third party processors, gateway providers, integrators of POS Systems, and any other providers to Merchants of POS Systems, or other payment processing solutions or services.

Targeted Analysis Programme means a programme that provides early identification of a potential Cardholder data compromise in your Cardholder Data Environment (CDE). See Section 5, "Targeted Analysis Programme (TAP)".

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

Transaction means a Charge, Credit, Cash Advance (or other cash access), or ATM Transaction completed by the means of a Card.

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

Validation Documentation means 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 Security Technology Enhancement Programme Attestation.

Section 9 Useful Websites

American Express Data Security: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

EMVCo: www.emvco.com

AMERICAN EXPRESS

Notification of Changes

Important current and future scheduled changes are set out in the Notification of Changes section of the *Merchant Regulations*. Updated provisions from previous publications are in **bold**.

Notification of Current Changes

Effective Date	Subject	Description of change	Page
April 17, 2026	Travel Authorisations	Updated the Authorisation Validity Period for Car Rental, Lodging, and Steamships & Cruise Lines Authorisations from the duration of the stay or the agreement to 30 days.	132
May 18, 2026	Changes to the Merchant Regulations	• Added new provision outlining Merchant obligations and acceptance process for changes to the *Merchant Regulations*. • Revised language to address scheduled and unscheduled changes to the *Merchant Regulations*.	133

Notification of Previously Announced Changes

Effective Date	Subject	Description of change	Page
October 16, 2026	MCC Mismatch	• Updated policy to state that an MCC Mismatch may lead to a Chargeback. • Updated Chargeback Reason Code A08 in ISO Code 4521 Invalid Authorisation to include an MCC Mismatch.	134

Travel Authorisations

Overview	Updated the Authorisation Validity Period for Car Rentals, Lodging, and Steamships & Cruise Lines.
Effective date	**April 17, 2026**
Merchant benefits and implications	Standardised the Authorisation Validity Period for Car Rentals, Lodging, and Steamships & Cruise Lines.
Date announced in *Merchant Regulations*	October 2024
Text in the *Merchant Regulations*	Review the highlighted text in the following sections/subsections that support this policy. • Section 3.3.1, "Estimated Authorisation" • Section 3.3.2, "Estimated Charge Amount"

Changes to the Merchant Regulations

Overview	• Added new provision outlining Merchant obligations and acceptance process for changes to the *Merchant Regulations*. • Revised language to address scheduled and unscheduled changes to the *Merchant Regulations*.
Effective date	**May 18, 2026**
Merchant benefits and implications	Changes to the *Merchant Regulations* will take effect at least 30 days after publication unless otherwise necessary to comply with Applicable Law.
Date announced in *Merchant Regulations*	April 2026
Text in the *Merchant Regulations*	Review the highlighted text in the following sections/subsections that support this policy. • Section 1.2, "Changes in the Merchant Regulations"

MCC Mismatch

Overview	Updated policy language to advise Merchant that an incorrect MCC in the Submission could expose the Merchant to Chargebacks and expanded ISO 4521 - Invalid Authorisation to include MCC Mismatch.
Effective date	**October 16, 2026**
Merchant benefits and implications	Merchants should ensure the MCC sent with the Submission matches the MCC sent in the Authorisation.
Date announced in *Merchant Regulations*	October 2025
Text in the *Merchant Regulations*	Review the highlighted text in the following sections/subsections that support this policy. • Subsection 1.4.1 Merchant Category Codes • Subsection 5.6.1 Authorisation

1.4.1 Merchant Category Codes

a. You must provide us with an accurate and complete description of your business so we can assign a Merchant Category Code (MCC) and industry classification to your Merchant Number. You must use the most accurate MCCs in all Authorisations and Submissions. If you have multiple, distinct businesses that may qualify for more than one MCC, we will assign the appropriate MCCs and Merchant Numbers. If you have multiple businesses, but a distinction between them is unclear, then we will assign the MCC most closely representing your primary business.

b. 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. **Failure to correctly utilise the MCC in the Submission could expose the Merchant to Chargebacks.**

c. We reserve the right to require and implement corrections to the MCC assignments and use in our sole discretion and without advance notice.

5.6.1 Authorisation

Table 5-5: Invalid Authorisation (ISO 4521) / Authorisation approval expired or MCC Mismatch (A08)

Invalid Authorisation (ISO 4521) / Authorisation approval expired or **MCC Mismatch** (A08)	
Description	The Transaction was submitted after the Authorisation Approval **expired or the MCC in the Submission did not match the MCC in the Authorisation request**.
Information provided with the Chargeback	• Transaction Data **In addition, for MCC Mismatch** • **The MCC received in the Authorisation and the Submission; and** • **An explanation on why the Issuer took a loss due to the MCC in the Submission and a statement that the Issuer would have declined the Authorisation with the MCC from the Submission.**
Support required to request a Chargeback Reversal	• Proof that a valid Authorisation Approval was obtained in accordance with the Agreement~~, or~~ • Proof that a Credit which directly offsets the Disputed Transaction has already been processed**, or** • **Proof that the MCC submitted in the Authorisation matches the MCC in the Submission.**

AMERICAN EXPRESS

Previous Versions

2025

April 2025

October 2025

2024

April 2024

October 2024

2023

April 2023

October 2023

2022

April 2022

October 2022

2021

April 2021

October 2021

2020

April 2020

October 2020