AMERICAN EXPRESS

Merchant Regulations

International

October 2020

DON'T *do business* WITHOUT IT℠

AMERICAN EXPRESS

AMERICAN EXPRESS

Summary of Changes

Change Icons

Important updates are listed in the Summary of Changes Table and also indicated in the *Merchant Regulations* with a change icon. A change icon alongside the title of a section or subsection denotes revised, added, or removed text from the section or subsection. Changes in the *Merchant Regulations* are indicated with a change icon as shown here.

Summary of Changes Table

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

Chapter	Section/Subsection	Description of Change
Chapter 1, "Introduction"	Section 1.1, "About the Merchant Regulations"	Clarified Applicable Law.
	Section 1.3, "Compliance with our Specifications"	Added requirement to comply with Specifications.
Chapter 2, "General Policies"	Subsection 2.1.5, "Contactless"	Updated reference to Maximum Amount for a Contactless Transaction.
	Section 2.4, "Authorisation"	Updated Estimated Authorisation language.
	Subsection 2.4.1, "Estimated Authorisation"	Relocated Estimated Authorisation language.
	Section 2.7, "Disputed Charges"	Updated the Disputed Charge timeframe.
	Subsection 2.7.2, "Fraud Full Recourse Programme"	Added high risk industries requirement.
	Section 2.10, "American Express SafeKey Programme"	Updated language by removing specific versions of SafeKey. Updated language applies to all SafeKey Transactions. Created two sections for SafeKey Programme with respective terms.

Chapter	Section/Subsection	Description of Change
Chapter 3, "Special Regulations for Specific Industries"	Subsection 3.2.1, "Prohibited Industries"	Added Merchant Category Codes (MCCs) for clarification. Updated descriptions.
	Subsection 3.2.2, "Restricted Industries"	Added Merchant Category Codes (MCCs) for clarification.
	Subsection 3.5.1, "Onboard Charges"	Relocated Estimated Authorisation language.
	Subsection 3.7.1, "Authorisation"	Relocated Estimated Authorisation language.
	Subsection 3.8.2, "Rental"	Relocated Estimated Authorisation language.
	Section 3.9, "Payment Aggregators"	Provided detail on Payment Aggregators' acquiring requirements.
	Section 3.10, "Restaurants"	Relocated Estimated Authorisation language.
	Section 3.11, "Taxicabs and Limousines"	Relocated Estimated Authorisation language.
Chapter 4, "Country Specific Policies"		Updated Maximum Amount for a Contactless Transaction with No CVM thresholds for select countries. Added Mexico-related thresholds and requirements.
Glossary		Added/modified definitions (e.g., American Express Card or Cards, Debit Card, Electronic Commerce Indicator, Merchant Category Code, Third Party Issuer.)
Appendix A, "Data Security Operating Policy (DSOP)"	Throughout Appendix	Updated Trustwave references to SecureTrust.
	Section 1, "Standards for Protection of Encryption Keys, Cardholder Data, and Sensitive Authentication Data"	Enhanced language for clarification and ease of communicating compliance expectation.
	Section 3, "Indemnity Obligations for a Data Incident"	Clarified language regarding the exclusion of Card Account Numbers for calculation purposes of an Indemnity claim.
	Section 4, "Important Periodic Validation of Your Systems"	Clarified language for Actions 1, 2, and 4. Clarified language on the non-validation fee.

Notification of Future Changes Table

Important updates are described in the following table.

<table>
<tr><th>Effective Date</th><th colspan="2">Current Language</th><th colspan="2">New Language</th></tr>
<tr><td>April 2021</td><td colspan="2">N/A - New Section</td><td colspan="2">2.3.1.1 Introductory Offers
a. If you offer Cardmembers an option to make Recurring Billing Charges that include an Introductory Offer, you must comply with all requirements set forth in this Subsection 2.3.1, "Recurring Billing", in addition to the following requirements:
i. Clearly and conspicuously disclose all material terms of the Introductory Offer to the Cardmember, including a simple and expeditious cancellation process that allows the Cardmember to cancel before submitting the first Recurring Billing Charge;
ii. Obtain the Cardmember's express consent to accept 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 Charge, that allows the Cardmember a reasonable amount of time to cancel.</td></tr>
<tr><td rowspan="2">April 2021</td><td colspan="2">Chapter 4, "Country Specific Policies"</td><td colspan="2">Chapter 4, "Country Specific Policies"</td></tr>
<tr><td>Country</td><td>EMV Requirement</td><td>Country</td><td>EMV Requirement</td></tr>
<tr><td></td><td>Mexico</td><td>Chip Only Country</td><td>Mexico</td><td>Chip and PIN Country</td></tr>
</table>

AMERICAN EXPRESS

Table of Contents

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* at the beginning of the document. 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.

1.3 Compliance with our Specifications

a. You must comply with our *Technical Specifications* 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.

1.4 Compliance with our Data Security Operating Policy

a. You must comply with our Data Security Operating Policy, as set forth in Appendix A, "Data Security Operating Policy (DSOP)". 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

General Policies

2

2.1 In-Person Charges

a. For all In-Person Charges the Card must be presented and you must:

i. not accept a Card that is visibly altered or mutilated, or presented by anyone other than the Cardmember, and, if a Transaction is declined, you must notify the Cardmember immediately;

ii. follow the Card acceptance steps outlined below in Subsection 2.1.1, "Chip Cards" through Subsection 2.1.6, "Unattended Terminals" as applicable; and

iii. obtain an Authorisation.

2.1.1 Chip Cards

a. For Chip and personal identification number (PIN) Countries and Chip Only Countries, as indicated in Chapter 4, "Country Specific Policies", you must ensure that your POS Systems accepts Chip Cards, and follow the procedures below.

i. When presented with a Chip Card, the Card must be inserted into the reader of the POS System (unless the Charge is processed through Contactless Technology, in which case you must follow the steps outlined in Subsection 2.1.5, "Contactless").

ii. If you are in a Chip and PIN Country, the POS System must capture Chip Card Data and the POS System should advise the Cardmember to enter the PIN (a "Chip and PIN Transaction") or any other Cardholder Verification Method (CVM), excluding Cardmember signature. Upon such advice, your Establishment must ensure that the Cardmember completes the applicable CVM when prompted by the POS System. In a Chip Only Country, the POS System may also advise for the Cardmember to enter a CVM. In a Chip Only Country, if you choose to obtain a Cardmember signature, see Subsection 2.1.3, "Obtaining Cardmember Signature".

iii. If the Establishment 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 Establishment to capture full magnetic stripe data by following the procedure for non-Chip Card Transactions (See Subsection 2.1.2, "Non-Chip Cards").

iv. If your Establishment swipes a Chip Card through, or manually keys a Charge into, the POS System when no technical problem exists, the issuer may decline the Transaction and, if it does not, we may have Chargeback rights for fraudulent In-Person Charges.

v. In addition to Subsection 2.1.1. (iv), you will be liable for any losses that we may suffer and we will have Chargeback rights for fraudulent In-Person Charges, and/or we may terminate the agreement, if:

a. the POS System has not been upgraded to accept Chip Cards; or

b. you and your Processing Agent do not have the ability to capture and send Chip Card Data; or

c. we have not certified the POS System to accept Chip Transactions or Chip and PIN Transactions as indicated under EMV®[1] Requirements, as specified in Chapter 4, "Country Specific Policies".

vi. In all cases, you will be liable for fraudulent Charges arising from a failure to comply with our Card acceptance procedures.

2.1.2 Non-Chip Cards

a. For In-Person Charges where the Card is not a Chip Card, or in non-Chip Countries, the POS System will provide instructions for you to swipe, and you must swipe the Card through the POS System (unless the Charge is processed through Contactless Technology, in which case you must follow the steps outlined in Subsection 2.1.5, "Contactless"). You must:

i. ensure that the Card is being used within any valid dates shown on its face;

ii. ensure that the account number on the face of the Card matches the account number on its back and there is a Card Identification Number (CID);

iii. verify that the signature panel of the Card is signed, where applicable, and is the same name as the name on its face (except for Prepaid Cards that show no name on their face);

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.

iv. verify that the Cardmember's name and signature, if obtained, on the Charge Record matches the name and signature on the Card, or for a Prepaid Card that shows no name on its face, that the signature on the back of such Prepaid Card matches the signature on the Charge Record, if obtained; and

v. verify that the Card account number and expiration date printed on the Charge Record matches the Card account number and expiration date on the Card.

b. You may obtain the Cardmember's signature on the Charge Record. If you choose to obtain a Cardmember signature, or are required to do so by law, see Subsection 2.1.3, "Obtaining Cardmember Signature".

c. If your POS System fails then, in addition, you must seek a voice Authorisation (See Section 2.4, "Authorisation").

d. If the magnetic stripe is unreadable, the Charge may be keyed into the POS System manually and you must obtain an imprint of the Card to verify that the Card was present. A pencil rubbing or photocopy of the Card is not considered to be a valid imprint. If you do not take a manual imprint where required, and make it available to us on request, we will have Chargeback rights for such Charge.

2.1.3 Obtaining Cardmember Signature

a. Obtaining Cardmember signature on In-Person Charges is optional to complete a Charge Record, and at your discretion, unless required by Applicable Law.

b. If you choose to obtain a Cardmember signature on a manual imprint, printed, or electronic In-Person Charge, you must:

i. obtain signature on the Charge Record; and

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

iii. verify that the signature on the Charge Record matches the signature on the Card; except in the case of Prepaid Cards that may not include a signature.

c. You must still obtain the Cardmember's signature for all Transactions that are made pursuant to an American Express instalment payment plan or as communicated to you from time to time that you need to do so.

2.1.4 No CVM Programme

a. Save as expressly set out elsewhere, Transactions conducted within the European Economic Area (EEA) will not qualify for the No CVM Programme unless it is a Contactless Transaction at an Expresspay enabled POS System. If your Establishment is located outside the EEA, you may choose not to request a CVM from Cardmembers where:

i. the Charge amount equals or is less than the value provided in the Maximum Amount for a Contact Transaction without a CVM column indicated in Chapter 4, "Country Specific Policies";

ii. the Charge submission includes the appropriate indicator to reflect the Card and the Cardmember were present at the POS System; and

iii. the Charge includes a valid Authorisation approval.

b. Under the No CVM Programme, we will not exercise Chargeback for such Charges based solely on the failure to obtain the Cardmember's CVM. Nonetheless, you are required to comply with our request for written response to a Disputed Charge related to fraud for not capturing a CVM. Even if an Establishment and a Charge qualify under the No CVM Programme, we have the right to Chargeback for reasons unrelated to the Establishment's failure to obtain a CVM from the Cardmember at the POS System. The No CVM Programme does not apply to Disputed Charges involving customer service or goods and services disputes. If we receive disproportionate numbers of Disputed Charges under the No CVM Programme, you must work with us to reduce the number of disputes. If such efforts fail, we may exercise our Chargeback rights and/or modify or terminate your participation in the No CVM Programme.

c. You may only participate in the No CVM Programme if we classify you in an industry that accepts In-Person Charges, except in the following instances:

i. Your Establishment does not conduct In-Person Charges (i.e., Internet, mail order, telephone order);

ii. We consider your Establishment to be high risk;

iii. Your Establishment is placed in the Fraud Full Recourse Programme; or

iv. We deem, in our sole discretion, your Establishment is ineligible for any other reason.

2.1.5 Contactless

a. When presented with a Chip Card or Mobile Device to be read via Contactless Technology and the Charge is equal or less than the applicable Maximum Amount for a Contactless Transaction with No CVM set out in Chapter 4, "Country Specific Policies", you must:

   i. capture the Charge Data using the Contactless reader; and

   ii. obtain Authorisation;

b. If the Charge amount is over the Maximum Amount for a Contactless Transaction with No CVM, if you are unable to complete a Contactless Transaction, or if prompted by your POS System, you will need to follow the process set out in Subsection 2.1.1, "Chip Cards".

c. For Digital Wallet Contactless-initiated Transactions, a Consumer Device Cardmember Verification Method (CDCVM) is permitted if the Mobile Device and the POS System are capable of performing CDCVM. For these Charges, you must create a Charge Record as described in Section 2.5, "Charge or Credit Records", including an indicator that the Transaction is a Digital Wallet Contactless-initiated Transaction. To ensure proper POS System acceptance for Digital Wallet Contactless-initiated Transactions, you should comply with the most current American Express Contactless-enabled POS System requirements.

d. We will not exercise missing imprint, counterfeit, lost, stolen, or non-received fraud Chargebacks for Contactless or Digital Wallet Contactless-initiated Transactions if the Establishment successfully verifies the Cardmember and meets all of the criteria and requirements listed above. This does not apply to Disputed Charges involving dispute reasons other than fraud (e.g., it does not apply to goods or services disputes). Nonetheless, you are required to comply with our request for written response to a Disputed Charge related to fraud for Contactless or Digital Wallet Contactless-initiated Transactions.

e. If you have the ability to process Consumer-Presented Quick Response Code (CPQR) Transactions, you must:

   i. clearly inform the Cardmember that they can pay for the purchase by generating a QR Code;

   ii. use a scanning device easily accessible to the Cardmember, but placed in such a manner that there is no possibility that the Cardmember's device is triggered due to proximity; and

   iii. if the presented QR Code fails to be scanned, request:

      a. the QR Code be re-presented;

      b. an alternative payment method be used; or

   iv. obtain an Authorisation.

2.1.5.1 Merchant-Presented Quick Response (MPQR)

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

   i. have the Cardmember use their Mobile device to scan the MPQR code;

   ii. display the Quick Response (QR) code, which can be dynamic or static, for scanning by the Cardmember;

   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 you do not receive the notification, you should contact us to confirm the status of the MPQR Transaction;

   v. contact us or decline the Transaction if you are suspicious of the Cardmember or receive notification from us to do so;

   vi. retain records of MPQR Transactions. These can be in the form of a notification from us, an invoice, or other documentation of the Transaction; and

   vii. obtain an Authorisation.

2.1.6 Unattended Terminals

a. We will accept Charges for purchases at your unattended POS Systems (e.g., Customer Activated Terminals (CATs) or payment kiosks) subject to the Charge Records requirements in Section 2.5, "Charge or Credit Records", and the following additional requirements. You must:

- **i.** include in all requests for Authorisation the full magnetic stripe stream or Chip Card Data;
- **ii.** ensure the Charge complies with the 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 we may provide to you if you accept the Card at an unattended POS System that is part of, or attached to, a fuel dispenser; and
- **iv.** ensure that the unattended POS System notifies the Cardmember if the Transaction is declined, where technically feasible.

b. In Chip and PIN Countries, as indicated in Chapter 4, "Country Specific Policies", if an unattended POS System is not configured for Chip and PIN Transactions then you may still accept the Card and the provisions of Subsection 2.1.1, "Chip Cards" will not apply in relation to completing the applicable CVM. However, if you do so, you will be liable for any losses and we will have Chargeback rights for fraudulent In-Person Charges made with lost, stolen and non-received Chip Cards.

c. In Chip Only Countries, as indicated in Chapter 4, "Country Specific Policies", if an unattended POS System is not configured for Chip Card Transactions you may still accept the Card. However, if you do so, you will be liable for any losses and we will have Chargeback rights for fraudulent In-Person Charges made with counterfeit Chip Cards.

2.2 Card Not Present Charges

a. For Card Not Present Charges, you must:

- **i.** create a Charge Record as described in Section 2.5, "Charge or Credit Records", including an indicator that the Transaction is Card Not Present and a designation of "mail order," "telephone order," "Digital Order," "fax order" or "Signature on File," as applicable, on the signature line or the appropriate electronic descriptor on the Charge Record;
- **ii.** obtain the Cardmember's name as it appears on the Card, the Card account number or Token and expiry date, the Cardmember's billing address, and the delivery address;
- **iii.** obtain Authorisation;
- **iv.** if the order is to be shipped or delivered more than seven (7) days after the original Authorisation, obtain a new Authorisation before shipping or delivering the order; and
- **v.** 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 you should treat the Transaction as an In-Person Charge and comply with the provisions provided in Section 2.1, "In-Person Charges".

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

d. If you wish to accept orders for goods or services where the card is not physically presented to you, then you do so at your own risk. We have Chargeback rights for any Card Not Present Charge that the Cardmember denies making or authorising. This excludes Transactions that qualify for the AESK Programme. We will not exercise our Chargeback rights for Card Not Present Charges based solely upon a Cardmember claim that he or she did not receive the disputed goods if you have verified with us that the address to which the goods were shipped is the Cardmember's billing address and obtained a receipt signed by an authorised signer verifying the delivery of the goods to such address.

2.2.1 Digital Orders

a. We will accept Charges for Digital Orders subject to the requirements above in this Section 2.2, "Card Not Present Charges" and the following additional requirements. You must:

- **i.** send Charge Data concerning any Digital Order via the internet, email, intranet, extranet, or other digital network or any other electronic mail medium only to the Cardmember who made the Digital Order, your Processor or us, in accordance with Appendix A, "Data Security Operating Policy (DSOP)";
- **ii.** submit all Charges for Digital Orders electronically;
- **iii.** use any separate Establishment Numbers that we provide you for Digital Orders in all your requests for Authorisation and submissions of Charges for Digital Orders;
- **iv.** ensure your websites that permit Cardmembers to make Digital Orders are identified by extended validation certificates or by other similar authentication methods in order to restrict the use of fraudulent websites;
- **v.** employ appropriate controls to separate payment related processes from your online shop to enable the Cardmember to determine whether they are communicating with you or us; and
- **vi.** provide us with at least one (1) month's prior written notice of any change in your website address.

b. We reserve the right not to accept Digital Orders immediately if any event or series of events occurs which in our opinion may affect your ability to comply with your obligations under the Agreement or to any Cardmember.

c. We may dispense with the notice period, as set out in the Agreement, and immediately notify you of additional requirements, including our encryption software requirements and security guidelines, in order to protect the security of Digital Orders and/or Cardmember Information and/or to prevent fraud.

d. We will not be liable for fraudulent Digital Orders. We will have the right to Chargeback for Charges transacted over the Internet, even if you have received an Authorisation approval code and have complied with all other provisions of this Agreement. Additionally, if a Disputed Charge arises involving a Card Not Present Charge that is a Digital Delivery Transaction, we will exercise our Chargeback rights for the full amount of the Charge.

e. You must ensure that your website or applicable digital medium notifies the Cardmember if the Transaction is declined for Authorisation.

f. For Digital Wallet Application-initiated Transactions, you will (i) certify for Digital Wallet Application-initiated Transactions with your Processor, terminal provider, or if you have a direct link to us, your American Express representative and (ii) follow Card Not Present Charge requirements set forth in this Section 2.2, "Card Not Present Charges". If applicable, a CDCVM is permitted if the Mobile Device is capable of performing CDCVM. For these Charges, you must create a Charge Record as described in Section 2.5, "Charge or Credit Records". For these Charges to qualify as a Digital Wallet Application-initiated Transaction, you must include an indicator that the Transaction is a Digital Wallet Application-initiated Transaction on the Charge Record. We will not exercise a missing imprint fraud Chargeback for Digital Wallet Application-initiated Transactions if the Establishment meets all off the criteria and requirements set out in this paragraph. The preceding sentence does not apply to Disputed Charges involving dispute reasons other than fraud (e.g., it does not apply to goods or services disputes).

g. In circumstances where you accept Charges for Digital Orders that are verified by the American Express SafeKey Programme, we may offer the Cardmember the option to pay for their purchase with points. This does not impact the relationship between you and us and does not change either party's rights or obligations under this Agreement. However, if you prefer that we do not offer this functionality to Cardmembers using your digital platform then please write to us using the correspondence address for your country found in your Agreement.

h. For Digital Wallet Application-initiated Transactions that are also Recurring Billing Charges, you must follow the process set out in Subsection 2.3.1, "Recurring Billing". The Charge Record should include indicators that the Charge is a Recurring Billing Charge and not a Digital Wallet Application-initiated Transaction.

2.3 Other Charges

2.3.1 Recurring Billing

a. Before submitting your first Recurring Billing Charge you must:

- **i.** clearly and conspicuously disclose all material terms of the offer including, if applicable, the fact that Recurring Billing Charges will continue until the option is cancelled by the Cardmember;
- **ii.** disclose details of your cancellation/refund policy, and obtain the Cardmember's consent to bill their Card and the Recurring Billing Charges terms before submitting the first Recurring Billing Charge;
- **iii.** obtain the Cardmember's name, the Card number, the Cardmember's signature (if applicable), Card expiry date, the Cardmember's billing address, and a statement confirming consent:
  - **a.** for you to charge their Card for the same or different amounts at specified or different times; and
  - **b.** that the Cardmember can withdraw such consent at any time.
- **iv.** comply with any instructions of which we may reasonably notify you; and
- **v.** notify the Cardmember that they are able to discontinue Recurring Billing Charges at any time and provide contact details for cancelling Recurring Billing Charges.

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

c. In addition to our other Chargeback rights, we may exercise Chargeback for any Charge that does not meet the requirements set forth in this Subsection 2.3.1, "Recurring Billing". We may exercise our Chargeback rights for any Charge of which you have notified the Cardmember and to which the Cardmember does not consent.

d. Before submitting any Recurring Billing Charge you must:

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

e. Before submitting any "Signature on File" Charge you must:

- **i.** obtain Authorisation; and
- **ii.** create a Charge Record with the words "Signature on File" and the appropriate electronic descriptor.

f. The cancellation of a Card constitutes immediate cancellation of that Cardmember's consent for Recurring Billing Charges. We need not notify you of such cancellation, nor will we have any liability to you arising from such cancellation. You must discontinue the Recurring Billing Charges immediately if requested to do so by a Cardmember directly, or through us or the financial institution issuing the Cardmember's Card. If a Card account is cancelled, or if a Cardmember directly (or through us or the Card issuer) withdraws consent to Recurring Billing Charges, you are responsible for arranging another form of payment (as applicable) with the Cardmember (or former Cardmember).

g. If the Agreement is terminated for any reason, then you shall at your own cost notify all Cardmembers for whom you have submitted Recurring Billing Charges of the date when you will no longer be accepting the Card. At our option you will continue to accept the Card for up to ninety (90) days after any termination takes effect.

2.3.1.1 Recurring Billing – European Economic Area

a. If you are located in the EEA, and in relation to a Card issued in the EEA, if you submit a Recurring Billing Charge for an amount which was not specified in full when the Cardmember provided consent to Recurring Billing Charges and you do not obtain the Cardmember's consent specifically in relation to the full exact amount of such Charge, we 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.

b. If notification is required prior to each varying Recurring Billing charge, you must notify the Cardmember of the amount and date of each Recurring Billing Charge:
   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.
c. You will permit us to establish a hyperlink from our website to your website (including its home page, payment page or its automatic/recurring billing page) and list your customer service contact information.

2.3.2 Delayed Delivery Charges

a. You may accept the Card for Delayed Delivery Charges. For a Delayed Delivery Charge, you must:
   i. clearly disclose your intent and obtain written consent from the Cardmember to perform a Delayed Delivery Charge before you request an Authorisation;
   ii. obtain a separate Authorisation for each of the two (2) Delayed Delivery Charges on their respective Charge dates;
   iii. clearly indicate on each Charge Record that the Charge is either for the "deposit" or for the "balance" of the Delayed Delivery Charge;
   iv. submit the Charge Record for the balance of the purchase only after the goods have been shipped or provided or services rendered;
   v. submit each Charge Record within our submission timeframes, and any in case, 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; and
   vii. treat deposits on the Card no differently than you treat deposits on all Other Payment Products.

2.3.3 Advance Payment Charges

a. Advance Payment Charge procedures are available for custom orders (e.g., orders for goods to be manufactured to a customer's specifications), entertainment / ticketing (e.g., sporting events, concerts, season tickets), tuition, room and board, and other mandatory fees (e.g., library fees) of higher educational institutions, airline tickets, vehicle rentals, rail tickets, cruise line tickets, lodging, and travel-related services (e.g., tours, guided expeditions).
b. If you offer Cardmembers the option, or require them to make Advance Payment Charges, you must:
   i. state your full cancellation and refund policies, clearly disclose your intent and obtain written consent from the Cardmember to bill the Card for an Advance Payment Charge before you request an Authorisation. The Cardmember's consent must include:
      a. his or her 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);
   ii. obtain Authorisation; and
   iii. complete a Charge Record.
c. If the Advance Payment Charge is a Card Not Present Charge, you must also:
   i. ensure that the Charge Record contains the words "Advance Payment"; and
   ii. within twenty-four (24) hours of the Charge being incurred, provide the Cardmember written confirmation (e.g., email or facsimile) of the Advance Payment Charge, the amount, the confirmation number (if applicable), a detailed description and expected delivery date of the goods and/or services to be provided (including expected arrival and departure dates, if applicable) and details of your cancellation/refund policy.

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

e. In addition to our other Chargeback rights, we may exercise Chargeback for any Advance Payment Charge that is a Disputed Charge or portion thereof if, in our sole discretion, the dispute cannot be resolved in your favour based upon unambiguous terms contained in the terms of sale to which you obtained the Cardmember's written consent.

2.3.4 Aggregated Charges

a. This Subsection 2.3.4, "Aggregated Charges" applies only to Transactions processed by your Establishments conducting business over the internet. You may process Aggregated Charges provided the following criteria are met:

i. you clearly disclose your intent and obtain consent from the Cardmember that their purchases or refunds (or both) on the Card may be aggregated and combined with other purchases or refunds (or both) before you request an Authorisation;

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

iii. obtain Authorisation of no more than the applicable limit shown in Chapter 4, "Country Specific Policies" (or Local Currency equivalent) or such other amount as notified to you;

iv. create a Charge Record for the full amount of the Aggregated Charge;

v. the amount of the Aggregated Charge must not exceed the applicable limit set forth in Chapter 4, "Country Specific Policies" (or such other amount as notified to you) or the amount for which you obtained Authorisation, whichever is lower;

vi. submit each Charge Record within our submission timeframe. A Charge will be deemed "incurred" on the date of the first purchase or refund (or both) that comprises the Aggregated Charge; and

vii. provide the Cardmember with an email containing:

a. the date, amount, and description of each individual purchase or refund (or both) that comprises the Aggregated Charge, and

b. the date and the amount of the Aggregated Charge.

2.3.5 No Show Charges

a. If we classify you in one of the following industries, you may process No Show Charges provided that the criteria set out below are met:

- lodging,
- trailer park/campground, or
- vehicle, aircraft, bicycle, boat, equipment, motor home, or motorcycle rentals.

b. The amount of any No Show Charge must not exceed:

i. the cost of the stay in the case of a lodging reservation; or

ii. the equivalent of one (1) day's rental in the case of other reservations.

c. If the Cardmember made a reservation with you and failed to show, you may process a No Show Charge if:

i. the Cardmember has guaranteed the reservation with their Card;

ii. you have recorded the Card number, its expiry date and the Cardmember's billing address;

iii. at the time of accepting the reservation you provided the Cardmember with the applicable daily rate and a reservation number or confirmation code;

iv. you held the accommodation/vehicle for the Cardmember until the published check-out/return time the day following the first day of the reservation and you did not make the accommodation/vehicle available to any other customers; and

v. you have a documented "No Show" policy, which reflects common practice in your industry and is in accordance with the prevailing law, which policy has been advised to the Cardmember at the time they made the reservation.

d. You must obtain an Authorisation for any No Show Charges prior to submitting them. If the Cardmember does not honour their reservation, you must include in the Charge Record an indicator that the Charge is a "No Show Charge".

e. Prepaid Cards may not be used to guarantee reservations.

2.4 Authorisation

a. You must obtain Authorisation for all Charges according to our Specifications, except for Charges under any applicable Floor Limit for Card Present Charges. Every Authorisation request must include the full Card account number or Token and be for the full amount of the Charge. You may create multiple Charge Records for a single purchase placed on different Cards, if you obtain full Authorisation on each Card.

b. We will have Chargeback rights for any Charge for which Authorisation is not properly obtained, or for which Authorisation was refused, or for which no approval code number was given or properly recorded. Authorisation does not guarantee that we will accept the Charge without exercising our Chargeback rights, nor is it a guarantee that the person making the Charge is the Cardmember or that you will be paid. You must not seek Authorisation on behalf of a third party.

c. Authorisation approvals are valid for seven (7) days after the original Authorisation date. Establishments must obtain a new Authorisation approval if you submit a Charge to us more than seven (7) days from the original Authorisation date, except as otherwise indicated by us. For Charges for goods or services shipped or provided more than seven (7) days after an order is placed, you must obtain Authorisation of 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. If your POS System is unable to connect to our computer authorisation system for Authorisation or we ask you to do so (i.e., a referral), you must obtain Authorisation for all Charges by calling us at our Authorisation telephone number. We reserve the right to charge you a fee for each Charge for which you request Authorisation by telephone, unless such failure to obtain Authorisation electronically is due to the unavailability or inoperability of our computer authorisation system, or unless prohibited by law.

e. If you are located outside of the EEA, we may assign you a Floor Limit. In the event that any one Charge or series of Charges made on the same day by any one Cardmember at your Establishment is equal to or greater than the Floor Limit established by us, you must, before accepting the Charge, request Authorisation by calling us at our Authorisation telephone number. We reserve the right to change your Floor Limit at any time, and will give you notice of the change and the effective date.

2.4.1 Estimated Authorisation

a. You may only obtain an Estimated Authorisation in the industries listed below. You must obtain the Cardmember's consent to such estimated amount prior to requesting the Authorisation.

b. You must submit the corresponding Charge as soon as you become aware of the full 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.

c. If the final amount of the Charge is:

   i. no greater than the amount for which you obtained Authorisation plus the applicable Estimated Authorisation percentage listed below of that amount, no further Authorisation is necessary; or

   ii. greater than the amount for which you obtained Authorisation by more than the applicable Estimated Authorisation percentage listed in the table below of that amount, you must obtain a new Authorisation. If you fail to obtain such Authorisation, or your request for such Authorisation is declined, we will have Chargeback rights for the amount in excess of the original Authorisation amount plus the applicable Estimated Authorisation percentage of that amount. For the avoidance of doubt, we will have Chargeback rights for the final amount of the Charge for reasons other than the failure to obtain an approved Authorisation.

Industry	Estimated Authorisation Percentage
Cruise Lines (Section 3.5.1)	15%
Grocery (Card Not Present)	15%
Lodging (Section 3.7.1)	15%
Rentals (Section 3.8.2)	15%
Restaurants	20%
Retail (Card Not Present)	15%
Taxicabs and Limousines	20%

2.5 Charge or Credit Records

a. For every Charge or Credit, you must create an electronically reproducible Charge Record or Credit Record at the time of purchase that complies with the Specifications or in a form approved by us containing the following information:
   i. full Card number or Token for Charge Records;
   ii. the expiry date of the Card;
   iii. the date the Charge or Credit was incurred;
   iv. your Establishment's name, address and Establishment Number;
   v. the amount of the Charge or Credit, including applicable taxes;
   vi. for Charge Records, a description of the goods and services purchased;
   vii. for Charge Records, the Authorisation approval code number; and
   viii. all other information as required from time to time by us or Applicable Law.

b. On copies of Charge Records delivered to Cardmembers, you must truncate the Card number and you must not print the Card's expiry date nor the CID. Truncated Card Number digits must be masked with replacement characters such as "x," " *," or "#," and not blank spaces or numbers;

c. You may create multiple Charge Records for a single purchase placed on different Cards, but you must not create multiple Charge Records for a single purchase to the same Card, by dividing the purchase into more than one Charge, except in the case of a Delayed Delivery Charge or where we have authorised you to do so for Charges above a certain value.

d. For Corporate Purchasing Card (CPC) Charges, you must comply with our Charge Record requirements above. In addition, you are required to capture additional Card Data on the Charge Record, and Transmission Data on the Transmissions, according to our 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;

e. You must process CPC Charges under your CPC Establishment Number.

2.5.1 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 multi-currency platform, in accordance with the Agreement, unless American Express otherwise agrees in writing or unless required by Applicable Law. 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 *Specifications* and not previously agreed to by American Express as an eligible currency on the American Express multi-currency platform, you shall immediately notify American Express in writing; and you shall, 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 *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.

2.5.1.1 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.

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 2.3.2, "Delayed Delivery Charges" and Subsection 2.3.3, "Advance Payment Charges".

2.5.1.1.1 Submitting Charges – European Economic Area

a. If you are located in the EEA, 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, 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 2.1, "In-Person Charges".

2.5.1.2 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. Establishments must submit the Credit under the Establishment Number where the Credit originated. 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 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. You must submit all Charges and Credits under the Establishment Number of the Establishment where the Charge or Credit originated. 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. 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.

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

2.5.1.3 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 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 Charge Records and Credit Records.

b. If you upgrade your system for Chip Card acceptance for Other Payment Products, you agree to comply with 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. With our prior approval, you may retain, at your expense, a Processor which (together with any of your other Covered Parties) you must ensure cooperates with us to enable your Card acceptance. You, and not American Express, are responsible and liable for any problems, errors, omissions, delays, or expenses caused by your Processor including in relation to the handling of confidential Cardmember Information; and for any fees that your Processor charges us or our Affiliates, or that we or our Affiliates incur as a result of your Processor's system for transmitting requests for Authorisations and Charge Data to us or our Affiliates; and your Processor's compliance with the Specifications. You must ensure that your Processor 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. We may bill you for any fees charged by your Processor or deduct them from our payments to you. You must notify us promptly if you change your Processor and provide us, on request, with all relevant information about your Processor.

f. 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.

2.5.1.4 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.

2.5.1.5 Submission Errors and Adjustments

a. In the event that American Express' reconciliation of Charges indicates an error (e.g., incorrect calculations, inclusion of another party's charge forms, inclusion of invalid Card Numbers), the following procedures will apply:

i. The adjustment will be calculated in the currency in which the Charges were submitted.

ii. If monies are to due American Express, American Express shall, upon presentation to you or the Establishment, as applicable, of appropriate documentation substantiating the amount due, deduct such amount from the payment due to the relevant Establishment, in American Express' discretion, for such submission.

iii. 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, or American Express will consider the statement to be conclusively settled as complete and correct in respect of such amounts. In the event monies are due to you or the Establishment, as applicable, American Express shall add the appropriate amount to payment due for said submission.

2.6 Retaining Charge and Credit Records

a. You must retain the original Charge Record or Credit Record (as applicable) and all documents and data evidencing the Transaction, including evidence of the Cardmember's consent to it, or reproducible records thereof, for the full Record Retention Period as defined in Chapter 4, "Country Specific Policies", from the later of the date you submitted the corresponding Charge or Credit to us or the date you fully delivered the goods or services to the Cardmember, or for a different retention period as required by law. If we send you a request, you must provide a copy of the Charge Record or Credit Record and other supporting documents and data to us within the Response Timeframe from the date of our request.

2.7 Disputed Charges

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

- **i.** we have Chargeback rights, prior to contacting you, if we determine we have sufficient information to substantiate the Cardmember's claim and resolve the Disputed Charge in their favour; or
- **ii.** we will contact you prior to exercising our Chargeback rights giving you the opportunity to provide a written response to the dispute.

b. The paragraph above does not apply to Charges subject to the Fraud Full Recourse Programme.

c. We will provide twenty (20) days after the date we contact you or the Chargeback to provide to us a written response containing the information we request, including the full Card account number, or in the case of Chargeback, seeking a Chargeback reversal. We have Chargeback rights (or our previous decision to exercise our Chargeback rights will remain in effect) for the amount of the Disputed Charge if, by the end of the Response Timeframe, you have not either provided the Cardmember with a full refund or provided us with the information requested.

d. If we determine, based upon the information provided by you and the Cardmember, to resolve the Disputed Charge in the Cardmember's favour, or the Cardmember is entitled to withhold payment by law, we will have Chargeback rights for that Disputed Charge, or our previous exercise of our Chargeback rights will remain in effect. If we resolve the Disputed Charge in your favour, we will take no further action (if we have not previously exercised our Chargeback rights) or we will reverse our previous exercise of our Chargeback rights.

e. The foregoing does not affect procedures under any special Chargeback programmes (such as Fraud Full Recourse Programme) that apply to you and under which you do not receive inquiries or notices regarding certain types of Charges prior to our final exercise of our Chargeback rights.

f. If we exercise our Chargeback rights with respect to a Disputed Charge that would have been avoided had our Card acceptance procedures been followed (an Avoidable Chargeback), we may charge you a fee which we will notify to you. We will provide you with a list of Avoidable Chargebacks upon request.

g. 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.

2.7.1 Disputed Charges – European Economic Area

a. If a Disputed Charge relates to a Card issued in the EEA and involves a claim that the Cardmember was not advised of the full exact amount of the Charge 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.

2.7.2 Fraud Full Recourse Programme

a. In all countries in which we operate the Fraud Full Recourse Programme (see Chapter 4, "Country Specific Policies"), we may put you onto a Fraud Full Recourse Programme for all Charges, if:

i. 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; or

ii. an Establishment experiences a disproportionately high number or amount of Disputed Charges or fraud relative to your prior history or industry standards; or

iii. you are in an industry we consider high risk.

b. In countries where Fraud Full Recourse applies (see Chapter 4, "Country Specific Policies"), we may place you in a Fraud Full Recourse Programme under which:

i. we may exercise our Chargeback rights without contacting you where a Cardmember disputes a Charge for actual or alleged fraud; and

ii. you will have no right to request a reversal of our decision to exercise our Chargeback rights.

c. We will have these rights even if we had notice of such defect at the time of payment, you have received an Authorisation and have complied with all other provisions of the Agreement.

d. We may place you in this programme upon signing, or at any time during the term of the Agreement upon notice to you.

e. For the avoidance of doubt, if you 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.

2.8 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.

2.9 Strong Customer Authentication

a. If you have Establishments in the EEA, 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 accept Charges made by Digital Orders, they should participate in our American Express SafeKey Programme.

2.10 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.

2.10.1 American Express SafeKey Fraud Liability Shift

a. Under our 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 paragraph 2.10 (d) 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.** Maintain a Fraud to Sales Ratio within the parameters contained in the relevant *SafeKey Implementation Guide*, which may be updated from time to time and is available at www.americanexpress.com/merchantspecs. 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.

AMERICAN EXPRESS

Special Regulations for Specific Industries

3

3.1 Introduction

a. This chapter sets forth additional policies and procedures applicable to Merchants classified in specific industries. If this applies to you, all other provisions and requirements of the *Merchant Regulations* will also apply to you. To the extent possible, the provisions of this Chapter 3, "Special Regulations for Specific Industries" and all the other provision of the *Merchant Regulations* shall be interpreted to give each their full effect. However, if a conflict is deemed to exist between them, then the provisions of this Chapter 3, "Special Regulations for Specific Industries" shall prevail.

3.2 Prohibited or Restricted Industries

3.2.1 Prohibited Industries

a. Your establishments are not permitted to accept the Card if they operate in any of the following Prohibited Industries. We may suspend acceptance of Cards by you or any of your Establishments or terminate the Agreement (including immediate termination without prior notice to you) if we determine or have reason to believe, in our sole discretion, that you or any of your Establishments are performing a prohibited activity or operating in a Prohibited Industry.

Prohibited Industry	Description	Industry Merchant Category Code (MCC)
Bankruptcy services	A company or agency that is in the business of recovering money owed on delinquent accounts or supporting the bankruptcy process.	—
Check cashing / guarantee	A business that provides customers with a way to turn a check into cash without having to rely on a bank account.	—
Child pornography	An individual or entity providing or associated with the visual depiction of a minor engaged in obscene or sexually explicit conduct, whether made or produced by electronic, mechanical, or other means.	—
Credit restoration	A service aimed at improving credit ratings by disputing errors and outdated claims with credit bureaus.	—
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.	—
Wire transfers in-person (not online)	A business that specialises in the transfer of money from one location to another.	4829

3.2.2 Restricted Industries

a. The following industries are restricted. In order to accept Transactions in the following industries, you will need to obtain written permission from us. We may in 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 (including immediate termination without prior notice to you) if we determine or have reason to believe, in our sole discretion, that you or any of your Establishments are performing a restricted activity or operating in a Restricted Industry without our written permission.

Restricted Industry	Description	Industry Merchant Category Code (MCC)
Bail / bail bond	Bail – A sum of money paid by a criminal defendant to be released from jail under the condition that they appear for court appearances. This does not include a bail bond fee.	9223
Cash at Point of Sale from a non-financial institution	A cash advance from a non-financial Institution.	6010 6011 6051
Charity	A non-profit, non-political organisation that collects donations, including fundraising.	8398
Condo (real estate) down payments	Down payments for purchase of a condominium.	6012 6051
Debt collection	The process of pursuing payments of debts owed by individuals and/or businesses.	7322
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 can also be called online storage or cloud storage.	4816
Door-to-door sales	Unsolicited individual (who may go from door to door) selling goods and/or services with immediate payment expected.	5963
Escort services	A business, agency or person who, for a fee, provides or offers to provide an escort.	7273
Foreign exchange	A business or financial institution that has the legal right to exchange one currency for another currency.	6051
Gambling	The wagering of money or something of value on an event with an uncertain outcome, with the primary intent of winning money or material goods. Examples include: • Betting, including lottery tickets, casino gaming chips, off-track betting, and wagers at racetracks; • Government-licensed online casinos (online gambling) • Government-licensed horse/dog racing • Government-owned and other lotteries	7800 7801 7802 7995
Investment on futures	A legal agreement to buy or sell something at a predetermined price at a specified time in the future, between parties not known to each other.	—
Leasing merchants	A business that conveys land, property, or other real estate to another for a specified time in return for regular periodic payment.	—
Licensed insolvency practitioners	A professional intermediary in insolvency procedures.	—

Restricted Industry	Description	Industry Merchant Category Code (MCC)
Marijuana-related businesses	Any individual or entity that manufactures, processes, distributes, or dispenses marijuana, or byproducts or derivatives of marijuana, whether for recreational or medicinal purposes, and whether or not subject to a governmental licensing regime.	—
Mortgage payments	A payment which includes principal and interest paid by borrower to lender of a home loan.	6012 6051
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.	5966 5967
Online adult entertainment	A business that primarily sells adult digital content via Internet Electronic Delivery.	—
Pharmacies (card not present)	A business that sells prescription drugs/products online.	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.	8651
Prostitution	A person or business providing sexual services in return for payment.	—
Telemarketing – travel related	A business that telemarkets travel related products or services or other travel arrangements.	5962
Tobacco and smokeless tobacco retailers (card not present)	A business that sells tobacco, smokeless tobacco, and e-cigarettes online.	5993
Top-Up Wallet	Functionality that provides a Stored Value Digital Facility (SVDF), 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.	6540
Travel tour operators	A business that provides travel information and booking services.	4722

Restricted Industry	Description	Industry Merchant Category Code (MCC)
Unlicensed massage parlours	A massage parlour that is not registered with a governing body.	7297
Virtual currency / cryptocurrency	Digital money not authorised or adopted by a government. Issued and controlled by its developers and used and accepted among members of a specific virtual community.	6051

3.3 Airline Merchants

3.3.1 Affiliate Carriers

a. You shall cause the Affiliate Carriers to accept Cards in accordance and in compliance with the Agreement. Transactions from Affiliate Carriers may only be submitted to American Express by you or Agents. You are responsible for settlement with each Affiliate Carrier and Agents. We will assign you unique Merchant Numbers which you, Affiliate Carriers, and Agents must use as instructed by us for submissions of Transactions. You are solely responsible for financial arrangements and for settling with each Affiliate Carrier and you are jointly and severally liable for the obligations of your Affiliate Carriers under the Agreement.

3.3.2 Charge Records

a. You must meet the requirements for Charge Records as detailed in Section 2.5, "Charge or Credit Records" and the Charge Record must clearly state: (i) Cardmember's name and passenger name (if not the Cardmember); (ii) the ticket number and the origin and destination of each flight and class code or, if not a ticket, a description of the goods or services being purchased; and (iii) airline merchant's and, if an Agent is involved, Agent's name and the location where Charge is being made.

3.3.3 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. You will have no liability if, without your knowledge, a Cardmember incorrectly identifies as having Extended Payment with American Express. You should not ask a Cardmember if he/she wishes to elect Extended Payment, but if the Cardmember indicates that Cardmember does, you will record the Cardmember's election by an entry on the Charge Record and on the Transmission, if you submit electronically.

3.3.4 In-Flight Charges

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

3.3.5 Private Charter Charges

a. For Charges for private charters (where all or most of the charter is being paid with the Card), you 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. Chargers 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). You shall not accept Prepaid Cards for private charters.

3.3.6 Submitting Transactions

a. Agents in the U.S. will submit electronically through ARC or its successor, and Agents outside the U.S. will do the same through the appropriate IATA or BSP process. Even if Establishments submit Transactions electronically, they must still complete and retain Charge Records and Credit Records. Establishments must submit all Transactions under the Establishment Number of the Establishment where that Transaction originated. You must submit Transactions to American Express in the country where the Transactions were made, or centrally, as agreed between American Express and you. Transactions from Affiliate Carriers may only be submitted to American Express by you or your Agents. You are responsible for settlement with each Affiliate Carrier and Agents. American Express will assign Carrier unique Establishment Numbers which Carrier, Affiliate Carriers, and Agents must use as instructed by American Express for submissions of Transactions.

b. Where American Express does not offer electronic submission, or where American Express agrees otherwise in advance in writing, you 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 Charge 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.

3.4 Charitable Donations

a. You represent and warrant that you are a non-profit organisation and are registered as a charity in the country.

b. 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.

3.5 Cruise Lines

a. If you operate in the cruise line industry, you may permit Cardmembers to use the Card to make purchases:

- **i.** at all cruise line ticket and sales offices worldwide including all central reservation systems (e.g., cruise ship travel, connecting air packages, air tickets, shore excursions and tours, port transfer and baggage charges, and pre- and post-cruise travel packages), and
- **ii.** for on-board purchases on cruise line ships (e.g., purchase on shipboard of cabin upgrades, entertainment, goods, beverages, laundry services, gratuities, deck chairs, spa services)

3.5.1 Onboard Charges

a. For on-board Charges, if you choose or are required by Applicable Law to obtain Cardmember signature, the Charge Record or a Folio or other Signature-on-File purchase authorisation form for Onboard Charges must be signed by the Cardmember. Notwithstanding the foregoing sentence, if prior to embarkation the Cardmember pre-registers via the internet for the applicable cruise and as a result has provided his or her electronic signature for use of the Card for on-board Charges (it being understood, for the avoidance of

doubt, that such pre-registration does not mean that a Cardmember will have completed an Internet Order or Charge at such time), then the Charge Record or Folio need not be otherwise signed, but any Transaction utilising an electronic signature shall be considered a Card Not Present Charge. We understand and agree that with respect to each Folio: (1) the Folio will be a total Charge (or portion of the total Charge if the Cardmember is also utilising an Other Payment Product per the Cardmember's request) for the entire cruise even though the same may have consisted of different individual on-board Charges through use of a cruise line card and for which the Cardmember has signed a ticket, chit, or other receipt for each such purchase (other than any additional Charges made by the Cardmember subsequent to the closing of the Cardmember's Folio account); and, so long as the foregoing terms have been followed, (2) no Cardmember signature needs to be sought by you or will be required by us during or at completion of the applicable cruise in order to process and close the applicable Charge other than the ticket, chit, or other receipt as provided in (1) above. (For purposes of clarification, we will not require you to submit to any such ticket, chit, or other receipt in order to process a Charge).

b. Special Authorisation Procedures. There may be times when you cannot obtain Authorisation for every on-board Charge made on the Card (or cruise line card, as applicable). Instead, you must:

- **i.** seek an Estimated Authorisation (see Subsection 2.4.1, "Estimated Authorisation") at embarkation or check-in (with Authorisation of any amounts in excess of such estimate to be obtained at the end of the cruise);
- **ii.** the Estimated Authorisation is valid for the duration of the stay;
- **iii.** seek Authorisation intermittently (no less than daily) through the duration of the cruise; and
- **iv.** if the POS System is unavailable to obtain an Authorisation, then you must either: obtain Authorisation by telephoning our Authorisation department, or collect all Charges during such nonfunctioning time and as soon as reasonably possible obtain an Authorisation.
- **v.** upon check-out, follow the procedures for estimated amounts in Subsection 2.4.1, "Estimated Authorisation".
- **vi.** If a Cardmember opts to use a Prepaid Card at the time of check-out when the final on-board Charge is known, you must obtain Authorisation for the full amount of the on-board Charge to be placed on the Prepaid Card.

3.5.2 Charge Records

a. You must meet the requirements for Charge Records as detailed in Section 2.5, "Charge or Credit Records" and the Charge Record must clearly state:

- **i.** Cardmember's name and passenger name (if not the Cardmember);
- **ii.** the ticket number and the origin and destination of each cruise or, if not a ticket, a description of the goods or services being purchased; and
- **iii.** your and, if an Agent is involved, Agent's name and the location where Charge is being made.

3.6 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. This 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 3.6, "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.

3.7 Lodging

3.7.1 Authorisation

a. Upon check-in,

   i. If a Cardmember wishes to use the Card to pay for a lodging stay, you must obtain an Estimated Authorisation for the full amount of the Charge (see Subsection 2.4.1, "Estimated Authorisation") based upon the room rate and the number of days that the Cardmember expects to stay, plus taxes and other known ancillary amounts, provided that you must not accept Prepaid Cards at check-in for purposes of Authorisation, guarantee, or pre-payment of the lodging stay.

   ii. The Estimated Authorisation is valid for seven (7) days from the date the Charge is incurred or seven (7) days following the conclusion of the lodging stay.

b. Upon check-out, follow the procedures for estimated amounts in Subsection 2.4.1, "Estimated Authorisation".

c. If Cardmembers opt to use Prepaid Cards at the time of check-out when the final Charge is known, you must obtain Authorisation for the full amount of Charges to be placed on the Prepaid Card.

3.7.2 Periodic Charges

a. In the case of any Cardmember who incurs Charges at one or more of your Establishments over a period of time rather than at the end of the stay, you must obtain Authorisation for each Charge before accepting each Charge. You must submit the Charge Record in accordance with this Agreement.

3.8 Motor Vehicles

3.8.1 Parking

a. If a Cardmember agrees to leave a motor vehicle with you for a specific number of days, you must submit the Charge within seven (7) days of the date of such agreement only for the amount you agreed with the Cardmember.

b. Where you provide a parking pass for a pre-determined number of days, you must submit the Charge within seven (7) days of the date of such provision only for the amount you agreed with the Cardmember.

c. Where the number of parking days is not known when the Cardmember leaves the motor vehicle with you, you shall not submit the Charge to us until the last day of parking.

3.8.2 Rental

a. When a Cardmember wishes to use the Card to rent a vehicle, ensure that the Cardmember has executed a standard rental agreement, provided a valid driving license, and met such other qualifications as the Establishment normally requires in the case of vehicle rentals and ensure that a Charge Record or rental agreement is completed. You must obtain an Estimated Authorisation for the full amount of the Charge (see Subsection 2.4.1, "Estimated Authorisation") by multiplying the rate by the rent period reserved by the Cardmember plus any known incidentals. You must not include an amount for any possible damage to or theft of the vehicle. In your rental agreement with the Cardmember, you must specify the full exact cost of the vehicle rental together with the exact cost of any additional goods or services made available 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 rent.

b. The Estimated Authorisation is valid for seven (7) days following the conclusion of the vehicle rental period set forth in the rental agreement.

c. If upon return of a rental vehicle, the vehicle has been damaged and the Cardmember has not purchased the car rental collision or loss insurance and the Cardmember voluntarily selects to use the Card to pay for property damage to a rented vehicle, you may submit a Charge, which will be submitted separately from any Charge submitted for the cost of the vehicle rental, for an estimate of the capital damages amount incurred, provided that:

- **i.** the Establishment must provide in writing, to the Cardmember, an itemised list and description of the specific damage which has occurred;
- **ii.** prior to submitting a Charge, the Establishment obtained a written, signed acknowledgement from the Cardmember of their responsibility for the capital damage, including a specific estimate of the capital damages amount and a written statement from the Cardmember that he/she wants to pay the specified capital damages with the Card (the Cardmember written statement must be made freely and without any threat or duress);
- **iii.** the Establishment must adhere to the requirements for completion of Charge Records and must obtain a separate and additional Authorisation for the estimate of the capital damages amount;
- **iv.** the original Charge for the car rental was made on the Card of the same Cardmember referred to above at the time the vehicle was checked out;
- **v.** the Charge submitted for capital damages is no greater than the estimated capital damages plus fifteen percent (15%) or, in the case of a total loss, the replacement cost of the vehicle. No amounts in excess of one hundred and fifteen percent (115%) of the disclosed amount will be charged to the Cardmember's Card, without the express prior written consent of the Cardmember.

d. You must comply with requests from the Cardmember or the Cardmember's insurance adjustor to supply documentation related to the capital damages incident.

e. You must never include the following in an Authorisation Request or in a Charge submission:

- **i.** Losses due to theft of the vehicle, or
- **ii.** Loss of revenue incurred by you due to loss of use of the rental vehicle in question.

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

g. You must not include an amount in any Charge for any damages, penalties, fines, charges, costs, or fees in addition to the Estimated Rental Charge whether or not such amounts are set out in the rental agreement unless such itemised amounts are expressly requested by the Cardmember to be charged to the Card. If you include 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 Rental Charge.

h. Upon return of the vehicle, follow the procedures for estimated amounts in Subsection 2.4.1, "Estimated Authorisation".

i. We may monitor your 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, you continue not to comply with these procedures, then we 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.

j. 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.

k. You shall not accept Prepaid Cards to reserve or pick up a rented vehicle, but you may accept Prepaid Cards for payments upon the return of vehicles when the final Charge amount is known.

3.8.3 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.

3.9 Payment Aggregators

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 Aggregator 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 Aggregator on the American Express network. As a Payment Aggregator, 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 required 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 Specifications or local network specifications.

c. Payment Aggregator cannot recruit Sponsored Merchant Prospects that fall within any of the following:

i. Any of the categories listed in Subsection 3.2.1, "Prohibited Industries" and Subsection 3.2.2, "Restricted Industries".

ii. Travel industry, including but not limited to:

- Airlines and air carriers (MCC 3000-3300, 4511)
- Car rental agencies (MCC 3351-3441, 7512)
- Lodging 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 Payment Aggregators (except to the extent the entity itself sells goods to which it has title).

d. Please contact your American Express representative to understand all your obligations as a Payment Aggregator. Failure to comply with your obligations may result in non-compliance penalties.

3.10 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 this 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.

AMERICAN EXPRESS

Country Specific Policies

4

4.1 Country Specific Policies

Country	EMV Requirements	Maximum Amount for a Contact Transaction with No CVM	Maximum Amount for a Contactless Transaction with No CVM	Aggregated Charge Limit	Record Retention Period	Fraud Full Recourse Programme Applies	Strong Customer Authentication (SCA)
Section	2.1.1 / 2.1.2	2.1.4	2.1.5	2.3.4	2.6	2.7.2	2.9
Australia	Chip Only Country	AUD 100	AUD 200	AUD 15	12 months	Y	N
Austria	Chip and PIN Country	EUR 0[1]	EUR 50	EUR 15	18 months	N	Y
Belgium / Luxembourg	Chip and PIN Country	EUR 0[1]	EUR 50	EUR 15	18 months	Y	Y
Finland	Chip and PIN Country	EUR 0[1]	EUR 50	EUR 10	18 months	Y	Y
France	Chip and PIN Country	EUR 0[1]	EUR 50	EUR 15	18 months	Y	Y
Germany	Chip and PIN Country	EUR 0[1]	EUR 50	EUR 15	18 months	N	Y
Hong Kong (Special Administrative Region of China)	Chip Only Country	HKD 1,000	HKD 1,000	USD 15	12 months	Y	N
Italy	Chip and PIN Country	EUR 0[1]	EUR 50	EUR 15	18 months	Y	Y
Japan	Chip Only Country	JPY 10,000	JPY 10,000	JPY 1,200	12 months	N	N
Mexico	Chip Only Country	MXN 400	MXN 1,500	USD 15	12 months	Y	N
Netherlands	Chip and PIN Country	EUR 0[1]	EUR 50	EUR 15	18 months	Y	Y
New Zealand	Chip Only Country	NZD 100	NZD 200	USD 15	12 months	Y	N
Singapore	Chip Only Country	SGD 200	SGD 200	USD 15	12 months	Y	N
Spain	Chip and PIN Country	EUR 0[1]	EUR 50	EUR 15	18 months	Y	Y
Sweden	Chip and PIN Country	SEK 0[1]	SEK 400	SEK 100	18 months	Y	Y
Taiwan (Province of China)	Non-Chip Country	TWD 3,000	TWD 3,000	USD 15	12 months	Y	N
Thailand	Non-Chip Country	THB 500	THB 500	USD 15	12 months	Y	N
United Kingdom	Chip and PIN Country	GBP 0[1]	GBP 45	GBP 10	18 months	Y	Y

[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.

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.

Advance Payment Charge

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.

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 Charge

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

Agreement

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

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 this Agreement.

American Express SafeKey Programme

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

American Express Technical Specifications

See “Specifications” (including but not limited to the *American Express Global Credit Authorization Guide*, *Global Financial Submission Guide*, *BIN Range Specifications*, *Global Sponsored Merchant File*, and *Secure File Transfer Protocol Quick Reference Guide*) which we may update from time to time.

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, judgment, 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.

Authorisation

The process for obtaining approval for a Charge, as described in this 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.

Avoidable Chargeback

A Disputed Charge that would have been avoided had our Card acceptance procedures been followed.

Buyer Initiated Payment (BIP) Transactions

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

Cardholder Data

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

Cardholder Verification Method (CVM)

An American Express 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 Information

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

Card Company

Us, our Affiliates and licensees that issue the Card.

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.

Carrier Affiliate Group

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. Each member of the Carrier Affiliate Group will be referred to as an Affiliate Carrier and it is understood and agreed that the Affiliate Carriers are regional or small carriers that meet the definition of Carrier Affiliate Group.

Chargeback

When used as a verb, means our right to: (i) reimbursement from you for the amount of a Charge which we have paid to you, or (ii) reverse 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.

Charge

A payment or purchase made using a Card.

Charge Data / Credit Data

One or more of the data elements listed in Section 2.5, "Charge or Credit Records".

Charge Record

A record of a Charge that contains Charge Data and complies with our requirements. This is sometimes referred to as Record of Charge or ROC in our materials.

Chip

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

Chip and PIN Transaction

A Chip Card Charge authenticated by a PIN.

Chip and PIN Country

A Country where Transactions must be processed on a Chip Card and authenticated by a PIN.
See Chapter 4, "Country Specific Policies".

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-Enabled Device

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

Chip Only Country

A country where Transactions must be processed with a Chip Card and do not need to be authenticated by a PIN.

Compromised Card Number

An American Express Card account number related to a Data Incident.

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.

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.

Customer Activated Terminal (CAT)

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

Data Incident

An incident involving the compromise or suspected compromise of American Express Encryption Keys, or at least one American Express Card account number in which there is:

- unauthorised access or use of Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) that are stored, processed, or transmitted on your equipment, systems, and/or networks (or the components thereof) of yours or the use of which you mandate;
- use of such Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) other than in accordance with the Agreement; and/or

- suspected or confirmed loss, theft, or misappropriation by any means of any media, materials, records, or information containing such Encryption Keys, Cardholder Data, or Sensitive Authentication Data (a combination of each).

Data Incident Event Window

The period that begins as of the date of compromise, if known, or 365 days prior to the Notification Date if the actual date of compromise is not known. The Data Incident Event Window ends 30 days after the Notification Date.

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.

Delayed Delivery Charge

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

Digital Delivery Transaction

The purchase of goods or services online or digitally and digitally delivered (e.g., images, apps or software downloads). Sometimes called "Internet Electronic Delivery Transaction" in our materials.

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.

Discount

An amount that we charge for accepting the Card as set out in your Application or elsewhere in this 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.

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.

Encryption Key or American Express Encryption Key

All keys used in the processing, generation, loading and/or protection of Account Data. This includes, but is not limited to, the following:

- Key Encrypting Keys: Zone Master Keys (ZMKs) and Zone PIN Keys (ZPKs)
- Master Keys used in secure cryptographic devices: Local Master Keys (LMKs)
- Card Security Code Keys (CSCKs)
- PIN Keys: Base Derivation Keys (BDKs), PIN Encryption Key (PEKs), and ZPKs

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 from the final submission amount.

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.

Folio

A purchase authorisation form generated by a cruise line merchant which itemises goods and services purchased by a customer that are sold onboard the cruise line merchant's ships, by shops onboard ships operated by the cruise line merchant, or by shipboard shops operated by others where the cruise line merchant is the merchant of record.

Franchisee

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

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.

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.

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*.

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.

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 Originated Payment (IOP) Transactions
A Transaction initiated by Cardmembers, using a payment solution provided by their Issuer to send funds to pay Service Establishments.

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

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 this Agreement.

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

Merchant-Presented Quick Response (MPQR)
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.

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.

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

Other Agreement
Any agreement, other than this 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 Aggregator
An entity whose business model provides that it accepts the Card on behalf of third parties (Sponsored Merchants). Formerly referred to as "Payment Service Provider" or "PSP" and sometimes called an "aggregator" or "master merchant" in our materials.

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

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

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

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

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

Personal Information

Information about an individual that is collected or held by you in the course of performing this 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.

Point-to-Point Encryption (P2PE)

A solution that cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption.

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 Charge 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.

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

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.

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

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.

Signature On File
The storage of Cardmember Information by you or on your behalf in support of billing services, including, but not limited to, Recurring Billing Charges.

Specifications
The set of mandatory, conditional, and optional requirements related to connectivity to the American Express network and electronic Transaction processing, including Authorisation and submission of Transactions, either available at www.americanexpress.com/merchantspecs or upon request from your American Express representative, and which we may update from time to time. Sometimes called "American Express Technical Specifications" or "Technical Specifications" in our materials.

Sponsored Merchant
A Sponsored Merchant Prospect that has entered into a Sponsored Merchant Agreement with a Payment Aggregator.

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

Any third-party seller of goods and services that either: (i) does not accept the Card and which operates one or more Sponsored Merchant websites or other Establishments, or (ii) accepts the Card with respect to its existing methods for selling goods and services but also proposes to submit Transactions through a Payment Aggregator and/or (iii) meets any other criteria specified by American Express from time to time.

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.

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.

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.

Transaction

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

Validation Documentation

The AOC rendered in connection with an Annual Onsite Security Assessment or SAQ, the AOSC and executive summaries of findings rendered in connection with Quarterly Network Scans, or the Annual STEP Attestation.

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 this Agreement and its Affiliates conducting business in the same industry.

AMERICAN EXPRESS

Appendix A: Data Security Operating Policy (DSOP)

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, 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.

Section 1 Standards for Protection of Encryption Keys, Cardholder Data, and Sensitive Authentication Data

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

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

You must protect all 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 4, "Important Periodic Validation of Your Systems", except as otherwise provided in that section).

Section 2 Data Incident Management Obligations

You must notify American Express immediately and in no case later than twenty-four (24) hours after discovery of a Data Incident.

To notify American Express, contact the American Express Enterprise Incident Response Programme (*EIRP*) at +1 (602) 537-3021 (+ indicates International Direct Dial "IDD" prefix, International toll applies), 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 forensic investigation of each Data Incident.
- For Data Incidents involving 10,000 or more unique Card Numbers, you must engage a PCI Forensic Investigator (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.
- You must promptly provide to American Express all Compromised Card Numbers. American Express reserves the right to conduct its own internal analysis to identify Card Numbers involved in the Data Incident.

Forensic investigation reports must be completed using the current Forensic Incident Final Report Template available from PCI. Such report must include forensic reviews, reports on compliance, and all other information related to the Data Incident; identify the cause of the Data Incident; confirm whether or not you were in compliance with the PCI DSS at the time of the Data Incident; and verify your ability to prevent future Data Incidents by (i) providing a plan for remediating all PCI DSS deficiencies, and (ii) participating in the American Express compliance programme (as described below). Upon 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 2, "Data Incident Management Obligations":

- American Express may, in its sole discretion, require you to engage a PFI to conduct an investigation of a Data Incident for Data Incidents involving less than 10,000 unique Card Numbers. Any such investigation must comply with the requirements set forth above in this Section 2, "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 agree to work with American Express to rectify any issues arising from the Data Incident, including consulting with American Express about your communications to Cardmembers affected by the Data Incident and 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.

Section 3 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 3, "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 3, "Indemnity Obligations for a Data Incident".

For Data Incidents that involve:

- 10,000 or more American Express Card Numbers with either of the following:
  - Sensitive Authentication Data, or
  - Expiration Date

  you shall compensate American Express at the rate of $5 USD per account number.

However, American Express will not seek indemnification from you for a Data Incident that involves:

- less 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 this Section 3, "Indemnity Obligations for a Data Incident",
  - 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 3, "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 $100,000 USD 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 2, "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 $100,000 USD.

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.

Merchants' 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:

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 below illustrate the calculation of the indemnity reduction.
- To qualify as a Risk-Mitigating Technology, you must demonstrate effective utilisation of the technology in accordance with its design and intended purpose. For example, deploying Chip Enabled Devices and processing Chip Cards as Magnetic Stripe or Key Entered Transactions, is NOT an effective use of this technology.
- 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.

Ex.	Risk- Mitigating Technologies in use	Enhanced Indemnity Obligation Reduction 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 $5 USD per account number (10,000 x $5 = $50,000 USD) may be eligible for a reduction of 50%, reducing the Indemnity Obligations from $50,000 USD to $25,000 USD, excluding any non-compliance fees.

Section 4 Important Periodic Validation of Your Systems

You must take the following actions to validate under PCI DSS annually and quarterly 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' compliance programme under this policy.

Action 2: Understand your Level and Validation 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 American Express' PCI Compliance Programme under this policy by providing the full name, email address, telephone number, and physical mailing address of an individual who will serve as their data security contact. You must submit this information to SecureTrust, a division of Trustwave (https://portal.securetrust.com), which administers the programme on behalf of American Express, by one of the methods listed in Action 4: "Send the Validation Documentation to American Express" below. You must notify SecureTrust if this information changes,

providing updated information where applicable. Your failure to provide such contact information will not affect our rights to assess fees for non-validation as outlined in the Non-Validation Fee Table.

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

Action 2: Understand your Level and Validation Requirements

There are four 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.* You will fall into one of the Levels specified in the Merchant and Service Provider tables below. Buyer Initiated Payments (BIP) Transactions are not included in the volume of American Express Card Transactions to determine Merchant Level and validation requirements.

* 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.

Merchant Requirements

Merchants (not Service Providers) have four possible classifications regarding their level and validation requirements. After determining the Merchant level from the list below, see the Merchant Table to determine validation documentation requirements.

- **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 2.5 million American Express Card Transactions per year.
- **Level 3 Merchant** – 10,000 to 50,000 American Express Card Transactions per year.
- **Level 4 Merchant** – Less than 10,000 American Express Card Transactions per year.

Merchant Table

	Validation Documentation		
Merchant Level/ Annual American Express Transactions	Onsite Assessment Report on compliance (ROC)	Self Assessment Questionnaire (SAQ) AND quarterly network scan	STEP Attestation for eligible Merchants
Level 1/ 2.5 million or more	Mandatory	Not applicable	Optional (replaces ROC)
Level 2/ 50,000 to 2.5 million	Optional	SAQ mandatory (unless submitting an Onsite Assessment); scan mandatory with certain SAQ types	Optional (replaces SAQ and network scan or ROC)
Level 3/ 10,000 to 50,000	Optional	SAQ optional (mandatory if required by American Express); scan mandatory with certain SAQ types	Optional (replaces SAQ and network scan or ROC)
Level 4/ 10,000 or less	Optional	SAQ optional (mandatory if required by American Express); scan mandatory with certain SAQ types	Optional (replaces SAQ and network scan or ROC)

* 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 accuracy and appropriateness of the PCI validation documentation provided as needed, including by engaging, at American Express' expense, a QSA or PFI of our choice.

Security Technology Enhancement Programme (STEP)

Merchants that are compliant with PCI DSS may also, 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:

- **EMV** – on an active Chip-Enabled Device having a valid and current EMVCo (www.emvco.com) approval/ certification and capable of processing AEIPS compliant Chip Card Transactions. (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

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.

Service Provider Requirements

Service Providers (not Merchants) have two possible classifications regarding their level and validation requirements. After determining the Service Provider level from the list below, see the Service Provider Table to determine validation documentation requirements.

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 – less than 2.5 million American Express Card Transactions per year; or any Service Provider not deemed Level 1 by American Express.

Service Providers are not eligible for STEP.

Service Provider Table

Level	Validation Documentation	Requirement
1	Annual Onsite Security Assessment Report on Compliance	Mandatory
2	Annual SAQ D (Service Provider) and Quarterly Network Scan or Annual Onsite Security Assessment Report on Compliance, if preferred.	Mandatory

It is recommended that Service Providers also comply with the PCI Designated Entities Supplemental Validation.

Action 3: Complete the Validation Documentation that you must send to American Express

The following documents are required for different levels of Merchant and Service Provider as listed in the Merchant Table and Service Provider Table above.

Annual Onsite Security Assessment – The Annual Onsite Security Assessment is a detailed onsite examination of your equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed, or transmitted. It must be performed by:

- a QSA, or

- you and attested to by your chief executive officer, chief financial officer, chief information security officer, or principal and submitted annually to American Express on the applicable Attestation of Compliance (AOC).

The AOC must support compliance with all requirements of the PCI DSS and, upon request, include copies of the full report on compliance (Level 1 Merchants and Level 1 Service Providers).

Annual Self-Assessment Questionnaire – The Annual Self-Assessment is a process using the PCI DSS SAQ that allows self-examination of your equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed, or transmitted. It must be performed by you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal. The AOC section of the SAQ must be submitted annually to American Express. The AOC section of the SAQ must certify your compliance with all requirements of the PCI DSS and include full copies of the SAQ on request (Level 2, Level 3, and Level 4 Merchants; Level 2 Service Providers).

Quarterly Network Scan – The Quarterly Network Scan is a process that remotely tests your Internet-connected computer networks and web servers for potential weaknesses and vulnerabilities. It must be performed by an Approved Scanning Vendor (**ASV**). You must complete and submit the ASV Scan Report Attestation of Scan Compliance (**AOSC**) or the executive summary of findings of the scan (and copies of the full scan, on request), quarterly to American Express. The AOSC or executive summary must certify that the results satisfy the PCI DSS scanning procedures, that no high risk issues are identified, and that the scan is passing or compliant (all Merchants except those who also submit an Onsite Security Assessment Report, STEP-eligible Merchants and all Service Providers). For the avoidance of doubt, Quarterly Network Scans are mandatory if required by the applicable SAQ.

Annual STEP Attestation Validation Documentation – The American Express Annual STEP Qualification Attestation ("STEP Attestation") is available only to merchants who meet the criteria listed in Action 2: "Understand your Level and Validation Requirements" above. The STEP Attestation involves a process using PCI DSS requirements that allows self-examination of your equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed, or transmitted. It must be performed by you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal. You must complete the process by submitting the STEP Attestation form annually to American Express. (STEP- eligible Merchants only). The Annual STEP Attestation form is available for download via SecureTrust's secure portal.

Summary of Compliance – The SOC is a document by which a Franchisor or Service Provider may report the PCI Compliance status of its franchisees. The SOC template is available for download via SecureTrust's secure portal.

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

- an Attestation of Compliance (AOC) including "Part 4. Action Plan for Non-Compliant Status"
- a PCI Prioritised Approach Tool Summary and Attestation of Compliance (PASAOC)
- a Project Plan Template (available for download via SecureTrust's secure portal)

Each of the above documents must designate a remediation date, not to exceed 12 months following the document completion date in order to achieve compliance. You must submit the appropriate document to American Express by one of the methods listed in Action 4: "Send the Validation Documentation to American Express" below. 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). For the avoidance of all doubt, Merchants that are not compliant with PCI DSS are not eligible for STEP. American Express shall not impose non-validation fees (described below) on you for non-compliance prior to the remediation date, but you remain liable to American Express for all indemnity obligations for a Data Incident and are subject to all other provisions of this policy.

Action 4: Send the Validation Documentation to American Express

All Merchants and Service Providers required to participate in the American Express PCI Compliance Programme must submit the Validation Documentation marked "mandatory" in the tables in Action 2: "Understand your Level and Validation Requirements". You must submit your Validation Documentation to SecureTrust by one of these methods:

- **Secure Portal**: Validation Documentation may be uploaded via SecureTrust's secure portal at https://portal.securetrust.com.

  Please contact SecureTrust at the phone number for your Country or via email at americanexpresscompliance@securetrust.com for instructions on using this portal.
- **Secure Fax**: Validation Documentation may be faxed to: +1 (312) 276-4019. (+ indicates International Direct Dial "IDD" prefix, International toll applies).

  Please include your name, DBA (Doing Business As) name, the name of your data security contact, your address and phone number, and, for Merchants only, your 10-digit American Express Merchant number.

If you have general questions about the programme or the process above, please contact SecureTrust at + 800 9000 1140 or +1 (312) 267-3208 or via email at americanexpresscompliance@securetrust.com.

Compliance and validation are completed at your expense. By submitting Validation Documentation, you represent and warrant to American Express that 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.

Markets	SecureTrust Phone Number
Argentina	+ 800 9000 1140
Australia	+ 800 9000 1140
Austria	+ 800 9000 1140
Bulgaria	+ 312 267 3208
Canada	1 866 659 9016
Croatia	+ 312 267 3208
Cyprus	+ 800 9000 1140
Czech Republic	+ 800 144 316
Denmark	+ 800 9000 1140
Estonia	+ 312 267 3208
France	+ 800 9000 1140
Germany	+ 800 9000 1140
Greece	+ 312 267 3208
Hong Kong	+ 800 9000 1140
Hungary	+ 800 9000 1140
Iceland	+ 800 9000 1140
IDC	+ 888 900 0114

Markets	SecureTrust Phone Number
Latvia	+ 312 267 3208
Lithuania	+ 312 267 3208
Malta	+ 312 267 3208
Mexico	+ 888 900 0114
Netherlands	+ 312 267 3208
New Zealand	+ 800 9000 1140
Norway	+ 800 9000 1140
Poland	+ 800 9000 1140
Portugal	+ 312 267 3208
Romania	+ 312 267 3208
Russian	+ 312 267 3208
Singapore	+ 800 9000 1140
Slovakia	+ 312 267 3208
Slovenia	+ 312 267 3208
Spain	+ 800 9000 1140
Sweden	+ 800 9000 1140
Taiwan	+ 312 267 3208

Markets	SecureTrust Phone Number
India	+ 800 9000 1140
Ireland	+ 800 9000 1140
Italy	+ 800 9000 1140
Japan	+ 312 267 3208

Markets	SecureTrust Phone Number
Thailand	+ 800 9000 1140
United Kingdom	+ 800 9000 1140
United States	1 866 659 9016

+ indicates International Direct Dial "IDD" prefix, International toll applies

Non-Validation Fees and Termination of Agreement

American Express has the right to impose non-validation fees on you and terminate the Agreement if you do not fulfil these requirements or fail to provide the mandatory Validation Documentation to American Express by the applicable deadline. American Express will notify you separately of the applicable deadline for each annual and quarterly reporting period.

Send documentation to American Express by the applicable deadline. American Express will notify you separately of the applicable deadline for each annual and quarterly reporting period. See Non-Validation Fee table below for fees applicable to your Country.

Description	Level 1 Merchant or Level 1 Service Provider	Level 2 Merchant, Level 2 Service Provider, or STEP Merchant	Level 3 or Level 4 Merchant
A non-validation fee will be assessed if the Validation Documentation is not received by the first deadline.	1st Month Fee for Level 1	1st Month Fee for Level 2	Monthly Fee
An additional non-validation fee will be assessed if the Validation Documentation is not received within 30 days of the first deadline.	2nd Month Fee for Level 1	2nd Month Fee for Level 2	
An additional non-validation fee will be assessed if the Validation Documentation is not received within 60 days of the first deadline.	3rd Month Fee for Level 1	3rd Month Fee for Level 3	

If American Express does not receive your mandatory Validation Documentation within 60 days of the first deadline, then American Express has the right to terminate the Agreement in accordance with its terms as well as impose the foregoing non-validation fees cumulatively on you.

Non-Validation Fee Table

Market	Level	Type	Currency	1st Month Fee	2nd Month Fee	3rd Month Fee
Australia	Level 1	Merchant or Service Provider	AUD	35,000	49,000	63,000
	Level 2	Merchant or Service Provider	AUD	7,000	14,000	21,000
	Level 3 & Level 4	Merchant	AUD	Monthly Fee: 20		
Bulgaria	Level 1	Merchant or Service Provider	BGN	28,000	40,000	51,000
	Level 2	Merchant or Service Provider	BGN	5,500	11,000	16,500
	Level 3 & Level 4	Merchant	BGN	Monthly Fee: 33		
Croatia	Level 1	Merchant or Service Provider	HRK	105,000	152,000	195,000
	Level 2	Merchant or Service Provider	HRK	21,000	42,000	63,000
	Level 3 & Level 4	Merchant	HRK	Monthly Fee: 130		
Cyprus, Estonia, France, Germany, Ireland, Spain, Latvia, Lithuania, Portugal, Slovakia, Slovenia	Level 1	Merchant or Service Provider	EUR	19,000	26,000	34,000
	Level 2	Merchant or Service Provider	EUR	4,000	7,500	11,000
	Level 3 & Level 4	Merchant	EUR	Monthly Fee: 15		
Czech Republic	Level 1	Merchant or Service Provider	CZK	392,000	564,000	721,000
	Level 2	Merchant or Service Provider	CZK	78,300	157,000	235,000
	Level 3 & Level 4	Merchant	CZK	Monthly Fee: 440		
Denmark	Level 1	Merchant or Service Provider	DKK	110,000	156,000	200,000
	Level 2	Merchant or Service Provider	DKK	22,000	42,000	65,000
	Level 3 & Level 4	Merchant	DKK	Monthly Fee: 130		

Market	Level	Type	Currency	1st Month Fee	2nd Month Fee	3rd Month Fee
Hong Kong	Level 1	Merchant or Service Provider	HKD	25,000	35,000	45,000
	Level 2	Merchant or Service Provider	HKD	5,000	10,000	15,000
	Level 3 & Level 4	Merchant	HKD	Monthly Fee: 150		
Hungary	Level 1	Merchant or Service Provider	HUF	4,650,000	6,700,000	8,600,000
	Level 2	Merchant or Service Provider	HUF	930,000	1,860,000	2,800,000
	Level 3 & Level 4	Merchant	HUF	Monthly Fee: 5,500		
Iceland	Level 1	Merchant or Service Provider	ISK	3,070,000	4,300,000	5,500,000
	Level 2	Merchant or Service Provider	ISK	615,000	920,000	1,227,200
	Level 3 & Level 4	Merchant	ISK	Monthly Fee: 2,400		
New Zealand	Level 1	Merchant or Service Provider	NZD	35,000	49,000	63,000
	Level 2	Merchant or Service Provider	NZD	7,000	14,000	21,000
	Level 3 & Level 4	Merchant	NZD	Monthly Fee: 20		
Norway	Level 1	Merchant or Service Provider	NOK	135,000	195,000	249,000
	Level 2	Merchant or Service Provider	NOK	27,000	54,000	81,000
	Level 3 & Level 4	Merchant	NOK	Monthly Fee: 170		
Singapore	Level 1	Merchant or Service Provider	SGD	38,000	53,000	68,000
	Level 2	Merchant or Service Provider	SGD	7,500	15,000	22,500
	Level 3 & Level 4	Merchant	SGD	Monthly Fee: 25		

Market	Level	Type	Currency	1st Month Fee	2nd Month Fee	3rd Month Fee
Sweden	Level 1	Merchant or Service Provider	SEK	175,000	245,000	315,000
	Level 2	Merchant or Service Provider	SEK	35,000	70,000	105,000
	Level 3 & Level 4	Merchant	SEK	Monthly Fee: 135		
United Kingdom	Level 1	Merchant or Service Provider	GBP	12,500	18,000	23,000
	Level 2	Merchant or Service Provider	GBP	2,500	5,000	7,500
	Level 3 & Level 4	Merchant	GBP	Monthly Fee: 15		

Section 5 Confidentiality

American Express shall take reasonable measures to keep (and cause its agents and subcontractors, including SecureTrust, 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 6 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.

Useful Websites

American Express Data Security: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

Glossary

For purposes of this Data Security Operating Policy (DSOP) only, the following definitions apply and control in the event of a conflict with the terms found in the *Merchant Regulations*.

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.

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.

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

Cardholder Data has the meaning given to it in the then current Glossary of Terms for the PCI DSS.

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).

Charge means a payment or purchase made on a Card.

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.

Covered Parties means 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 Cardmember Information 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.

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;
- 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 period that begins as of the date of compromise, if known, or 365 days prior to the Notification Date if the actual date of compromise is not known. The Data Incident Event Window ends 30 days after the Notification Date.

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

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 2.5 million American Express Card Transactions per year.

Level 3 Merchant means a Merchant with 10,000 to 50,000 American Express Card Transactions per year.

Level 4 Merchant means a Merchant with less 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 less 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.

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 Payment Card Industry Payment Application 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.

Processor means a service provider to Merchants who facilitate authorisation and submission processing to the American Express network.

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: EMV, Point-to-Point Encryption, and tokenisation.

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

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.

Summary of Compliance (SOC) means a PCI validation document used by a Franchisor or Service Provider to indicate the PCI compliance status of its affected franchisees.

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

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

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.