Appendix B
American Express Merchant Operating Guide

American Express OptBlue℠ Program

Merchant Operating Guide

1 INTRODUCTION

1.1 About the Merchant Operating Guide

For the purpose of the Merchant Operating Guide, ***our*** and ***us*** mean American Express Travel Related Services Company, Inc.; ***Merchant Agreement*** means a Merchant Processing Agreement or Sponsored Merchant Agreement, as applicable; and ***Program Merchant***, **Sponsored Merchant**, and ***Merchant*** means the individual or Entity accepting the Card under an Agreement.

The Merchant Operating Guide sets forth the policies and procedures governing each Merchant's acceptance of Cards under the Program. Participant shall ensure that (a) the Merchant Operating Guide is incorporated into all Merchant Processing Agreements and Sponsored Merchant Agreements governing a Merchant's acceptance of Cards under the Program; and (b) each Merchant complies with the Merchant Operating Guide.

1.2 Changes in the Merchant Operating Guide

American Express reserves the right to make changes to the Merchant Operating Guide in accordance with Section 1.3 of the Operating Regulations. Participant must implement such changes in all new and existing Merchant Processing Agreements and Sponsored Merchant Agreements by the earlier of (a) the date required by American Express in the update and (b) the next scheduled update that Participant (or, if applicable, a Participant Sales Entity) makes to its Merchant Processing Agreements and Sponsored Merchant Agreements.

1.3 Construct of the Merchant Operating Guide

The Merchant Operating Guide is divided into two categories. The flow-down requirements in **Exhibit B-1 to this Appendix B** must be incorporated verbatim into each Merchant Processing Agreement and Sponsored Merchant Agreement. The flow-down requirements in **Exhibit B-2 to this Appendix B** must be incorporated substantively in each Merchant Processing Agreement and Sponsored Merchant Agreement, but Participant has discretion as to exactly how they are incorporated.

Exhibit B-1 to Appendix B

Verbatim Flow-Down Requirements

The following provisions are required and must be incorporated verbatim into each Merchant Processing Agreement and Sponsored Merchant Agreement that governs a Program Merchant's acceptance of Cards, except as noted otherwise in the drafting notes below.

Drafting Notes

With respect to capitalized terms that are used but not defined in the verbatim requirements below, Participant must either (a) include definitions that are substantively similar to the definitions in the Operating Regulations or (b) modify the requirements to incorporate the substance of the corresponding definitions in the Operating Regulations.

References to "Participant" or "Merchant Services Provider" should be changed in each Merchant Processing Agreement and Sponsored Merchant Agreement to whatever term Participant uses to refer to itself or the Participant Sales Entity that is a party to such Merchant Processing Agreement and Sponsored Merchant Agreement, as applicable.

References to "Merchant" should be changed in each Merchant Processing Agreement and Sponsored Merchant Agreement to whatever term Participant or the Participant Sales Entity uses to refer to a Program Merchant or Sponsored Merchant that is a party to such Merchant Processing Agreement and Sponsored Merchant Agreement, as applicable.

Verbatim Flow-Down Requirements

- **Card Acceptance**

  Merchant must accept the Card as payment for goods and services (other than those goods and services prohibited under Section **[XX]**) sold, or (if applicable) for charitable contributions made, at all of its Establishments, except as expressly permitted by state statute. Merchant is jointly and severally liable for the obligations of Merchant's Establishments under the Merchant Agreement. **[Drafting Note: The section reference above should reference the section in the Merchant Agreement that lists the prohibited uses of the Card set forth in Section 3.3 of the Merchant Operating Guide.]**

- **Dispute Resolution**

  XX. ARBITRATION AGREEMENT (as to Claims involving American Express)

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

  If arbitration is chosen by any party, neither Merchant nor Merchant Services Provider nor American Express will have the right to litigate that Claim in court or have a jury trial on that Claim. Further, Merchant, Merchant Services Provider, and

American Express will not have the right to participate in a representative capacity or as a member of any class pertaining or be a named party to a class-action with respect to any Claim for which any party elects arbitration. Arbitration procedures are generally simpler than the rules that apply in court, and discovery is more limited. The arbitrator's decisions are as enforceable as any court order and are subject to very limited review by a court. Except as set forth below, the arbitrator's decision will be final and binding. Other rights Merchant, Merchant Services Provider, or American Express would have in court may also not be available in arbitration.

i. Initiation of Arbitration. Claims will be referred to either JAMS or AAA, as selected by the party electing arbitration. Claims will be resolved pursuant to this Arbitration Agreement and the selected organization's rules in effect when the Claim is filed, except where those rules conflict with the Merchant Agreement. Contact JAMS or AAA to begin an arbitration or for other information. Claims may be referred to another arbitration organization if all parties agree in writing, or to an arbitrator appointed pursuant to section 5 of the Federal Arbitration Act, 9 U.S.C. §§ 1-16 (*FAA*). Any arbitration hearing that Merchant attends shall take place in New York, New York unless all parties agree to an alternate venue.

ii. Limitations on Arbitration. **If any party elects to resolve a Claim by arbitration, that Claim will be arbitrated on an individual basis. There will be no right or authority for any Claims to be arbitrated on a class action basis or on bases involving Claims brought in a purported representative capacity on behalf of the general public, other merchants or other persons or entities similarly situated.** The arbitrator's authority is limited to Claims between Merchant, Merchant Services Provider, and American Express. Claims may not be joined or consolidated unless all parties to this agreement agree in writing. An arbitration award and any judgment confirming it will apply only to the specific case brought by Merchant, Merchant Services Provider or American Express and cannot be used in any other case except to enforce the award as between Merchant, Merchant Services Provider and American Express. This prohibition is intended to, and does, preclude Merchant from participating in any action by any trade association or other organization against American Express. Notwithstanding any other provision and without waiving the right to appeal such decision, if any portion of these *Limitations on Arbitration* is deemed invalid or unenforceable, then the entire Arbitration provision (other than this sentence) will not apply.

iii. Previously Filed Claims/No Waiver. Merchant, Merchant Services Provider, or American Express may elect to arbitrate any Claim that has been filed in court at any time before trial has begun or final judgment has been entered on the Claim. Merchant, Merchant Services Provider, or American Express may choose to delay enforcing or to not exercise rights under this arbitration provision, including the right to elect to arbitrate a Claim, without waiving the right to exercise or enforce those rights on any other occasion. For the avoidance of any confusion, and not to limit its scope, this section applies to any class-action lawsuit relating to the "Honor All Cards," "non-discrimination," or "no steering" provisions of the American Express Merchant Regulations, or any similar provisions of any prior American Express Card acceptance agreement, that was filed against American Express prior to the effective date of the Merchant Agreement.

iv. Arbitrator's Authority. The arbitrator shall have the power and authority to award any relief that would have been available in court, including equitable relief (e.g., injunction, specific performance) and cumulative with all other remedies, shall grant specific performance whenever possible. The arbitrator shall have no power or authority to alter

the Merchant Agreement or any of its separate provisions, including this section, nor to determine any matter or make any award except as provided in this section.

v. Split Proceedings for Equitable Relief. Merchant, Merchant Services Provider, or American Express may seek equitable relief in aid of arbitration prior to arbitration on the merits to preserve the status quo pending completion of such process. This section shall be enforced by any court of competent jurisdiction, and the party seeking enforcement shall be entitled to an award of all reasonable attorneys' fees and costs, including legal fees, to be paid by the party against whom enforcement is ordered.

vi. Small Claims. American Express shall not elect to use arbitration under this section for any Claim Merchant properly files in a small claims court so long as the Claim seeks individual relief only and is pending only in that court.

vii. Governing Law/Arbitration Procedures/Entry of Judgment. This arbitration section is made pursuant to a transaction involving interstate commerce and is governed by the FAA. The arbitrator shall apply New York law and applicable statutes of limitations and shall honor claims of privilege recognized by law. The arbitrator shall apply the rules of the arbitration organization selected, as applicable to matters relating to evidence and discovery, not the federal or any state rules of civil procedure or rules of evidence, provided that any party may request that the arbitrator to expand the scope of discovery by doing so in writing and copying any other parties, who shall have fifteen (15) days to make objections, and the arbitrator shall notify the parties of his/her decision within twenty (20) days of any objecting party's submission. If a Claim is for $10,000 or less, Merchant or American Express may choose whether the arbitration will be conducted solely on the basis of documents submitted to the arbitrator, through a telephonic hearing, or by an in-person hearing as established by the rules of the selected arbitration organization. At the timely request of a party, the arbitrator shall provide a written and reasoned opinion explaining his/her award. The arbitrator's decision shall be final and binding, except for any rights of appeal provided by the FAA. If a Claim is for $100,000 or more, or includes a request for injunctive relief, (a) any party to this Merchant Agreement shall be entitled to reasonable document and deposition discovery, including (x) reasonable discovery of electronically stored information, as approved by the arbitrator, who shall consider, *inter alia*, whether the discovery sought from one party is proportional to the discovery received by another party, and (y) no less than five depositions per party; and (b) within sixty (60) days of the initial award, either party can file a notice of appeal to a three-arbitrator panel administered by the selected arbitration organization, which shall reconsider *de novo* any aspect requested of that award and whose decision shall be final and binding. If more than sixty (60) days after the written arbitration decision is issued the losing party fails to satisfy or comply with an award or file a notice of appeal, if applicable, the prevailing party shall have the right to seek judicial confirmation of the award in any state or federal court where Merchant's headquarters or Merchant's assets are located.

viii. Confidentiality. The arbitration proceeding and all testimony, filings, documents, and any information relating to or presented during the proceedings shall be deemed to be confidential information not to be disclosed to any other party. All offers, promises, conduct, and statements, whether written or oral, made in the course of the Claim resolution process, including but not limited to any related negotiations, mediations, arbitration, and proceedings to confirm arbitration awards by either party, its agents, employees, experts or attorneys, or by mediator or arbitrator, including any arbitration award or judgment related thereto, are confidential and inadmissible for any purpose, including impeachment or estoppel, in any other litigation or proceeding involving any of the parties or non-parties; provided that evidence that is otherwise admissible or

discoverable shall not be rendered inadmissible or non-discoverable as a result of its use in the negotiation, mediation, or arbitration.

ix. Costs of Arbitration Proceedings. Merchant will be responsible for paying Merchant's share of any arbitration fees (including filing, administrative, hearing or other fees), but only up to the amount of the filing fees Merchant would have incurred if Merchant had brought a Claim in court. American Express will be responsible for any additional arbitration fees. At Merchant's written request, American Express will consider in good faith making a temporary advance of Merchant's share of any arbitration fees, or paying for the reasonable fees of an expert appointed by the arbitrator for good cause.

x. Additional Arbitration Awards. If the arbitrator rules in Merchant's favor against American Express for an amount greater than any final settlement offer American Express made before any arbitration award, the arbitrator's award will include: (1) any money to which Merchant is entitled as determined by the arbitrator, but in no case less than $5,000; and (2) any reasonable attorneys' fees, costs and expert and other witness fees incurred by Merchant.

xi. Definitions. For purposes of this section [XX] only, (i) *American Express* includes any of its affiliates, licensees, predecessors, successors, or assigns, any purchasers of any receivables, and all agents, directors, and representatives of any of the foregoing, and (ii) *Merchant* includes any of Merchant's affiliates, licensees, predecessors, successors, or assigns, any purchasers of any receivables and all agents, directors, and representatives of any of the foregoing, and (iii) *Claim* means any allegation of an entitlement to relief, whether damages, injunctive or any other form of relief, against American Express or against Merchant Services Provider or any other entity that American Express has the right to join in resolving a Claim, including, a transaction using an American Express product or network or regarding an American Express policy or procedure.

- **Treatment of the American Express Brand**

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

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

- promote any Other Payment Products (except Merchant's own private label card that Merchant issues for use solely at Merchant's Establishments) more actively than Merchant promote the Card, or

- convert the currency of the original sale Transaction to another currency when requesting Authorization or submitting Transactions (or both).

Merchant may offer discounts or in-kind incentives from Merchant's regular prices for payments in cash, ACH funds transfer, check, debit card or credit/charge card, provided that (to the extent required by Applicable Law): (i) Merchant clearly and conspicuously disclose the terms of the discount or in-kind incentive to Merchant's customers, (ii) the discount or in-kind incentive is offered to all of Merchant's prospective customers, and (iii) the discount or in-kind incentive does not differentiate on the basis of the issuer or, except as expressly permitted by applicable state statute, payment card network (e.g., Visa, MasterCard, Discover, JCB, American Express). The offering of discounts or in-kind incentives in compliance with the terms of this paragraph will not constitute a violation of the provisions set forth above in this Section **[XX]**, "Treatment of the American Express Brand".

- **Treatment of the American Express Marks**

  Whenever payment methods are communicated to customers, or when customers ask what payments are accepted, Merchant must indicate Merchant's acceptance of the Card and display American Express' Marks (including any Card application forms provided to Merchant) as prominently and in the same manner as any Other Payment Products. Merchant must not use the American Express Marks in any way that injures or diminishes the goodwill associated with the Mark, nor (without prior written consent from Merchant Services Provider) indicate that American Express endorse Merchant's goods or services. Merchant shall only use the American Express Marks as permitted by the Merchant Agreement and shall cease using American Express' Marks upon termination of the Merchant Agreement.

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

- **Treatment of American Express Card Member Information**

  Any and all Card Member Information is confidential and the sole property of the Issuer, American Express or its Affiliates. Except as otherwise specified, Merchant must not disclose Card Member Information, nor use nor store it, other than to facilitate Transactions at Merchant's Establishments in accordance with the Merchant Agreement.

Exhibit B-2 to Appendix B
Additional Flow-Down Requirements

The flow-down requirements in this Exhibit B-2 must be incorporated substantively in each Merchant Processing Agreement and Sponsored Merchant Agreement, but Participant has discretion as to exactly how they are incorporated.

1. RESERVED

2. DOING BUSINESS WITH AMERICAN EXPRESS

2.1 Compliance with the Technical Specifications

Merchant must ensure that it and any third parties it enlists to facilitate Transaction processing (i.e., Merchant's Merchant Services Provider) complies with the American Express Technical Specifications (valid and accurate data must be provided for all data elements in accordance with the American Express Technical Specifications). Failure to comply with the American Express Technical Specifications may impact Merchant's ability to successfully process Transactions.

Merchants may be assessed non-compliance fees if Merchant fails to comply with the Technical Specifications. To ensure compliance with the Technical Specifications, Merchants should work with their Merchant Services Provider.

[Drafting Note: The American Express Technical Specifications must be provided by the Participant, or Participant must direct the Merchant as to where they can obtain the American Express Technical Specifications.]

2.2 Establishment Closing

If a Merchant closes any of its Establishments, Merchant must follow these guidelines:

- Notify Merchant Services Provider immediately.
- Policies must be conveyed to the Card Member prior to completion of the Charge and printed on the copy of a receipt or Charge Record the Card Member signs. See Section 4.8, "Return and Cancellation Policies" for additional information.
- If not providing refunds or exchanges, post notices indicating that all sales are final (e.g., at the front doors, by the cash registers, on the Charge Record and on websites and catalogs).
- Return and cancellation policies must be clearly disclosed at the time of sale.
- For Advance Payment Charges or Delayed Delivery Charges, Merchant must either deliver the goods or services for which Merchant has already charged the Card Member or issue Credit for any portion of the Charge for which Merchant has not delivered the goods or services.

2.3 Verification and Disclosure of Information

Merchant acknowledges that when it provides information to its Merchant Services Provider that such information can be disclosed and shared with its Merchant Services Provider's agents, subcontractors, Affiliates and other parties including American Express, industry organizations and reporting agencies, for any purpose permitted by Applicable Law.

Merchant acknowledges that by entering into the Merchant Agreement, Merchant is providing permission to obtain or disclose information in connection with the Merchant Agreement, hereby releases and waives any right or Claim arising out of or related to such disclosure, including defamation Claims, even if the information that is disclosed is incorrect or incomplete. Merchant acknowledges that Merchant's business name and the name of Merchant's principals may be reported to the MATCH™ (Member Alert to Control High Risk Merchants) listing maintained by MasterCard. Merchant hereby specifically consents to the reporting, and waives and holds American Express and Merchant Services Provider harmless from all Claims and liabilities Merchant may have as a result of such reporting.

2.4 Merchant Information; Marketing Communication Opt-Outs

Merchant agrees that, upon providing contact information to its Merchant Services Provider, American Express may send Merchant commercial marketing messages, including important information about American Express products, services, and resources available to its business. These messages may be sent to the mailing address, phone numbers, email addresses or fax numbers Merchant provides. If Merchant provides a wireless phone number, Merchant agrees that it may be contacted at that number and the communications sent may include autodialed short message service (SMS or "text") messages or automated or prerecorded calls. If Merchant provides a fax number, Merchant agrees that it may be sent fax communications. American Express may otherwise use and share Merchant information for business purposes and as permitted by Applicable Law. American Express uses reasonable administrative, technical and physical security measures to protect Merchant information consistent with the sensitivity of the information.

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

3. CARD ACCEPTANCE

3.1 Reserved

3.2 Reserved

3.2.1 Reserved

3.3 Prohibited Uses of the Card

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

- adult digital content sold via Internet Electronic Delivery,
- amounts that do not represent bona fide sales of goods or services (or, if applicable, amounts that do not represent bona fide charitable contributions made) at Merchant's Establishments; for example, purchases at Merchant's Establishments by Merchant's owners (or their family members) or employees contrived for cash flow purposes, or payments that Merchant have accepted in order to advance cash to Card Members in connection with the Transaction,
- amounts that do not represent bona fide, direct sales by Merchant's Establishment to Card Members made in the ordinary course of Merchant's business,
- cash or cash equivalent; for example, purchases of gold, silver, platinum and palladium bullion and/or bars (collectible coins and jewelry are not prohibited), or virtual currencies that can be exchanged for real currency (loyalty program currencies are not prohibited),
- Charges that the Card Member has not specifically approved,
- costs or fees over the normal price of the goods or services (plus applicable taxes) that the Card Member has not specifically approved,
- damages, losses, penalties, or fines of any kind,
- gambling services (including online gambling), gambling chips, gambling credits, or lottery tickets,
- unlawful/illegal activities, fraudulent business transactions or when providing the goods or services is unlawful/illegal (e.g. unlawful/illegal online internet sales of prescription medications or controlled substances; sales of any goods that infringe the rights of a Rights-holder under laws applicable to American Express, Merchant, or the Card Member),
- overdue amounts or amounts covering returned, previously dishonored or stop-payment checks (e.g., where the Card is used as a payment of last resort),
- amounts that represent repayment of a cash advance including, but not limited to, payday loans, pawn loans or payday advances,

- sales made by third parties or Entities conducting business in industries other than Merchant's, or
- other items of which American Express or Merchant Services Provider notifies Merchant.

Merchant must not use the Card to verify a customer's age.

4. TRANSACTION PROCESSING

4.1 Completing a Transaction at the Point of Sale

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

To accept the Card for Charges at Merchant's Establishments, at the point of sale, Merchant must:

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

The Transaction Data the Merchant collects to facilitate the Charge must be or have been provided directly to the Merchant by the Card Member.

Merchant must not accept or have accepted Transaction Data from, nor shall Merchant provide or have provided Transaction Data to, any third parties other than Merchant's Covered Parties. If Merchant fails to comply with this requirement. Merchant may be assessed non-compliance fees and/or have its Card acceptance privileges suspended or disentitled.

4.2 Processing an In-Person Charge

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

For all In-Person Charges, the Card must be presented. There are several ways in which you can conduct the In-Person Charge. The steps you take vary according to how you go about conducting the following two types of In-Person Charges:

- electronic Charges
- key-entered Charges

4.2.1 Electronic Charges

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

- Magnetic Stripe Cards – contain Card Member and Card account information on the stripe on the back of the Card, or in a contactless Chip embedded in the Card.
- Chip Cards – contain a Chip on which data is stored (including Card Member and Card account information), which the Point of Sale System can read in order to guide the processing of the Transaction.

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

Merchants must work with their Merchant Services Provider if they have questions about their POS System's capabilities.

4.2.1.1 Magnetic Stripe Card Charges

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

1. Verify that the Card is not visibly altered or mutilated
2. Verify that the customer is the Card Member* (Cards are not transferable),
3. Capture Magnetic Stripe data by swiping the Card (unless the Charge was already initiated by waving the contactless Chip Card in close proximity to the Point of Sale System)
4. Obtain an Authorization Approval,
5. Obtain signature (excluding Charges at CATs) and verify that the signature is identical to the name on the Card.* Failure to obtain a signature, when required, can render Merchant liable for Chargebacks if the Card Member disputes the Charge. Obtaining a signature may not be required if Merchant's Establishment and the Charge qualify for the No Signature Program (see Section 4.15, "No Signature Program" for additional information),
6. Compare the signature (when obtained) on the Charge Record with the signature on the Card,
7. Verify the Card's Expiration Date,
8. Match the Card Number and the Expiration Date on the Card to the same information on the Charge Record, and
9. Ensure the name that prints on the Charge Record matches the name on the front of the Card.*

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

4.2.1.2 Contact Chip Card Charges

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

1. Verify that the Card is not visibly altered or mutilated
2. Verify that the customer is the Card Member* (Cards are not transferable),
3. Capture Chip Card Data by inserting the Card into the Chip Card reader,

   The Point of Sale System will advise Card Members to enter their PIN (a Chip and PIN Charge) or sign for the Charge (a Chip and signature Charge):

   - Chip and PIN Charges: Card Members will enter their PIN into the Point of Sale System using the keypad. If the Chip and PIN Charge is unable to be completed due to a technical problem, the Point of Sale System will show an error message. Follow the procedures for a swiped Charge in subsection 4.2.1.1, "Magnetic Stripe Card Charges"
   - Chip and signature Charge: Obtain the Card Member's signature on the Charge Record and compare the signature on the Charge Record to the name and signature on the Card.* Failure to obtain a signature, when required, can render Merchant liable for Chargebacks if the Card Member disputes the Charge. Obtaining a signature may not be required if Merchant's Establishment and the Charge qualify for the No Signature Program (see Section 4.15, "No Signature Program" for additional information),
4. Obtain an Authorization Approval,
5. Verify the Card's Expiration Date,
6. Match the Card Number and the Expiration Date on the Card to the same information on the Charge Record, and
7. Ensure the name that prints on the Charge Record matches the name on the front of the Card.*

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

4.2.1.3 Contactless Chip Card Charge

Some Chip Card Charges involve transmission of payment information when the Card is waved in close proximity to a contactless reader.

When presented with a Chip Card to be read via a contactless reader, and the Charge qualifies for the No Signature Program, Merchant must:

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

For Charges that do not qualify under the No Signature Program, follow the relevant Card acceptance procedures outlined in either:

- subsection 4.2.1.1, “Magnetic Stripe Card Charges”, or
- subsection 4.2.1.2, “Contact Chip Card Charges”

See Section 4.15, “No Signature Program” for additional information.

4.2.1.4 Mobile Contactless Charges

A mobile contactless Transaction is a Transaction initiated through a contactless-enabled mobile phone at a contactless-enabled Point of Sale System. These mobile phones contain a payment application which can initiate a contactless Transaction when the phone is waved in close proximity to a contactless-enabled Point of Sale System.

When presented with a contactless-enabled mobile phone, Merchant must:

1. Capture Magnetic Stripe or Chip Card data by waving the contactless-enabled mobile phone in close proximity to the contactless reader,
2. Obtain an Authorization Approval,
3. Obtain signature (excluding Charges at CATs), unless the Charge qualifies for the No Signature Program (see Section 4.15, "No Signature Program" for additional information),
4. Compare the signature (when obtained) on the Charge Record with the signature on the companion physical Card or a valid form of formal identification (e.g. driver's license). Merchant must not record or store the information from such formal identification in any way.

If a mobile contactless Transaction cannot be processed for any reason, Merchant should request that the Card Member provide the companion physical Card and complete the Transaction by following the relevant Card acceptance procedures outlined in:

- subsection 4.2.1.1, “Magnetic Stripe Card Charges”, or
- subsection 4.2.1.2, “Contact Chip Card Charges”.

4.2.1.5 Key-Entered Charges

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

If the Card cannot be read electronically, Merchant must:

1. Verify that the Card is not visibly altered or mutilated (see Chapter 9, “Fraud Prevention” for additional information),
2. Verify that the customer is the Card Member (Cards are not transferable),

3. Key-enter the data,

4. Obtain an Authorization Approval,

5. Obtain signature and verify that the signature is identical to the name on the Card.* Failure to obtain a signature, when required, can render Merchant liable for Chargebacks if the Card Member disputes the Charge. Obtaining a signature may not be required if Merchant's Establishment and the Charge qualify for the No Signature Program (see Section 4.15, "No Signature Program" for additional information),

6. Compare the signature (when obtained) on the Charge Record with the signature on the Card,

7. Verify the Card's Expiration Date,

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

9. Validate the Card's presence by taking an imprint of the Card (the imprint is for Merchant's records). Failure to validate the Card's presence by taking an imprint of the Card can render Merchant liable for Chargebacks if the Card Member disputes the Charge.

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

Merchant may also validate the Card's presence by ensuring the Charge meets the criteria of the Keyed No Imprint Program. See Section 4.14, "Keyed No Imprint Program" for additional information. Key-entered Charges are subject to a fee. Charges initiated with a contactless-enabled mobile phone must not be key-entered.

4.2.1.6 Actions for In-Person Charges

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

If	Then
The Card is obviously altered or counterfeit.	Do not accept the Card.
The Card Member is attempting to use the Card outside of its Valid Dates. Note: Cards are valid through the last day of the month on the front of the Card.	Do not accept the Card. Advise the Card Member to contact the customer service number on the back of the Card.
It appears that someone other than the Card Member is attempting to use the Card.	Do not accept the Card. Indicate that the Cards are non-transferable and that only the Card Member is permitted to use the Card.
The signature does not match the name on the Card.	Contact Merchant Services Provider.
Merchant unable to obtain Authorization electronically.	Contact Merchant Services Provider.

The Authorization is Declined.	Do not accept the Card, and follow Merchant's internal policies for handling various Authorization responses. See Section 5.4, "Possible Authorization Responses".
The customer presents an unsigned Card.	An unsigned Card is invalid. Show customer that the Card is not signed. Ask the customer to sign the Card and also request photo identification (ID) such as a valid driver's license or passport to compare the signatures. If the customer refuses to sign the Card, and Merchant accept it, Merchant are liable for a Chargeback.
The customer's signature on the Charge Record does not appear to match the customer's signature on the Card.	Contact Merchant Services Provider, or, if Merchant prefer, simply decline to accept the Card. For more information on Code 10, see Chapter 9, "Fraud Prevention".
The Card Numbers and Valid Dates on the Card do not match the Charge Record.	
The name on the Charge Record does not match the name on the Card (except in the case of a Prepaid Card which may not show a name on its face).	
The appearance of the Card or the actions of the customer make Merchant suspicious.	

4.3 Customer Activated Terminals

Charges for purchases at Merchant's Customer Activated Terminals (CATs) must meet the requirements for Charge Records as detailed in Section 4.5, "Charge Records" as well as comply with the Technical Specifications.

Merchant must include:

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

American Express will not be liable for actual or alleged fraudulent Charges occurring through Customer Activated Terminals and will have the right to Chargeback for those Charges.

4.4 Processing a Card Not Present Charge

Merchant must:

- Obtain information of the Card Member as described below;
- Obtain an authorization Approval
- Submit the Charge to Merchant Services Provider

For Card Not Present Charges, Merchant must create a Charge Record as described in Section 4.5, "Charge Records". The information Merchant must ask the Card Member to provide includes:

- Card Number, and

- Card Expiration Date.

In addition it is recommended that Merchant ask for:

- name as it appears on the Card,
- Card Member's billing address, and
- ship-to address, if different from the billing address.

American Express has the right to Chargeback for any Card Not Present Charge that the Card Member denies making or authorizing. American Express will not Chargeback for such Charges based solely upon a Card Member claim that he or she did not receive the disputed goods if Merchant has:

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

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

For Internet Orders, Merchant must:

- use any separate Merchant Numbers (Seller ID) established for Merchant for Internet Orders in all Merchant's requests for Authorization and Submission of Charges,
- provide American Express with at least one (1) month's prior written notice of any change in Merchant's internet address, and
- comply with any additional requirements that American Express provides from time to time.

Additionally, if a Disputed Charge arises involving a Card Not Present Charge that is an Internet Electronic Delivery Charge, American Express may exercise Chargeback for the full amount of the Charge and place Merchant in any of its Chargeback programs. When providing Proof of Delivery, a signature from the Card Member or an authorized signer of the Card is not required.

4.5 Charge Records

Merchant must create a Charge Record for every Charge. For each Charge submitted electronically, Merchant must create an electronically reproducible Charge Record, and the Charge must comply with the Technical Specifications.

The Charge Record (and a copy of the customer's receipt) must disclose Merchant's return and/or cancellation policies. See Section 4.8, "Return and Cancellation Policies" for additional information.

If the Card Member wants to use different Cards for payment of a purchase, Merchant may create a separate Charge Record for each Card used. However, if the Card Member is using a

single Card for payment of a purchase, Merchant shall not divide the purchase into more than one Charge, nor shall Merchant create more than one Charge Record.

For all Charge Records, Merchant must:

1. Submit the Charge to Merchant Services Provider for payment.
2. Retain the original Charge Record (as applicable) and all documents evidencing the Charge, or reproducible records thereof, for the timeframe listed in American Express' country-specific policies. See chapter 8, "Protecting Card Member Information" for additional information.
3. Provide a copy of the Charge Record to the Card Member.

Merchant may be able to create more than one Charge Record if the purchase qualifies for a Delayed Delivery Charge. See Section 4.13, "Delayed Delivery Charges".

The retention time frame for Charge Records is twenty-four (24) months from the date Merchant submitted the corresponding Charge to American Express.

Pursuant to Applicable Law, truncate the Card Number and do not print the Card's Expiration Date on the copies of Charge Records delivered to Card Members. Truncated Card Number digits must be masked with replacement characters such as "x," "*," or "#," and not blank spaces or numbers.

4.6 Processing a Credit

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

Follow these steps to issue a Credit:

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

Merchant must submit Credits to its Merchant Services Provider within seven (7) days of determining that a Credit is due and create a Credit Record that complies with Merchant Services Provider's requirements (see Section 4.7, "Credit Records" for additional information). Merchant must not issue a Credit when there is no corresponding Charge, nor issue a Credit in exchange for cash or other consideration from a Card Member.

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

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

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

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

4.7 Credit Records

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

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

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

For all Credit Records, Merchant must:

1. Submit the Credit through the Merchant Services Provider.
2. Retain the original Credit Records (as applicable) and all documents evidencing the Transaction, or reproducible records thereof, for the timeframe listed below.
3. Provide a copy of the Credit Record to the Card Member.

The retention time frame for Credit Records is twenty-four (24) months from the date. If, under extraordinary circumstances, Merchant submits Transactions on paper, Merchant must do so in accordance with Chapter 4, "Transaction Processing". Examples of circumstances that may prevent Merchants from submitting electronically are:

- special events (e.g., conferences, outdoor marketplaces, concerts)

- Merchants that do not conduct business from fixed locations (e.g., taxis and limousine services)
- remote locations, or Merchants who experience System Outages

If Merchant submits Charges on paper, Merchant must create a Charge Record containing all of the following required data:

- Full Card Number and Expiration Date (pursuant to Applicable Law), and if available, Card Member name.
- The date the Charge was incurred.
- The amount of the Charge, which must be the total price for the purchase of goods and services (plus applicable taxes and gratuities) purchased on the Card.
- The Authorization Approval.
- A clear description of the goods or services purchased by the Card Member.
- An imprint or other descriptor of Merchant's name, address, Merchant Number and, if applicable, store number.
- The words "No Refunds" if Merchant has a no refund policy, and Merchant's return and/or cancellation policies. See Section 4.8, "Return and Cancellation Policies" for additional information.

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

Pursuant to Applicable Law, Merchant must truncate the Card Number and must not not print the Card's Expiration Date on copies of Credit Records delivered to the Card Member.

4.8 Return and Cancellation Policies

Merchant's return and cancellation policies must be fair and clearly disclosed at the time of sale in compliance with Applicable Law. Merchant's policies must be conveyed to the Card Member prior to completion of the Charge and printed on a copy of a receipt or Charge Record.

Merchant must not give cash refunds to Card Members for goods or services they purchase on the Card, unless required by Applicable Law. Merchant's refund policy for purchases on the Card must be at least as favorable as Merchant's refund policy for purchases made with Other Payment Products or other payment methods.

Return Policy recommendations:

Provide clear return instructions for Merchant's customers, including the following information:

- customer service telephone number,
- reference number for the return,

- expected processing time for the Credit, and
- return address, preferably on a pre-formatted shipping label (if applicable).

Cancellation Policy recommendations

Document cancellation policy and terms and conditions on the contract the Card Member signs, or on Merchant's website, as applicable. Provide Card Member with a cancellation number that can be tracked in Merchant's records.

4.9 Return Policy for Prepaid Products

This section applies to Merchants who accept the Card for the purchase of any prepaid product (Prepaid Cards, non-American Express branded stored value or gift cards, or both). If Merchant's return policy for the purchase of prepaid products is different from Merchant's standard return policy, notwithstanding the requirements listed in Section 4.8, "Return and Cancellation Policies", Merchant must ensure that such prepaid product-specific return policy is clearly disclosed to the Card Member at the time of purchase and also coded to print on all receipts and copies of Charge Records Merchant provide to Card Members.

4.10 Processing Transactions for Specific Industries

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

4.11 Advance Payment Charges

An Advance Payment Charge is a Charge for which full payment is made in advance of Merchant's providing the goods and/or rendering the services to the Card Member. Purchases involving Advance Payment Charges generally carry a higher level of risk than other Charges, due to the fact that goods and services are not provided at the time the Charge is processed. For this reason, American Express may withhold settlement for part or all of such Charges until it is determined that the risk has diminished.

Merchant must follow these procedures if Merchant offers Card Members the option or require them to make Advance Payment Charges for the following types of goods and/or services:

- Custom-orders (e.g., orders for goods to be manufactured to a customer's specifications)
- Entertainment/ticketing (e.g., sporting events, concerts, season tickets)
- Tuition, room and board, and other mandatory fees (e.g., library fees) of higher educational institutions
- Travel-related services (e.g., tours, guided expeditions)

For an Advance Payment Charge, Merchant must:

- State Merchant's full cancellation and refund policies, clearly disclose Merchant's intent and obtain written consent from the Card Member to bill the Card for an Advance Payment Charge before Merchant request an Authorization. The Card Member's consent must include:
  - his or her agreement to all the terms of the sale (including price and any cancellation and refund policies), and
  - a detailed description and the expected delivery date of the goods and/or services to be provided.
- Obtain an Authorization Approval.
- Complete a Charge Record. If the Advance Payment Charge is a Card Not Present Charge, Merchant must also:
  - ensure that the Charge Record contains the words "Advance Payment" (see Section 4.5, "Charge Records"), and
  - within twenty-four (24) hours of the Charge being incurred, provide the Card Member written confirmation (e.g., email or facsimile) of the Advance Payment Charge, the amount, the confirmation number (if applicable), a detailed description and expected delivery date of the goods and/or services to be provided and details of Merchant's cancellation/refund policy.

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

In addition to other Chargeback rights, American Express may exercise Chargeback for any Disputed Advance Payment Charge or portion thereof if, in American Express' sole discretion, the dispute cannot be resolved in Merchant's favor based upon unambiguous terms contained in the terms of sale to which Merchant obtained the Card Member's written consent.

4.12 Aggregated Charges

Aggregated Charge is a Charge that combines multiple small purchases or refunds (or both) incurred on a Card into a single, larger Charge before submitting the Charge for payment. If Merchant is classified in an internet industry, Merchant may process Aggregated Charges provided the following criteria are met:

- Clearly disclose Merchant's intent and obtain written consent from the Card Member that their purchases or refunds (or both) on the Card may be aggregated and combined with other purchases or refunds (or both) before Merchant request an Authorization.
- Each individual purchase or refund (or both) that comprises the Aggregated Charge must be incurred under the same Establishment and on the same Card.

- Obtain a pre-Authorization of no more than $15. See Section 5.10, “Pre-Authorization” for additional information.
- Create a Charge Record for the full amount of the Aggregated Charge. For more information on Charge Records, see Section 4.5, “Charge Records”.
- The amount of the Aggregated Charge must not exceed $15 or the amount for which Merchant obtained pre-Authorization.
- Submit each Charge Record within American Express’ Submission timeframe (see Section 6.4, “Submission Requirements - Electronic”). For the purposes of Section 6.4, “Submission Requirements - Electronic”, a Charge will be deemed “incurred” on the date of the first purchase or refund (or both) that comprises the Aggregated Charge.
- Provide the Card Member with an email containing:
  - the date, amount, and description of each individual purchase or refund (or both) that comprises the Aggregated Charge, and
  - the date and the amount of the Aggregated Charge.

4.13 Delayed Delivery Charges

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

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

- Clearly disclose Merchant’s intent and obtain written consent from the Card Member to perform a Delayed Delivery Charge before Merchant request an Authorization,
- Obtain a separate Authorization Approval for each of the two Delayed Delivery Charges on their respective Charge dates,
- Clearly indicate on each Delayed Delivery Charge Record that the Charge is either for the deposit or for the balance of the Delayed Delivery Charge,
- Submit the Delayed Delivery Charge Record for the balance of the purchase only after the goods have been shipped, provided or services rendered,
- Submit each Delayed Delivery Charge Record within American Express’ Submission timeframes (see Section 6.4, “Submission Requirements - Electronic”). For the purposes of Section 6.4, “Submission Requirements - Electronic”, the Charge will be deemed “incurred”:
  - for the deposit - on the date the Card Member agreed to pay the deposit for the purchase.
  - for the balance - on the date the goods are shipped, provided or services are rendered.

- Submit and Authorize each Delayed Delivery Charge under the same Establishment, and
- Treat deposits on the Card no differently than Merchant treat deposits on all Other Payment Products.

4.14 Keyed No Imprint Program

The Keyed No Imprint Program allows Merchant to submit In-Person Charges without taking an imprint of the Card if Merchant meets the following Charge criteria. All Cards qualify for the Keyed No Imprint Program.

Charge criteria:

- the Charge must be key-entered,
- the Charge Submission must include the appropriate indicator to reflect that the Card and the Card Member were present at the point of sale,
- the Charge Submission must include a valid Approval, and
- the CID Number must be confirmed as a positive match.

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

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

4.15 No Signature Program

Merchants may participate in American Express' No Signature Program. The No Signature Program allows Merchants not to request a signature from Card Members on the Charge Record.

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

Merchant criteria:

If a Merchant is classified in an industry that accepts In-Person Charges, then such Merchant may participate in the No Signature Program with the exception of the following categories:

- Merchants who do not conduct In-Person Charges (i.e., internet, mail order or telephone order).
- Prohibited Merchants or prohibited Transactions (or both) as defined in Chapter 10, "Risk Evaluation". See Section 3.3, "Prohibited Uses of the Card".
- High Risk Merchants (e.g., internet electronic services or nightclubs/lounges) as defined in Section 10.3, "High Risk Merchants".

- Merchants placed in American Express' Fraud Full Recourse Program.

Charge criteria:

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

Under the No Signature Program, American Express will not exercise Chargeback for such Charges based solely on the Merchant's failure to obtain the Card Member's signature at the point of sale.

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

The established threshold for charges to qualify under the No Signature Program is $50.00 or less.

4.16 Recurring Billing Charges

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

If Merchant offers Card Members the option to make Recurring Billing Charges, Merchant must:

- obtain the Card Member's express written consent for Merchant to bill the Card before submitting the first Recurring Billing Charge, and
- notify the Card Member that he or she can withdraw such consent at any time.

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

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

Before submitting a Recurring Billing Charge, Merchant must obtain Authorization and complete a Charge Record (see Section 4.5, "Charge Records"), except with the words "signature on file," if applicable, on the signature line and the appropriate electronic descriptor on the Charge Record. For complete Authorization requirements, see Chapter 5, "Authorization".

If the Merchant Agreement terminates for any reason, then Merchant must notify all Card Members for whom Merchant has submitted Recurring Billing Charges that Merchant no longer accepts the Card.

Merchant must fulfill Card Members' requests that Merchant discontinue the Recurring Billing Charges immediately and provide cancellation numbers to them.

The cancellation of a Card constitutes immediate cancellation of that Card Member's consent for Recurring Billing Charges. American Express will not notify Merchant or its Merchant Services Provider of such cancellation, nor will American Express have any liability to Merchant arising from such cancellation.

If a Card is cancelled, or if a Card Member withdraws consent to Recurring Billing Charges, Merchant is responsible for arranging another form of payment (as applicable) with the Card Member.

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

If Merchant offers Card Members the option to make Recurring Billing Charges, Merchant must:

- ensure that Merchant’s process for cancellation of Recurring Billing is simple and expeditious
- clearly and conspicuously disclose all material terms of the option, including, if applicable, the fact that Recurring Billing will continue until the option is cancelled by the Card Member,
- within twenty-four (24) hours of incurring the first Recurring Billing Charge, provide the Card Member written confirmation (e.g., email or facsimile) of such Charge, including all material terms of the option and details of Merchant’s cancellation/refund policy, and
- where the material terms of the option change after Submission of the first Recurring Billing Charge, promptly notify the Card Member in writing of such change and obtain the Card Member's express written consent to the new terms prior to submitting another Recurring Billing Charge.

If Merchant’s Recurring Billing Charge amounts vary, Merchant must offer the Card Member the right to receive written notification of the amount and date of each Recurring Billing Charge:

- at least ten (10) days before submitting each Charge, or
- whenever the amount of the Charge exceeds a maximum Recurring Billing Charge amount specified by the Card Member.

American Express may exercise Chargeback for any Charge of which Merchant has notified the Card Member and to which the Card Member does not consent.

4.17 Processing Prepaid Cards

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

Prepaid Cards are valid through the date on the Card. Follow the relevant Card acceptance procedures outlined in Chapter 4, "Transaction Processing" when presented with a Prepaid Card at the point of sale just like any other Card. A Prepaid Card must be tendered for an amount that is no greater than the funds available on the Card.

- Instruct Card Members that, before making a purchase, they must check their remaining funds by:
  - calling the twenty-four (24) hour, toll-free number on the back of the Card,
  - checking online, or
  - using the mobile app offered by their Issuer (where available).
- Because Prepaid Cards are pre-funded, if Merchant receives a Decline when seeking Authorization, ask the customer to go online, use their mobile app, or call the toll-free number on the back of the Card to confirm that the purchase price does not exceed the available funds on the Prepaid Card.
- If the Prepaid Card does not have enough funds to cover the purchase price, process a Split Tender Transaction or request an alternative form of payment. See Section 5.11, "Additional Authorization Requirements".
- Merchant must create a Charge Record for a Prepaid Card as Merchant would any other Card.

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

4.18 Processing Travelers/Gift Cheques

American Express Travelers Cheques, Cheques for Two, and Gift Cheques are easy to accept provided that the cheque is an authentic American Express Travelers Cheque. See Section 4.19, "Acceptance Procedures".

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

Travelers Cheques

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

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

Gift Cheques

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

- Contact Travelers Cheque/Gift Cheque Customer Service.
- Do not accept it.
- Write the word “VOID” across the front of the counterfeit Cheque.

For further information, see Chapter 9, “Fraud Prevention”.

4.19 Acceptance Procedures

Accepting American Express Travelers and Gift Cheques is easy:

- Watch customer countersign in the lower left corner of the Cheque, and compare the countersignature to the signature in the upper left corner for American Express Travelers Cheques and Gift Cheques. For Cheques for Two, the customer's countersignature must match either one of the two signatures on top.
- Validate Security Features - Validating these features will help reduce the acceptance of counterfeit cheques. See Section 9.8, “Travelers Cheque and Gift Cheque Security Features”.
- Obtain Authorization - American Express recommends obtaining an authorization to reduce the chances of accepting fraudulent cheques. American Express offers a variety of authorization tools. See authorization methods in the following table to determine the appropriate course of action:

If	Then
The signature and countersignature are a reasonable match (they look alike, but may not be identical)	Accept the cheque. There is no need to obtain any identification.
Merchant suspects that the countersignature may be false, or Merchant did not watch the customer countersign	Ask the customer to turn the cheque over and sign again across the left-hand side (in the same manner one typically endorses a check). Then take the cheque and fold up the bottom right-hand corner so that Merchant can compare the original signature with the new one.
The signatures are not the same, or if there is a question regarding the validity of the cheque	Call the Travelers Cheque/Gift Cheque Customer Service.

Merchant suspects that the Travelers cheque being presented is fraudulent	Use any of the following methods to verify that the cheque Merchant is accepting is authentic: o Perform a smudge test (see chapter 9, "Fraud Prevention" for details). o Obtain online Authorization at www.americanexpress.com/verifyamextc.

5. AUTHORIZATIONS

5.1 Introduction

The payment card industry devotes significant amounts of time and resources to developing Authorization systems and decision models in an effort to mitigate the financial losses.

Every Transaction begins and ends with the Card Member. Between the time the Card Member presents the Card for payment and receives the goods or services, however, a great deal of data is exchanged, analyzed and processed. A process that literally takes seconds at the point of sale is actually a highly complex approach to analyzing each Transaction.

5.2 Transaction Cycle

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

5.3 The Purpose of Authorization

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

For every Charge, Merchant is required to obtain an Authorization Approval except for Charges under a Floor Limit. The Authorization Approval must be for the full amount of the Charge except for Merchants that are classified in the restaurant industry (see Section 12.7, “Restaurants”).

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

5.4 Possible Authorization Responses

Responses to Merchant’s requests for Authorization are generated by Issuers and transmitted to Merchant. The following are among the most commonly generated responses to Merchant’s request for Authorization. The exact wording will vary so Merchant should check with its Merchant Services Provider or Terminal Provider to determine what Authorization responses will display on its equipment.

Authorization Response	What It Means
Approved	The Charge is approved.
Partially Approved (for use with Prepaid Cards only)	The Charge is approved. The Approval is for an amount less than the value originally requested. The Charge must only be submitted for the approved amount. Collect the remaining funds due from the Card Member via another form of payment. See Section 5.11, "Additional Authorization Requirements" for more information about split tender.
Declined or Card Not Accepted	The Charge is not approved. Do not submit the Charge. If you nevertheless choose to submit the Charge, you will be subject to a Chargeback. Inform the Card Member promptly that the Card has been Declined. If the Card Member has questions or concerns, advise the Card Member to call the customer service telephone number on the back of the Card. Never discuss the reason for the Decline.
Please Call or Referral	Additional information is required to complete the Charge. Call your Merchant Services Provider for resolution. See Section 5.6, "Obtaining a Voice Authorization" for instructions.
Pick up	Merchant may receive an Issuer point of sale response indicating that Merchant must pick up the Card. Follow your internal policies when you receive this response. Never put yourself or your employees in unsafe situations. If your policies direct you to do so, you may initiate the pick up process by calling your Merchant Services Provider.

5.5 Obtaining an Electronic Authorization

Generally, Merchants must obtain an electronic Authorization.

Merchant must ensure that all Authorization requests comply with the Technical Specifications (see Section 2.1, "Compliance with the Technical Specifications"). If the Authorization request does not comply with the Technical Specifications, the Submission may be rejected or a Chargeback may be issued.

If the Card is unreadable and Merchant has to key-enter the Charge to obtain an Authorization, then Merchant must follow the requirements for key-entered Charges. See subsection 4.2.1.5, "Key-Entered Charges" for additional information.

If Merchant uses an electronic Point of Sale System to obtain Authorization, the Approval must be printed automatically on the Charge Record.

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

Non-compliance fees may be assessed for Authorization requests that do not comply with the American Express Technical Specifications.

5.6 Obtaining a Voice Authorization

When Authorization is required, if Merchant's electronic Point of Sale System is unable to reach American Express' Authorization system, or Merchant does not have an electronic Point of Sale System, Merchant must seek Authorization using the following steps:

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

   In some situations, Merchant may be asked for additional information such as Expiration Date or Card Identification (CID) Number.
3. A response will be provided. If the request for Authorization is approved, capture the Approval for Submission.
4. If Merchant is submitting electronically, Merchant must enter the Approval into its Point of Sale System. For instructions on how to complete this type of Charge, contact your Merchant Services Provider or Terminal Provider.

Non-compliance fees may be assessed for each Charge for which Merchant request a Voice Authorization unless such a failure to obtain Authorization electronically is due to the unavailability or inoperability of American Express' computer Authorization system.

5.7 Card Identification (CID) Number

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

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

Note: CID Numbers must not be stored for any purpose. They are available for real time Charges only. See Chapter 8, "Protecting Card Member Information."

See Chapter 9, "Fraud Prevention" for more information on CID Numbers and CID Verification.

5.8 Authorization Reversal

Merchants may reverse an Authorization for a corresponding Charge by:

- initiating an Authorization reversal message, or
- Contacting your Merchant Services Provider.

After a Charge Record has been submitted, however, the Authorization cannot be cancelled or changed. For example, if Merchant makes an error in a Charge but has already submitted the Charge Record, Merchant cannot systematically request a change in the Charge. Merchant must instead, follow the procedures for Processing a Credit, as defined in Section 4.6, "Processing a Credit".

5.9 Authorization Time Limit

Authorization Approvals are valid for seven (7) days after the Authorization date except for certain Charges from Merchants that American Express classifies in the cruise line, lodging, and vehicle rental industries. Merchant must obtain a new Approval if Merchant submits the Charge more than seven (7) days after the original Authorization date.

For Charges of goods or services that are shipped or provided more than seven (7) days after an order is placed, Merchant must obtain an Approval for the Charge at the time the order is placed and again at the time Merchant ships or provides the goods or services to the Card Member.

The new Approval must be included in the Charge Record. If either of the Authorization requests is Declined, do not provide the goods or services or submit the Charge. If Merchant does, Merchant may be subject to a Chargeback.

5.10 Pre-Authorization

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

5.11 Additional Authorization Requirements

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

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

Topic	Additional Requirements
Recurring Billing	Merchant must flag all requests for Authorization with a Recurring Billing indicator. To improve the likelihood of obtaining an Approval to an Authorization request, it is recommended that Merchant periodically verify with Card Members that all their information (e.g., Card Number, Expiration Date and billing address) is still accurate. See Section 4.16, "Recurring Billing Charges".
American Express Gift Cheques and American Express Travelers Cheques	Merchant are not required to obtain Authorization prior to accepting Gift and Travelers Cheques. Merchant must, however, follow the appropriate procedures outlined in Section 4.18, "Processing Travelers/Gift Cheques". Questions concerning the validity of Gift or Travelers Cheques can be raised by calling the Travelers Cheque/Gift Cheque Customer Service.

Split Tender	During a Split Tender Transaction, the Card Member uses multiple forms of payment for a single purchase (e.g., prepaid cards, cash, Card). Merchant may follow its policy on combining payment on Prepaid Cards with any Other Payment Products or methods of payment. If the other payment method is a Card then Merchant is required to follow all provisions of the Merchant Agreement. Check with your Merchant Services Provider or Terminal Provider to determine if your Point of Sale System is set up for Split Tender functionality.

5.12 Floor Limit

American Express maintains a zero-dollar Floor Limit on all Charges. Therefore, Merchants must obtain an Authorization on all purchases, regardless of the amount.

6. SUBMISSIONS

6.1 Introduction

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

Since payment cannot occur until the Transactions are submitted, American Express encourages Merchant to submit Transactions daily even though Merchant has up to seven (7) days to do so.

See Section 4.2, "Processing an In-Person Charge" and Section 4.6, "Processing a Credit" for additional information.

6.2 Transaction Cycle

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

6.3 Purpose of Submission

After American Express receives the Submission, American Express will process and settle with your Merchant Services Provider. Transactions will be deemed accepted on a given business day if processed by American Express before the close of business.

6.4 Submission Requirements - Electronic

Merchants must submit Transactions electronically except under extraordinary circumstances.

When a Merchant transmits Charge Data and Transmission Data electronically, Merchant must still complete and retain Charge Records and Credit Records.

A Submission must comply with the American Express Technical Specifications. Failure to follow these requirements could result in a rejection of a Submission or delay in payment (or both). If a Batch rejects, Merchant may not be paid until the Submission is corrected and resubmitted. Merchant must work with its Merchant Services Provider, to correct the error, and then resubmit. Submissions which fail to comply with the Technical Specifications may result in a Chargeback.

Merchant must submit Charges and Credits only in U.S. Dollars.

6.4.1 Charge Submissions

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

For Aggregated Charges, the Charge must be submitted within seven (7) days of the date of the last purchase (and/or refund as applicable) that comprises the Aggregated Charge. See Section 4.12, “Aggregated Charges” for additional information.

Delayed Delivery Charges and Advance Payment Charges may be submitted before the goods are shipped, provided or the services are rendered. See Section 4.13, “Delayed Delivery Charges” and Section 4.11, “Advance Payment Charges” for additional information.

6.4.2 Credit Submissions

Merchant must submit all Credits within seven (7) days of determining that a Credit is due. Merchant must submit each Credit under the Establishment where the Credit originated.

6.5 How to Submit

In many cases, Merchant’s Point of Sale System automatically processes the Transactions in Batches at the end of the day. To be sure, contact your Merchant Services Provider or review the instructions for Submissions that were provided with your Point of Sale System.

On busy days, Merchant’s Transaction volume may be greater than Merchant’s Point of Sale System's storage capability. Work with your Merchant Services Provider to determine your storage capacity, then determine if you will need to submit more than once each day (e.g., submit a Batch at mid-day and again in the evening).

7. SETTLEMENT

7.1 Introduction

All settlement activity is the responsibility of the Merchant Services Provider. Merchant Services Provider will deduct from the payment to Merchant (or debit Merchant's Bank Account), the full amount of all applicable deductions, rejections and withholdings.

American Express will send Settlement amounts to the Merchant Services Provider electronically for payment to Merchant.

Merchant must provide its Merchant Services Provider with its bank's name, routing information, and Bank Account number, and Merchant must notify its bank that the Merchant Services Provider will have access to Merchant's account for debiting and crediting the Bank Account.

Merchant must immediately notify its Merchant Services Provider of any changes to its Bank Account information. Failure to notify Merchant Services Provider of such changes may cause a delay in Settlement until updated.

The policies of the financial institution at which Merchant has a Bank Account govern when funds are available from the Bank Account.

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

- Chargeback has been exercised for such Charge,
- Merchant has fully paid for such Charge, and
- Merchant otherwise has the right to do so.

8. PROTECTING CARD MEMBER INFORMATION

8.1 Merchant Data Security Requirements

As a leader in consumer protection, American Express has a long-standing commitment to protect Card Member Information, ensuring that it is kept secure.

Compromised data negatively impacts consumers, Merchants, and Issuers. Even one incident can severely damage a company's reputation and impair its ability to effectively conduct business. Addressing this threat by implementing security operating policies can help improve customer trust, increase profitability, and enhance a company's reputation.

American Express knows that Merchant shares American Express' concern and requires, as part of Merchant's responsibilities, that Merchant complies with the data security requirements in the Merchant Agreement and this Chapter 8. These requirements apply to all Merchants' equipment, systems, and networks on which encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted.

8.2 Definitions

For the purposes of this Chapter 8, the following definitions apply:

Annual EMV Attestation (AEA) – A declaration of the status of Merchant's compliance with PCI DSS.

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

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

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

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

Card Member Information means information about American Express Card Members and Card transactions, including names, addresses, card account numbers, and card identification numbers ("CIDs").

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 American Express ICC (Integrated Circuit Card) Payment Specification compliant Chip Card Transactions.

Compromised Card Number – A Card Number related to a Data Incident.

Covered Party means any or all of Merchant's employees, agents, representatives, subcontractors, Processors, service providers, providers of Merchant's point-of-sale equipment or systems or payment processing solutions, and any other party to whom Merchant may provide Card Member Information access.

Data Incident – An incident involving at least one Card Number in which there is (i) unauthorized access or use of encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) that are stored, processed, or transmitted on a Merchant's equipment, systems, and/or networks (or the components thereof); (ii) use of such encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) other than in accordance with the Merchant Agreement; and/or (iii) 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 (or a combination of each).

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

Merchant Level – The designation assigned to Merchants related to their PCI DSS compliance validation obligations, as described in Section 8.6, "Periodic Validation of Merchant Systems".

Payment Application – has the meaning given to it in the then Glossary of Terms for Payment Card Industry Payment Application Data Security Standard, which is available at https://www.pcisecuritystandards.org.

PCI-Approved – 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 https://www.pcisecuritystandards.org.

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

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

Qualified Security Assessors (QSAs) – Entities that have been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to the Payment Card Industry Data Security Standard. See Section 8.6, "Periodic Validation of Merchant Systems".

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

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

Validation Documentation – Documents to be provided by Merchants under Section 8.6, "Periodic Validation of Merchant Systems".

8.3 Standards for Protection of Cardholder Data and Sensitive Authentication Data

Merchant must, and Merchant must cause Merchant's Covered Parties, to:

- store Cardholder Data only to facilitate Transactions in accordance with, and as required by, the Merchant Agreement.
- comply with the current version of the Payment Card Industry Data Security Standard ("PCI DSS"), which is available at www.pcisecuritystandards.org, no later than the effective date for implementing that version.
- use, when deploying new or replacement PIN Entry Devices or Payment Applications (or both), only those that are PCI-Approved.

Merchant must protect all Charge Records and Credit Records retained pursuant to the Merchant Agreement in accordance with these data security provisions; Merchant must use these records only for purposes of the Merchant Agreement and safeguard them accordingly. Merchant is financially and otherwise liable to Merchant Services Provider for ensuring Merchant's Covered Parties' compliance with this Chapter 8, "Protecting Card Member Information" (other than for demonstrating Merchant's Covered Parties' compliance with this policy under Section 8.6, "Periodic Validation of Merchant Systems").

8.4 Data Incident Management Obligations

Merchant must notify its Merchant Services Provider immediately and in no case later than twenty-four (24) hours after discovery of a Data Incident.

Merchant must conduct a thorough forensic investigation of each Data Incident. For Data Incidents involving 10,000 or more unique Card Numbers (or otherwise at Merchant Services Provider's request), a PCI Forensic Investigator (PFI) must conduct this investigation. Merchant must promptly provide to its Merchant Services Provider all Compromised Card Numbers and the forensic investigation report of the Data Incident. Merchant must work with its Merchant Services Provider to rectify any issues arising from the Data Incident, including consulting with the Merchant Services Provider about Merchant's communications to Card Members affected by the Data Incident and providing (and obtaining any waivers necessary to provide) to its Merchant Services Provider all relevant information to verify Merchant's ability to prevent future Data Incidents in a manner consistent with the Merchant Agreement.

Forensic investigation reports must include forensic reviews, reports on compliance, and all other information related to the Data Incident; identify the cause of the Data Incident; confirm whether or not Merchant was in compliance with the PCI DSS at the time of the Data Incident, and verify Merchant's ability to prevent future Data Incidents by providing a plan for remediating all PCI DSS deficiencies. Upon its Merchant Services Provider's request, Merchant shall provide validation by a Qualified Security Assessor (QSA) that the deficiencies have been remediated.

Notwithstanding any contrary confidentiality obligation in the Merchant Agreement, American Express has the right to disclose information about any Data Incident to Card Members, Issuers, other participants on the American Express Network, and the general public as required by Applicable Law; by judicial, administrative, or regulatory order, decree, subpoena, request, or

other process; in order to mitigate the risk of fraud or other harm; or otherwise to the extent appropriate to operate the American Express Network.

8.5 Reserved

8.6 Periodic Validation of Merchant Systems

Merchant must take steps to validate under PCI DSS annually and quarterly the status of Merchant's equipment, systems and/or networks (and their components) on which encryption keys, Cardholder Data or Sensitive Authentication Data (or a combination of each) are stored, processed or transmitted.

Step 1 – Enroll in a Compliance Program

Level 1 Merchants, Level 2 Merchants, those Level 3 Merchants whom American Express has designated (as described below), and Level EMV Merchants, as described below, must submit applicable periodic Validation Documentation to its Merchant Services Provider. Please contact your Merchant Services Provider for more information regarding its data security compliance requirements.

American Express may require certain Level 3 merchants to enroll in American Express' compliance program under this policy by sending them written notice. The designated Level 3 Merchant must enroll no later than ninety (90) days following receipt of the notice.

Step 2 – Determine Merchant Level and Validation Requirements

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

Merchant Level	Definition	Validation Documentation	Requirement
1	2.5 million Transactions or more per year; or any Merchant that American Express otherwise deems a Level 1 Merchant	annual on-site security assessment report and quarterly network scan	Mandatory
2	50,000 to 2.5 million Transactions per year	annual Self Assessment Questionnaire and quarterly network scan	Mandatory
3	Less than 50,000 Transactions per year	annual Self Assessment Questionnaire and quarterly network scan	Strongly recommended, except mandatory for designated Level 3 merchants*

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

Determine Merchant Level and the Validation Documentation to send to Merchant Services Provider.

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

Step 3 – Send the Validation Documentation to Merchant Services Provider

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

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

Compliance and validation are completed at Merchant's expense. By submitting Validation Documentation to its Merchant Services Provider, Merchant represents and warrants to its Merchant Services Provider that Merchant is authorized to disclose the information contained therein and is providing the Validation Documentation without violating any other party's rights.

8.6.1 Merchants Not Compliant with PCI DSS

If Merchant is not compliant with the PCI DSS, then Merchant must complete an AOC including "Part 4. Action Plan for Non-Compliant Status" and designate a remediation date, not to exceed twelve (12) months following the date of the AOC, for achieving compliance. Merchant must submit this AOC with "Action Plan for Non-Compliant Status" to its Merchant Services Provider. Merchant shall provide its Merchant Services Provider with periodic updates of Merchant's progress toward remediation under the "Action Plan for Non-Compliant Status."

8.6.2 Non-Validation Fees and Termination of Merchant Agreement

Merchant Services Provider has the right to impose non-validation fees on Merchant and terminate the Merchant Agreement if Merchant does not fulfill these requirements or fails to provide the mandatory Validation Documentation by the applicable deadline.

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

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

8.6.3 Periodic Validation of Level EMV Merchants

If Merchant meets certain criteria, its Merchant Level may be classified as EMV.

To be eligible for Merchant Level EMV, Merchant must submit 50,000 (or more) American Express Card Transactions per year, of which total Transactions at least seventy-five percent (75%) are made by the Card Member with the physical Card present at a Point of Sale System compliant with EMV Specifications and capable of processing contact and contactless transactions on a Chip-Enabled Device.

If Merchant is classified as Merchant Level EMV, Merchant may submit the Annual EMV Attestation (AEA) instead of other Validation Documentation.* The AEA involves a process using PCI DSS requirements that allows self-examination of Merchant's equipment, systems, and networks (and their components) where encryption keys, Cardholder Data or Sensitive Authentication Data (or a combination of each) are stored, processed or transmitted. It must be performed by Merchant and certified by Merchant's chief executive officer, chief financial officer, chief information security officer, or principal. Merchant must complete the process by submitting the AEA annually to its Merchant Services Provider. To fulfill validation obligations under this policy, the AEA must certify that Merchant meets the requirements for Merchant Level EMV.

* For the avoidance of doubt, if Merchant falls into Merchant Level 1 or 2 and is classified as Merchant Level EMV, Merchant needs to submit only the AEA, not the other Merchant Level 1 and 2 Validation Documentation set forth in the table in Section 8.6, “Periodic Validation of Merchant Systems”.

9. FRAUD PREVENTION

9.1 Introduction

This chapter of the Merchant Operating Guide offers fraud mitigation tips for both Card Present and Card Not Present Transactions.

9.2 Strategies for Deterring Fraud

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

Layers of Protection

Merchant's first layer for mitigating fraud is to follow American Express' Card acceptance policies and procedures, as outlined in Chapter 4, "Transaction Processing." Other fraud mitigation strategies that Merchant chooses to implement may include any combination of:

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

The implementation and use of the strategies and tools detailed in this chapter, however, does not guarantee that (i) the person making the Charge is the Card Member, (ii) the Charge is in fact valid or bona fide, (iii) Merchant will be paid for the Charge, or (iv) Merchant will not be subject to a Chargeback.

9.3 Card Acceptance Policies

A critical component in Merchant's overall fraud mitigation strategy is to follow American Express Card acceptance procedures, as defined in Chapter 4, "Transaction Processing". The procedures outlined in the "transaction processing" chapter are required under the Merchant Agreement and can also serve as a Merchant's first line of defense against potential fraud. The additional layers of fraud mitigation mentioned previously can supplement this line of defense.

9.4 Card Security Features

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

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

Merchants must look for the following:

1. Pre-printed Card Identification (CID) Numbers usually appear above the Card Number, on either the right or the left edge of the Card.

2. All American Express Card Numbers start with "37" or "34." The Card Number appears embossed on the front of the Card. Embossing must be clear, and uniform in sizing and spacing. Some Cards also have the Card Number printed on the back of the Card in the signature panel. These numbers, plus the last four digits printed on the Charge Record, must all match.

3. Do not accept a Card outside the Valid Dates.

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

5. Some Cards contain a holographic image on the front or back of the plastic to determine authenticity. Not all American Express Cards have a holographic image.

6. Some Cards have a Chip on which data is stored and used to conduct a Charge.

7. The signature on the back of the Card must match the Card Member's signature on the Charge Record, and must be the same name that appears on the front of the Card. The signature panel must not be taped over, mutilated, erased or painted over. Some Cards also have a three-digit Card Security Code (CSC) number printed on the signature panel.

   Note: The security features for Prepaid Cards and Travelers Cheques are listed in Section 9.7, “Prepaid Card Security Features” and Section 9.9, “Travelers Cheque and Gift Cheque Security Features”.

9.4.1 Compromised Card Security Features

Do not accept a Card if:

Altered Magnetic Stripe

- The Magnetic Stripe has been altered or destroyed.

- The Card Number on the front of the Card does not match the number printed on the back (when present), or the last four digits printed on the Charge Record (or both).

Altered Front of the Card

- The Card Number or Card Member name on the front of the Card appears out of line, crooked, or unevenly spaced.

- The ink on the raised Card Number or Card Member name is smudged or messy.

- The Card Number or Card Member name is not printed in the same typeface as the American Express typeface.

Altered Back of the Card

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

Altered Appearance of the Card

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

If your suspect Card misuse, follow your internal store policies, and, if directed to do so, call your Merchant Services Provider and state that you have a Code 10. **Merchants should never put themselves or their employees in unsafe situations, nor physically detain or harm the holder of the Card.**

Often, Merchant can look closely at Cards to determine if they're altered or counterfeit. As another layer in Merchant's internal fraud prevention program, educate all Merchant personnel on how to identify a potentially altered Card. For more information, visit American Express' website at: www.americanexpress.com/fraudinfo.

9.5 Recognizing Suspicious Activity

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

Suspicious Behavior

A suspicious situation may arise, causing a Merchant to question the authenticity of the Card, or the legitimacy of the person presenting it. Any single behavior may not be risky. However, when customers exhibit more than one of the following behaviors, Merchant's risk factor may increase:

- larger-than-normal Transaction dollar amounts,
- orders containing many of the same items,
- orders shipped to an address other than a billing address,

- orders using anonymous/free email domains,
- orders sent to postal codes or countries where Merchant shows a history of fraudulent claims,
- orders of a “hot” product (i.e., highly desirable goods for resale),
- customer is a first-time shopper,
- customer is purchasing large quantities of high-priced goods without regard to color, size, product feature, or price,
- customer comes in just before closing time and purchases a large quantity of goods,
- customer wants to rush or overnight the order,
- customer has a previous history of Disputed Charges,
- customer is rude or abusive toward Merchant; wanting to rush or distract Merchant,
- customer frequents Merchant to make small purchases with cash, then returns to make additional purchases of expensive items with a Card.

If you suspect Card misuse, follow your internal store policies, and, if directed to do so, call your Merchant Services Provider with a Code 10. **Merchants should never put themselves or their employees in unsafe situations, nor physically detain or harm the holder of the Card.**

9.6 Prepaid Card Security Features

Merchants are responsible for following all American Express’ Prepaid Card acceptance procedures in Section 4.20, “Processing Prepaid Cards”. Although there are a number of unique Prepaid Cards, all Prepaid Cards share similar features, except that:

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

1. The American Express logo generally appears in the bottom right corner.
2. The words PREPAID or INCENTIVE will generally be shown above the American Express logo.
3. Cards pre-loaded with funds may show the dollar amount or the total points (reloadable Cards generally will not show a number).
4. The CID Number will appear usually above the Card Number or above the logo.
5. The Card Number appears on the Card.
6. The Valid Date or Expiration Date appears on the Card.

7. The recipient's name or company name may appear on the Card; otherwise a generic "Recipient" or "Traveler" may appear, or this area might be blank.

9.7 Recognizing Suspicious Activity for Prepaid Cards

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

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

9.8 Travelers Cheque and Gift Cheque Security Features

Even though American Express’ Travelers Cheques and Gift Cheques offer more convenience and security, counterfeit products circulate worldwide. Merchant must verify all cheque products presented at Merchant’s Establishment and contact the Travelers Cheque/Gift Cheque Customer Service with questions or suspicions.

One of the easiest and most effective tests to determine authenticity is the smudge test:

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

For Travelers and Gift Cheque acceptance procedures, see Section 4.21, “Processing Travelers/Gift Cheques”. American Express also recommends that Merchant follows the procedures in the preceding Section 9.5, “Recognizing Suspicious Activity” to assist Merchant in the mitigation of fraud.

As another layer of protection, there are a number of security features inherent in American Express’ Travelers Cheque and Gift Cheque products.

9.9 Fraud Mitigation Tools

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

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

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

Failure to comply with all applicable sections of the Technical Specifications can impair or prevent Merchant's use of American Express' fraud mitigation tools.

9.10 Verification Services

American Express offers tools that help verify information provided by Merchant's customer for both Card Present Charges and Card Not Present Charges. These verification tools can be used in multiple layers simultaneously to help Merchants mitigate the risk of fraud, but are not a guarantee that (i) the person making the charge is the Card Member, (ii) the Charge is in fact valid or bona fide, (iii) Merchant will be paid for the Charge, or (iv) Merchant will not be subject to a Chargeback.

These verification services help mitigate the risk of fraud prior to the completion of a purchase by comparing information provided by the customer at the point of sale with information on file with the Issuer. The response from the Issuer only indicates the validity of and/or discrepancies in the information Merchant provided for the customer. Although the Authorization may have been approved, Merchants can decide whether to submit the Charge based on the verification response and its' internal policies.

Prepaid Cards do not always require a Card Member to provide an address to the Issuer. For these Charges Merchants may receive an "Information Unavailable" response. Merchant should apply its existing policies for handling online purchases that receive an "Information Unavailable" response.

9.11 Electronic Verification Services

Electronic verification services offer a cost effective way to help mitigate the risk of fraud at the point of sale. These services allow Merchants to compare information provided by the customer with information about the Card Member not available on the Card, thereby allowing Merchants to make a more informed decision about the validity of the Charge prior to completion of the purchase.

Electronic verification can be used:

- when processing Authorizations in real time and/or when combining Authorizations and submitting all at once,
- to help identify high-risk Charges, and
- with or in the case of some verification tools, without an Authorization request.

9.11.1 Card Identification (CID) Verification

Description

The Card Identification (CID) Verification tool helps mitigate fraud on keyed and swiped Charges. The CID Number is associated with each individual Card. Merchants request the four-digit CID Number printed on the Card from the customer at the time of purchase and then submit the CID Number with the Authorization request. Verification of the CID Number is one method to authenticate whether an individual making a purchase has possession of the Card.

CID

The CID Number must not be stored after Authorization even if it has been encrypted. See Section 8.3, “Standards for Protection of Card Member Information” for additional information. Merchants to utilize the CID Verification tool for In-Person Charges may also qualify for the Keyed No Imprint Program. See Section 4.14, “Keyed No Imprint Program”.

Training is recommended to minimize incorrect entries of the CID Number. Training materials are available for sales and/or telephone order representatives. To obtain these materials, see American Express’ website at: www.americanexpress.com/fraudinfo.

10. RISK MANAGEMENT

10.1 Reserved

10.2 Prohibited Merchants

Any violation of the terms of the Merchant Agreement, including requirements specific to American Express card acceptance, are grounds for termination of American Express Card acceptance.

Additionally, American Express may cancel or disentitle Card acceptance if:

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

Business type	Description
Adult entertainment	Internet adult digital content sites.
Check cashing/guarantee and Bureau de Change Merchants	Card Member cashes a check using the Card as a check guarantee.
Child pornography	Any written or visual depiction of a minor engaged in obscene or sexually explicit conduct.
Debt collection	Collection agencies, payday lenders, factoring companies, liquidators, bailiffs, bail bondsmen, credit restoration services and bankruptcy lawyers. *Exceptions: outside agency collection fees and bail bondsmen fees (i.e., Merchant must not accept Cards to pay for a bail bond but Merchant may accept the Card to pay the fee to the bail bondsman. Merchant must not accept Cards to pay the amount of a Card Member's collection debt, but Merchant may accept the Card to pay the fee to the collection agency).*
Door-to-door sales	Unsolicited vendors where payment is rendered on the spot.
Escort services and massage parlors	Payment of potentially sexually related services. *Exceptions: licensed massage therapists.*

Financial services	Banks, credit unions, savings and loans associations, equities (defined as an instrument that signifies an ownership position, or equity, in a corporation, and represents a claim on its proportionate share in the corporation's assets and profits, e.g., stocks, bonds, and securities), unit trusts, mutual funds, foreign exchange, Bureau de Change, and payday lenders. *Exceptions: taxation, brokerage fees, leasing merchants, mortgage payments, condo down payments and financial advisor fees.*
Future services	Merchants that provide investment on future maturity goods/services (greater than four (4) months for delivery) with an intention of gaining return on investment (e.g., wines/spirits or timber investment). *Exceptions: travel related services, membership services (e.g., magazine subscriptions), ticket sales to future events or real estate deposits*.
Gambling	Casino chips, bookmaker, federal, state and local lotteries, bingo, internet gambling and casino sites. *Exceptions: lodging, restaurant, bar or gift shop facilities within a casino complex*.
Marijuana dispensaries	Sellers of marijuana, whether sold for recreational or medicinal purposes.
Multi-level pyramid sales	Multi-level marketing system using one or more of the following practices: • Participants pay for the right to receive compensation for recruiting new participants. • Participants are required to buy a specific quantity of products, other than at cost, for the purpose of advertising before participants are allowed to join the plan or advance within the plan. • Participants are sold unreasonable quantities of the product or products (also known as inventory loading). • Participants are not allowed to return products on reasonable commercial terms.
Prostitution	Payment for sexual services.
Timeshares	Selling partial ownership of a property for use as a holiday home, whereby a Card Member can buy the rights to use the property for the same fixed period annually.

Mixed Business

If any segment of Merchant's Charge volume is submitted from the aforementioned business types, Merchant must not accept the Card for those Transactions. If Merchant accepts the Card for these Transactions, Merchant may be subject to a Chargeback. Merchant may also be placed in one of American Express' Chargeback programs or cancelled (or disentitled) for Card acceptance (or both).

10.3 High Risk Merchants

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

If American Express determines, in American Express' sole discretion, that Merchant meets the criteria for one or more of the High Risk Merchant categories, American Express may place Merchant in a Chargeback program and/or request termination of Card acceptance.

American Express considers a Merchant to be "high risk" if Merchant meets at least one criteria in the following table:*

Category	Description
High risk industry	A Merchant whose type of business has had historically high occurrences of fraud and Disputed Charges with American Express or as compared to other similarly situated Merchants (or both). Examples of high risk industries include: internet electronic services, nightclubs/lounges, Customer Activated Terminals (CATs).
Performance	A Merchant whose recent high occurrences of fraud present an excessive risk to American Express. These Merchants have high occurrences of fraud and/or high fraud amounts for a number of consecutive months.
Cancelled derogatory	A Merchant whose Merchant Agreement was cancelled due to unsatisfactory activity.
Fictitious	A Merchant that accepts Cards fraudulently.
Prohibited	A Merchant is not eligible to accept the Card on the American Express Network. For prohibited criteria see Section 10.2, "Prohibited Merchants".

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

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

If it is determined or there is reason to believe, in American Express' sole discretion, that a Merchant engages or has engaged (or knowingly participates or knowingly has participated) in any of the activities listed in the following table; in any scheme that defrauds American Express, Issuers, and/or Card Members; or in business practices that American Express deems illegal, an illegal, fraudulent, deceptive, unfair or abusive, American Express may take corrective action which may include, but is not limited to:

- placement in American Express' Chargeback programs
- exercising Chargeback, rejecting Charges or withholding Settlements, or
- request termination of the Merchant Agreement (including immediate termination without prior notice to Merchant) or disentitlement of Card acceptance through Merchant's Merchant Services Provider.

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

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

A Merchant may be assessed non-compliance fees if American Express determines or has reason to believe, in American Express' sole discretion, that a Merchant engages or has engaged (or knowingly participates or knowingly has participated) in any of the activities listed in the table in Section 10.4, "Fraudulent, Deceptive, or Unfair Business Practices, Illegal Activities, or Prohibited Uses of the Card" in any scheme that defrauds American Express, Issuers, and/or Card Members; or in business practices that are deemed fraudulent, deceptive and/or unfair.

11. DISPUTED CHARGES, CHARGEBACKS AND INQUIRIES

Occasionally, Card Members question a Charge appearing on their billing statement. For example:

- Card Member may not recognize a Charge and requests additional information about it.
- Card Member is billed for goods or services not yet received.

If a Card Member disputes a Charge, American Express opens a case. American Express may also open cases when Issuers or the Network initiates disputes.

11.1 Disputed Charge Process

With respect to a Disputed Charge:

- A Merchant may receive an Inquiry from their Merchant Services Provider prior to exercising Chargeback, or
- Prior to receiving an Inquiry, a Merchant may receive a Chargeback from their Merchant Services Provider if it is determines that sufficient information is available to resolve the Disputed Charge in favor of the Card Member.

American Express has Chargeback rights:

- whenever Card Members bring Disputed Charges, as described in this chapter, or have rights under Applicable Law or contract to withhold payments,
- in cases of actual or alleged fraud relating to Charges,
- if a Merchant does not comply with the Merchant Agreement (including omitting any Transaction Data from Charge Submissions), even if American Express had notice when the Merchant was paid for a Charge that Merchant did not so comply and even if such Merchant obtained Authorization for the Charge in question, or
- as provided elsewhere in the Merchant Agreement

None of these actions affect procedures under any Chargeback programs in which a Merchant has been placed.

12. SPECIFIC INDUSTRIES

12.1 Introduction

This chapter states additional policies and procedures applicable to Merchants classified in specific industries that may or may not be applicable under the Merchant Agreement. All other provisions and requirements of the Merchant Agreement apply to these Merchants as well. To the extent possible, the provisions of this Chapter 12 and the other provisions of the Merchant Operating Guide shall be interpreted to give each their full effect. However, if a conflict is deemed to exist between them, then the provisions of this Chapter 12 shall govern.

12.2 Auto dealers

This section applies to Merchants classified in an auto dealer industry.

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

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

- Merchant must not submit a Charge for the down payment price of a used motor vehicle unless and until Merchant have a written agreement/bill of sale signed by the Card Member setting forth the terms of the sale, including down payment price, and Merchant's cancellation policy.
- In addition to American Express' other Chargeback rights, American Express also has Chargeback rights for any portion of the Charge for the down payment price of a used motor vehicle which is disputed by the Card Member, if such Disputed Charge cannot be resolved in Merchant's favor based upon unambiguous language contained in the written agreement/bill of sale.
- Should a Card Member exercise his or her right to rescind the written agreement/bill of sale during any rescission period set forth in the Card Member's agreement with Merchant or at law, Merchant shall submit a Credit to American Express promptly.
- If American Express has classified Merchant as an auto dealer of used motor vehicles exclusively, the down payment must not exceed 50% of the full purchase price of the motor vehicle.
- If the Card Member denies making or authorizing the Charge, American Express will have Chargeback rights for such Charge in addition to American Express' other Chargeback rights (see If the Card Member denies making or authorizing the Charge, American Express will have Chargeback rights for such Charge in addition to American Express' other Chargeback rights (see Chapter 11, "Disputed Charges, Chargeback and Inquiries ").

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

- Merchant is classified as an auto dealer of new or new and used motor vehicles (i.e., Merchant's dealership sells new motor vehicles exclusively or both new and used motor vehicles).
- The amount of the Charge does not exceed the total price of the motor vehicle after deduction of applicable discounts, taxes, rebates, cash down payments, and trade-in values.
- Merchant must not submit a Charge for the entire purchase price of a new or used motor vehicle unless and until Merchant have a written agreement/bill of sale signed by the Card Member setting forth the terms of the sale, including purchase price, delivery date and Merchant's cancellation policy.
- In addition to other Chargeback rights, American Express also has Chargeback rights for any portion of the Charge for the entire purchase price of a new or used motor vehicle which is disputed by the Card Member, if such Disputed Charge cannot be resolved in Merchant's favor based upon unambiguous language contained in the written agreement/bill of sale.
- Should a Card Member exercise his or her right to rescind the written agreement/bill of sale during any rescission period set forth in the Card Member's agreement with Merchant or at law, Merchant shall submit a Credit to American Express promptly.
- If the Card Member denies making or authorizing the Charge and Merchant have not transferred title or physical possession of the motor vehicle to the Card Member, American Express will have Chargeback rights for such Charge in addition to its other Chargeback rights.

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

If Merchant is classified in the business-to-business (B2B) or wholesale distribution industries, and American Express determine that Merchant is not in the Telecommunications industry, then notwithstanding the prohibition in Section 3.3, "Prohibited Uses of the Card", Merchant may accept the Card for overdue amounts to the extent that acceptance of overdue amounts is a common practice in Merchant's industry and does not constitute an attempt to obtain payment from the Card Member whose prior methods of payment have, in American Express' reasonable judgment, been difficult to collect or uncollectible. An indicator of such difficulty, for example, may be the fact that Merchant has sent an overdue customer account to collections.

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

To minimize Merchant's risk of a Chargeback with B2B Charges, always:

- obtain a signature for all In-Person Charges. For Card Not Present Charges, obtain Proof of Delivery, and
- maintain clear and accurate records of orders and returns.

Notwithstanding the restriction in Section 6.4, "Submission Requirements - Electronic", Merchant must not submit any Charge until the goods have been shipped or services have been provided to the Card Member. To the extent that Merchant have clearly disclosed Merchant's intentions to the Card Member and the Card Member agrees, then Merchant may submit the following types of Charges to American Express before Merchant ships the goods to the Card Member:

- Charges representing deposits on custom and special orders (so long as Merchant comply with Applicable Law) or goods not in inventory at the time the order is placed.
- Charges representing advance, partial, or full payment for goods that the Card Member requests Merchant to ship at a later date.

12.4 Insurance

This section contains provisions specific to Establishments that are classified in the insurance industry. If any of Merchant's goods or services are sold or billed by independent Agencies, then Merchant must provide to American Express a list of such independent Agencies and notify American Express of any subsequent changes in the list.

American Express may use this list to conduct mailings that encourage such independent Agencies to accept the Card. American Express may mention Merchant's name in such mailings, and Merchant must provide American Express with a letter of endorsement or assistance as American Express may require.

Merchant must use Merchant's best efforts to encourage independent Agencies to accept the Card. American Express acknowledges that Merchant has no control over such independent Agencies. From time to time, and subject to Chapter 3, "Card Acceptance", American Express may establish joint marketing campaigns that promote Card acceptance specifically at Merchant's Establishments or, generally, at insurance companies. A necessary purpose for which Merchant submit Card Member Information that is responsive to such joint marketing campaigns includes American Express' use of that information to perform back-end analyses to determine the success of such joint marketing campaigns.

American Express undertakes no responsibility on Merchant's behalf for the collection or timely remittance of premiums. American Express will not be subject to any liability, under any circumstances, for any claim arising from, or related to, any insurance policy issued by Merchant or Merchant's Agencies. Merchant and its Merchant Services Provider must indemnify, defend, and hold harmless American Express and American Express' Affiliates, successors, assigns, and Issuers, from and against all damages, liabilities, losses, costs, and expenses, including legal fees, to Card Members (or former Card Members) arising or alleged to have arisen from Merchant's or Merchant's Agencies termination or other action regarding their insurance coverage; breach, negligent or wrongful act or omission; failure to perform under the Merchant Agreement; or failure in the provision of Merchant's or their goods or services.

If the Card is accepted as payment for fixed rate cash value life insurance policies or fixed rate annuities under the Merchant Agreement, Merchant represents and warrant to its Merchant Services Provider that the fixed rate cash value life insurance policies and fixed rate annuities for which the Card will be accepted for premium payments are not securities requiring registration under the Securities Act of 1933, and, in addition to Merchant's other indemnification obligations to American Express, Merchant must further indemnify, defend, and hold harmless American Express and American Express' Affiliates, successors, assigns and Issuers from and against all damages, liabilities, losses, costs, and expenses, including legal fees, arising or alleged to have arisen from Merchant's and/or its Merchant Services Provider's breach of this representation and warranty.

12.5 Oil/Petroleum

If Merchant is classified in the oil and petroleum industry, American Express may place Merchant in the Fraud Full Recourse Program if Merchant accepts Charges originating at a Customer Activated Terminal (CAT) gas pump. American Express will not exercise Chargeback up to a certain dollar amount for Charges that qualify under the Oil Fraud Protection Program (see Section 12.6, "Oil Fraud Protection Program". For information about Customer Activated Terminals, see Section 4.3, "Customer Activated Terminals".

12.5.1 Oil/Petroleum Requirements

Merchant must:

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

12.5.2 Oil/Petroleum Recommendations

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

American Express recommends that Merchant:

- Set a pre-Authorization request of $100 at Merchant's CAT gas pumps.
- For higher Charges such as diesel, adjust the pre-Authorization amount to accommodate the higher Charges.
- Set Merchant's CAT gas pumps to shut off when they reach the pre-Authorization amount.
- Request a separate Authorization for purchases that exceed the original pre-Authorization amount.

12.6 Oil Fraud Protection Program

The Oil Fraud Protection Program addresses counterfeit fraud Chargebacks at fuel pump Customer Activated Terminals (CATs). Under this program, American Express will not exercise Chargeback for the amount of the Charge up to $100 provided that both the Establishment and each Charge meet the following criteria:

- the Authorization request meets the data requirements listed in Section 4.3, "Customer Activated Terminals",
- the Authorization request must include the correct Merchant Category Code (MCC) for "automated fuel dispensers" (5542),
- the Issuer determines that the Card used to initiate the Charge was counterfeit, and
- the Establishment qualified for Chargeback protection under the program at the time of the Charge, as follows:

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

American Express offers a variety of fraud prevention tools which may enable Merchants to reduce fraud in order to qualify and retain eligibility for the program. See Chapter 9, "Fraud Prevention" for more details.

12.7 Restaurants

If Merchant is classified in the restaurant or bar industry, then the following Authorization procedures apply. If the final restaurant or bar Charge is no greater than the amount for which Merchant obtained Authorization plus 20% of that amount, no further Authorization is necessary. If the final restaurant or bar Charge is greater than the amount for which Merchant obtained Authorization by more than 20%, Merchant must obtain Authorization for any additional amount of the Charge that is greater than the original Authorization. When submitting the Charge, only include the initial Approval.

See Section 4.5, "Charge Records" for additional information on paying a single bill with multiple Cards.

12.8 Telecommunications

If American Express classifies Merchant in the Telecommunications industry, notwithstanding anything to the contrary in the Merchant Agreement, American Express may place Merchant in one or more of the following Chargeback programs:

- Partial Immediate Chargeback Program for an amount of $50 or less; or
- Fraud Full Recourse Program

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

12.9 Government/Utilities/Education

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

Customers should feel free to use all forms of payment that Merchants accept without being penalized for choosing a particular form of payment. To promote consumer choice, Merchants are generally prohibited from imposing any restrictions, conditions, or disadvantages when the Card is accepted that are not imposed equally on all Other Payment Products. See Section 3.2, "Treatment of the American Express Brand". Merchants in these specific industries may assess convenience fees on Charges, provided that they comply with the other requirements of this section, as follows:

- Merchant must not impose a higher convenience fee on Charges than it imposes on Other Payment Products, except for automated clearing house funds transfers, cash, and checks. American Express views discrimination against Card Members as a breach of the Merchant Agreement.
- Merchants classified as government Entities, including government utilities, and privately owned utilities may assess convenience fees on all Charges.

- Merchants classified as educational institutions may assess convenience fees only on Charges for tuition, room and board, school lunch payments or other mandatory fees.
- Merchant must clearly disclose the amount of convenience fees to the customer and give the customer the opportunity to cancel the Charge if the customer does not want to pay the convenience fee.
- Any explanation, verbal or written, describing why the convenience fee is being assessed, or how it is calculated, must characterize the convenience fee as an assessment to cover the Merchant's administrative costs and not as an assessment to cover the Merchant's cost of accepting the Card.
- Charges relating to the payment of obligations made to, or goods or services purchased from, the Merchant and the convenience fee must appear as two separate Charges on the Card Member's statement. Merchants must obtain separate Authorizations and Approval codes for each of the principal Charge and the convenience fee. Furthermore, the descriptor on the convenience fee must clearly state that it is a convenience fee (e.g., *Official Payments – City of X* (principal payment) and *Official Payments Convenience Fee* (convenience fee)).

Merchant's third-party service provider can only assess a convenience fee when it accepts the Card for the foregoing Charges in compliance with the requirements of this section.

12.10 Internet/Online Pharmacies

If it is determined that Merchant is an internet/online pharmacy Merchant that accepts the Card for sales of prescription medications (as defined by Applicable Law) in the Card Not Present environment:

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

Upon request, Merchant or its Merchant Services Provider must promptly provide documentation that Merchant fulfills the foregoing requirements. Failure to provide this documentation promptly may result in suspension or disentitlement of Card acceptance privileges.

Specific procedures exist for Transaction processing by internet/online Merchants. These procedures appear in Section 4.4, "Processing a Card Not Present Charge".

12.11 Online/mail order tobacco retail

If Merchant is classified or it is otherwise determined that Merchant is an online or mail order (or both) tobacco or e-cigarette Merchant, then Merchant must provide the website address of the online store from which Merchant sell Merchant's tobacco products. If Merchant's website facilitates tobacco sales, Merchant will be required on request to provide an executed and notarized Affidavit of Compliance with Laws - Online/Mail Order Tobacco. If Merchant fails to complete the Affidavit, Card Acceptance privileges may be suspended. American Express may monitor Merchant's website.

Merchant Operating Guide Glossary

Advance Payment Charge means a Charge for which full payment is made in advance of Merchant providing the goods and/or rendering the services to the Card Member.

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

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

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

American Express means American Express Travel Related Services Company, Inc., a New York corporation.

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

American Express Card or Cards means (i) Any card, account access device, or payment device or service bearing American Express or American Express Affiliates' Marks and issued by an Issuer or (ii) a Card Number.

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

Annual EMV Attestation (AEA) means a declaration of the status of Merchant's compliance with the PCI DSS.

Applicable Law means (i) any law, statute, regulation, ordinance, or subordinate legislation in force from time to time to which Merchant or its Merchant Services Provider is subject, (ii) the common law as applicable to them from time to time, (iii) any court order, 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.

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

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

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

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

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

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

Batch means a group of Transactions, submitted to American Express, usually on a daily basis.

Card - See American Express Card or Cards.

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

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

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

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

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

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

Card Member means an individual or Entity (i) that has entered into an agreement establishing a Card account with an Issuer or (ii) whose name appears on the Card.

Card Member Information means any information about Card Members and Transactions, including, but not limited to, Transaction Data, and Card Member name, addresses, Card Numbers, and Card Identification (CIDs) Numbers.

Charge means a payment or purchase made on the Card.

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

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

Chargeback - When used as a verb, means (i) American Express' reimbursement from Merchant for the amount of a Charge subject to such right, or (ii) American Express' reversal of a Charge for which American Express have not paid Merchant; when used as a noun, means the amount of a Charge subject to reimbursement from Merchant or reversal. (Chargeback is sometimes called "full recourse" or "Full Recourse" in American Express' materials).

Chip means an integrated microchip embedded on a Card containing Card Member 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 Card Member or account information contained in the Chip, or both, (sometimes called a "smart Card", an "EMV Card", or an "ICC" or "integrated circuit Card" in American Express' materials).

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

Code 10 means a phrase that Merchant provides to an American Express representative to alert them of a possible suspicious Card and/or Transaction. Code 10 situations usually occur during Authorization.

Collusion means any Transaction, activity or agreement conducted by a Merchant or its agent with another party, including another Merchant or a Card Member, that the Merchant knew or should have known was not legitimate, or carried out in violation of Chapter 10, "Risk Evaluation".

Compromised Card Number means a Card Number related to a Data Incident.

Covered Parties means any or all of Merchant's employees, agents, representatives, subcontractors, Processors, service providers, providers of Merchant's Point of Sale Systems or payment processing solutions, and any other party to whom Merchant may provide Card Member Information access in accordance with the Merchant Agreement.

Credit means the amount of the Charge that you refund to Card Members for purchases or payments made on the Card.

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

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

Data Incident means an incident involving at least one Card Number in which there is (i) unauthorized access or use of encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) that are stored, processed, or transmitted on a Merchant's equipment, systems, and/or networks (or the components thereof); (ii) use of such encryption keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) other than in accordance with the Merchant Agreement; and/or (iii) 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 (or a combination of each).

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

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

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

EMV Specifications means the specifications issued by EMVCo, LLC, which are available at http://www.emvco.com.

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

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

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

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

Fraud Full Recourse Program is one of American Express' Chargeback programs.

Gift Card means a Prepaid Card with limited funds and that is marked "Gift" or "Gift Card" on the front of the Card.

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

Immediate Chargeback Program is one of American Express' Chargeback programs.

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

Inquiry is American Express' request for information about a Disputed Charge.

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

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

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

Keyed No Imprint Program is a program that allows a Merchant to submit In-Person Charges without an imprint of the Card. See Section 4.14, “Keyed No Imprint Program” for additional information.

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

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

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

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

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

Merchant Data Security Requirements means the American Express data security policy, as described in Chapter 8, “Protecting Card Member Information,” of the *Merchant Operating Guide*.

Merchant Level means the designation American Express assigns Merchants related to PCI DSS compliance validation obligations, as described in Section 8.6, “Periodic Validation of Merchant Systems”.

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

Merchant Services Provider means any Entity with which Merchant receives merchant processing services. These services may include, but are not limited to, processing transactions, facilitating authorizations on purchases, and capturing data, merchant accounting, backroom operations (e.g., chargebacks and detecting fraud), provision of point of sale equipment, solutions, or systems, sales, or customer service.

Network - See American Express Network or Network.

No Signature Program means a program that allows an Establishment to not request a signature from Card Members. See Section 4.15, “No Signature Program” for additional information.

Oil Fraud Protection Program is American Express’ program providing Establishments in the oil/petroleum industry protection from counterfeit fraud Chargebacks, provided both the Establishment and Charge meet certain criteria. See subsection 12.6, “Oil Fraud Protection Program” for additional information.

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

Partial Immediate Chargeback Program is one of American Express' Chargeback programs.

Payment Application has the meaning given to it in the then Glossary of Terms for Payment Card Industry Payment Application Data Security Standard, which is available at https://www.pcisecuritystandards.org.

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

PCI-Approved means 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 https://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.

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

PIN Entry Device has the meaning given to it in the then current Glossary of Terms for the Payment Card Industry PIN Transaction Security Requirements, which is available at https://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 Authorizations or to collect Transaction Data, or both.

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

Processor means a service provider to Merchants who facilitates Authorization and Submission processing to the Network (sometimes referred to as an "Authorized Gateway Provider") in American Express' materials.

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

Qualified Security Assessors (QSAs) are Entities that have been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to the Payment Card Industry Data Security Standard. See Section 8.6, "Periodic Validation of Merchant Systems".

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

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

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

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 in the then current Glossary of Terms for the PCI DSS.

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

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

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

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

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

Telecommunications means the communication services, including personal communication services; cellular, paging, long distance, etc. See Section 12.8, "Telecommunications" for additional information.

Terminal Provider means the Processor, vendor or company that provides Merchant's POS System.

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

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

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

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

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

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

Validation Documentation are the documents to be provided by Merchants under the Merchant Data Security Requirements described in Chapter 8.

Voice Authorization means the Authorization of a Charge obtained by calling the American Express Authorization Department.

Appendix D
Information Protection Contract Requirements

Participant shall comply, and cause Covered Parties to comply, with all of the provisions of the Information Protection Contract Requirements ("**IPCR**").

1) **Definitions**. For the purposes of this IPCR:

a) **"Agreement"** means [*insert master agreement name and contract number*] to which the IPCR is attached.

b) **"Amexco" or "AXP"** means the American Express entity or entities executing the Agreement and/or any Statement of Work thereunder.

c) "**Amexco Data**" means any Amexco confidential information as defined in the Agreement, including any adaptations, derivative works and translations, in any media or form, in whole or in part, and in addition, regardless of whether it constitutes confidential information as defined in the Agreement, any Personal Data, in each case, in any form, format or media whatsoever, including electronic and paper records, and including text, image, audio and video formats, that Participant receives access to in connection with the Agreement (other than Participant's Personal Data or any other data owned by the Participant as specifically set forth in the Agreement).

d) "**Applicable Law**", means all Applicable Laws, rules and regulations including all data protection, privacy, encryption and information security-related laws, rules and regulations and, where applicable, industry standards and other standards issued by self-regulatory organizations.

e) "**Including**", whether or not capitalized, means including without limitation.

f) **"Personal Data"** means any (i) individually identifiable information from or about an identified or identifiable individual in any form, format or media whatsoever, or any information that is combined with such individually identifiable information, including information that can be used to authenticate that individual or access an account, such as passwords or PINs, biometric data, recordings of individuals, unique identification numbers, answers to security questions, or (ii) information protected under Applicable Laws, such as, where applicable, "personal data" as defined by the European Data Protection Directive (95/46/EC).

g) "**Subcontractor**" means collectively and individually any third party authorized by Participant, including, any affiliate or subsidiary of the Participant, agent, representative, vendor, service provider, outsourcer, or the like, to which Participant discloses, or allows access to, Amexco Data in connection with this Agreement. Notwithstanding anything to the contrary herein, Subcontractors shall not disclose or allow access to any Amexco Data to any third party.

2) **Compliance**

Participant represents, warrants, and covenants that it (a) does and will comply with all Applicable Laws, and where applicable, industry standards (e.g. Payment Card Industry Data Security Standard (PCI DSS), ISO 22307 and ISO 27000)**;** and (b) has developed and implemented, and will maintain and monitor a written and comprehensive information security program in compliance with this IPCR and Applicable Laws**.** Upon request from time-to-time, Participant will certify its compliance with the foregoing.

3) **General**

a) All Amexco Data remains, at all times, the sole property of Amexco. Amexco reserves the right, where technically feasible and reasonable for the services provided as determined by Amexco, to require Participant to promptly change, update, delete, encrypt, truncate and/or mask any Amexco Data, in any manner, stored by Participant. Amexco Data or any portion thereof shall not be retained in any manner whatsoever, beyond the expiration or termination of the Agreement, except as required by Applicable Law and on prior notice to Amexco detailing the Applicable Law.

b) Prior to any storage media containing Amexco Data being assigned, allocated or reallocated to another user, or prior to such storage media being permanently removed from a facility, Participant will irreversibly delete such Amexco Data from both a physical and logical perspective, such that the media contains no residual data, or if necessary physically destroy such storage media such that it is impossible to recover any portion of data on the media that was destroyed. Participant shall maintain an auditable program implementing the disposal and destruction requirements set forth in this Section 3(b) for all storage media containing Amexco Data.

c) Unless otherwise instructed by Amexco, all Amexco Data must be (i) securely returned or (ii) properly and immediately disposed of in a secure manner that is reasonably designed to render the information permanently unreadable and not reconstructable into a usable format (i.e., in accordance with the then-current U.S. Department of Defense, or similar data destruction standard or CESG standards, as applicable). Any such return or disposal shall occur at such time that any such Amexco Data is no longer reasonably required to perform the services hereunder, but in any event, no later than upon completion of the relevant services. Upon request, Participant will certify that all such Amexco Data has been returned or disposed o in accordance with this IPCR.

d) Notwithstanding anything to the contrary herein, to the extent and for so long as Participant retains Amexco Data on any archival systems, back-up systems, data storage solutions, or any existing or future recordation medium whatsoever, Participant's obligations with respect to such Amexco Data shall survive in accordance with Section 11 below.

e) Participant shall establish and maintain administrative, technical, organizational and physical safeguards to protect the security, integrity, confidentiality and availability of Amexco Data, including to protect Amexco Data against any anticipated threats or hazards and to protect against any unauthorized or unlawful access to, use of, acquisition of or disclosure of Amexco Data, or any other compromise of Amexco Data.

f) Participant agrees to deploy applicable and necessary security patches to all systems that process, store or otherwise support the services described in the Agreement, including

operating system, open source, and application software, and the like, as quickly as reasonably possible.

g) Participant agrees to employ supported software (e.g., software under active maintenance, including operating system, open source, application software and/or the like) on any systems that process, store or otherwise support the services described in the Agreement.

h) Participant shall not access, acquire, use, process or disclose Amexco Data for any purpose other than the purpose stated in the Agreement.

i) Participant shall ensure each individual to whom Amexco Data is disclosed or made accessible will comply with and remain bound by Participant policies at least as protective of Amexco Data as those found in the Data Protection and Confidentiality Rules ("**DPCR**") attached hereto as **Exhibit A**. Each such individual shall be informed of and shall acknowledge their understanding of the security and data protection rules as stated in such Participant's policies by a tangible means and Participant, upon request, shall promptly provide to Amexco evidence of each individual's acknowledgement.

j) Amexco may provide Participant with test data that is approved for use in non-production environments. Participant agrees that no other Amexco Data will be used by or on behalf of Participant in non-production environments unless authorized by Amexco and then only if all data, as determined by Amexco, has been masked, aliased, truncated, scrambled, scrubbed, anonymized, obfuscated, deidentified or otherwise sanitized before replication to non-production systems, or the Amexco Data is in a secured and controlled environment with limited access and appropriate controls. Participant may not return this data to any production system.

k) Participant shall document the consequences for violations of Participant's data protection, information security, privacy and confidentiality-related policies.

4) **Indemnity**

a) Participant shall, at its own expense, defend, indemnify and hold harmless Amexco, its parent, and their respective employees, agents, subsidiaries, and affiliates, from and against any and all claims, suits, demands, actions, damages, losses, liabilities, proceedings, litigation, costs and expenses, including reasonable attorney's fees, relating to or arising out of this IPCR, including (i) the acts, omissions or obligations undertaken by Participant or Subcontractor pursuant to this IPCR, including any improper, unauthorized or unlawful access to, use or processing, acquisition of, or disclosure of Amexco Data, (ii) any misrepresentation or breach of warranty made by Participant herein, (iii) or any breach of this IPCR by Participant.

b) Amexco reserves the right to assume the exclusive defense and control of any matter otherwise subject to indemnification by Participant, and Participant shall fully cooperate with Amexco in asserting a defense. Participant shall pay Amexco's reasonable attorneys' fees and expenses incurred from any and all lawsuits or arbitrations brought against Participant by Amexco in connection with this IPCR.

5) **Security Records Retention**

Participant agrees to maintain and enforce retention policies for any and all reports, logs, audit trails and any other documentation that provides evidence of security, systems, and audit processes and procedures according to requirements mutually agreed upon by Amexco and Participant and in accordance with all Applicable Laws.

6) **Data Security Breach Notification**

In the event there is, or Participant reasonably believes that there is or was, any improper, unauthorized or unlawful access to, use of, acquisition of, or disclosure of Amexco Data or any other compromise of the security, confidentiality, privacy or integrity, of Amexco Data ("**Security Incident**"), Participant shall immediately notify Amexco by phone at for U.S.: 1-888-732-3750 or International: 1-602-537-3021 and in writing via email to: EIRP@aexp.com (send a secure email) of the Security Incident. Participant shall fully cooperate with Amexco to investigate and resolve any privacy, data protection, information security, integrity or confidentiality issues involving Amexco Data, including any Security Incident and/or notifications related thereto. Participant shall be responsible for all costs related to or arising from any Security Incident, including investigating the Security Incident and providing notification to all individuals affected by the Security Incident. Subject to Applicable Law, the Participant shall not make any public or other announcements or admissions of liability without the prior written consent of Amexco. Subject to Applicable Law, the provision of such notifications, if any, including the content, shall be solely at the discretion and direction of Amexco.

7) **Compliance Assessments and Inspections**

a) Participant shall document and, if requested by Amexco, promptly provide to Amexco, at a minimum, access to copies of all relevant Participant privacy, data protection, and information security and/or confidentiality-related policies, procedures and standards (including escalation procedures for non-compliance) for Amexco review.

b) Participant shall fully cooperate with Amexco in connection with any inspections, on-site or by phone, including inspections for privacy, data protection and information security compliance, and with self-assessment security compliance reviews. On-site inspections will be done by Amexco authorized representatives upon reasonable advance notice during regular business hours.

c) Upon Amexco's request, Participant shall promptly make available to Amexco copies of any third party data processing or information security, data protection and/or privacy-related assessment, test results, audit or review (e.g., SSAE 16, SOC I, II and III, SysTrust, WebTrust), or other equivalent evaluations in its possession or control.

d) If the services to be supplied by Participant will, at any time, include Participant hosting an Internet facing application and/or mobile application**,** Participant agrees to promptly perform and provide to Amexco a summary attestation from a vulnerability threat assessment ("**VTA**") test or such other testing, at minimum on an annual basis, demonstrating that the Internet facing application and/or mobile application has no material security vulnerabilities. The attestation report must include, at a minimum, a definition of how the vulnerabilities are rated (e.g., high / medium / low, serious / moderate / minimal) and evidence that the application has no open vulnerabilities at the highest rating and shows the number of vulnerabilities at any lower ratings. The VTA shall be performed by a vendor listed on the then current Amexco Chief Information Security Office (**"CISO"**) approved vendor list (which includes PCI Approved Scanning Vendors). Amexco reserves the right to review the detailed report from any such VTA at Amexco's sole discretion.

e) Participant agrees to allow Amexco to assess the manner in which Participant uses, stores, accesses, acquires or processes Amexco Data, subject to Participant's reasonable confidentiality and security precautions and procedures. Participant shall ensure that it has obtained sufficient permissions or consents that may be required under Applicable Law to ensure that Amexco is permitted to conduct such assessments. The purpose of such

assessments is to detect any improper, unlawful, or unauthorized access to, or use, acquisition, processing, or disclosure of Amexco Data. Amexco acknowledges and agrees that it will not be permitted to perform such an assessment if Participant can demonstrate that the assessment would: (i) cause Participant to be in breach of any Applicable Law, or Participant's internal data protection, information security, privacy and confidentiality-related policies or (ii) adversely impact or compromise any Amexco Data or third party customer data. In no event will the method of assessing such Participant's use, storage or processing of Amexco Data involve online access, or any other access, to Participant's systems, network, or infrastructure.

f) Participant shall remedy any issues identified under this Section 7 in a timely manner acceptable to Amexco.

8) **Security Administration**

a) Participant shall provide information security, data protection and privacy awareness training, utilizing either Amexco's or Participant's training course at Amexco's discretion, to all individuals authorized by Participant to have access to Amexco Data. The training shall be consistent with best practices in the financial services industry and designed, at a minimum, to educate all such individuals on maintaining the security, confidentiality, integrity and availability of Amexco Data, and shall occur before such individuals are allowed access to Amexco Data and no less than annually thereafter. Amexco reserves the right to review Participant's training and to require Participant to modify that training if Amexco deems this necessary.

b) Participant's assigned administrator(s) must retain sole responsibility for granting access to Amexco Data for all Participant employees and other users, and for providing a process by which employee and other user accounts shall be created and deleted in a secure and timely fashion. This process must include appropriate leadership approval, auditable history of all changes, and an annual review of access authorization and excess access remediation.

c) Participant shall establish, maintain and enforce the security access principles of "segregation of duties" and "least privilege" with respect to the Amexco Data hereunder. "Least Privilege" for this purpose of this Section 8(c) shall mean the minimum access required to perform a job function.

9) **Material Changes Affecting the Delivery of Services**

a) In the event Participant desires to materially modify the process, method or means by which Amexco Data is used, disclosed, accessed, acquired, stored, processed or otherwise transmitted or handled hereunder, or change the geographic location(s) where the Amexco Data is accessed, processed or stored, Participant shall provide Amexco at least ninety (90) days prior written notice. Amexco shall have the right, in its sole discretion, to determine if the modifications represent unacceptable risks to Amexco or Amexco Data and to prohibit Participant from implementing any such material modification to the service(s) supplied under the Agreement until such time as the risks can be mitigated to Amexco's reasonable satisfaction or an alternate source for the service(s) can be found. Examples of such material modifications include: (i) disclosing Amexco Data to a new Subcontractor, or (ii) rerouting Amexco Data flows.

b) As part of the provisioning of the service(s) contemplated under the Agreement, any material changes to the service(s), and/or any new service(s), Participant agrees to provide any requested information in connection with, and/or actively participate in, Amexco's security governance processes. If significant additional capital investment is required for Participant to comply with Amexco's security requirements or policies and standards, Participant and Amexco shall mutually agree upon the allocation of such expenses.

10) **Use of Sub-Vendors**

a) Participant shall take all necessary steps to cause Amexco to be deemed a third party beneficiary to all agreements between Participant and Subcontractors under Applicable Law, and shall provide copies of such agreements to Amexco upon request (redacted with respect to provisions unrelated to the IPCR obligations).

b) Participant (i) shall ensure each Subcontractor adheres to all of the terms hereunder; (ii) shall be liable for each Subcontractor's compliance hereto as if such Subcontractor were a party to this Agreement and any such non-compliance, action or omission were undertaken by the Participant under this Agreement; and, (iii) shall be responsible for all fees and costs related to each Subcontractor meeting all of Amexco's requirements hereunder, including any financial and/or security audits, inspections, and/or related security assessments during the term of the Agreement.

c) In the event that Participant has knowledge of a breach of the terms of the IPCR by a Subcontractor, Participant shall notify Amexco immediately. In the event Amexco determines that Subcontractor has violated the IPCR, Amexco reserves the right to require Participant to promptly cease and desist using the Subcontractor for any of the services described in the Agreement immediately and to require the Subcontractor to securely return or securely delete all Amexco Data from all of Subcontractor's systems immediately in accordance with Section 3(a) hereof. If requested by Amexco, Participant will confirm in writing to Amexco that all Amexco Data has been securely destroyed or permanently erased by the Subcontractor.

d) Amexco reserves the right to review Participant's due diligence processes performed on any Subcontractor and perform additional due diligence of its own on Subcontractor and/or Participant, including to ascertain whether the proposed changes contemplated to the service(s) meet Amexco security requirements. Participant shall implement in a timely manner at its own cost any commercially reasonable remedies required by Amexco hereunder.

11) **Survival Rights**

This IPCR and all provisions herein shall survive so long as Participant retains any Amexco Data. Notwithstanding the return or destruction of the Amexco Data, Sections 1, 2, 3(a), 4, 5, 6, 7, 10, and 11 shall survive indefinitely solely with respect to Participant's activities under the Agreement and the IPCR.

Exhibit A

Data Protection and Confidentiality Rules

The protection of confidential information and personal data is of utmost importance to American Express. Whenever you perform services or your other job duties that involve receipt of or access to confidential information, you must - at a minimum - comply with these Data Protection and Confidentiality Rules ("**DPCR"**).

In these rules, several words are capitalized; these words have particular meanings.

- Wherever we use the term "**Amexco**" or "**AXP**" we mean the entire American Express corporate family and third parties that have relationships with American Express; namely, American Express Travel Related Services Company, Inc., and its parent, subsidiaries, affiliates, as well as its and their consultants, contractors, joint ventures, licensees, franchisees, and Participants authorized to represent American Express' interests or to use or provide services related to your Job Duties.

- Wherever we use the capitalized term "**Job Duties**," we mean the services performed by and other job duties of the individuals covered by this DPCR.

- Wherever we use the capitalized term "**Personal Data**," we mean (i) individually identifiable information from or about an identified or identifiable individual in any form, format or media whatsoever, or any information that is combined with such individually identifiable information, including information that can be used to authenticate that individual or access an account, such as passwords or PINs, biometric data, recordings of individuals, unique identification numbers, answers to security questions, or (ii) information protected under Applicable Laws, such as, where applicable, "personal data" as defined by the European Data Protection Directive (95/46/EC).

- Finally, wherever we use the term "**Amexco Confidential Information**," we mean Amexco's and its customers' and clients' trade secrets, documents, data, information, systems, files, records, forms and any information used in the provision of Job Duties, including without limitation, Personal Data.

You SHALL:

1. Safeguard all Amexco Confidential Information;
2. Agree that any work product produced or developed in the performance of Job Duties for Amexco constitutes Amexco Confidential Information subject to this DPCR and the agreement between your employer and Amexco around ownership of intellectual property;
3. Always sign off of or lock with a password protected screensaver your workstation whenever you are not working on it, including, time away for breaks, lunch, meetings, etc.;
4. not disclose, share or allow the use by another person of your password, and if, nevertheless that happens resulting in errors or fraud, you shall be held accountable for such errors or fraud;
5. Understand that, except where prohibited by law, computer terminals are subject to monitoring and terminal monitoring may occur simultaneously with telephone monitoring;

6. Understand that all transactions in the system are recorded by the computer and that these recordings of any transactions by a personal identification number and password may be monitored at any time;
7. Help safeguard Customers' (and/or employees', as applicable) expectations of privacy by exercising diligence and care in the handling of Amexco Confidential Information relating to them; and
8. Understand that this DPCR and the rules contained herein are extremely important and any individual who willfully disregards these rules is subject to discipline.
9. Help to ensure that your colleagues and other individuals under your supervision comply with this DPCR.
10. Ensure systems are periodically evaluated to identify and address vulnerabilities.
11. Ensure necessary security patches are deployed to systems that process, store or otherwise support Amexco Confidential Information.
12. Ensure account passwords are strong and periodically changed for those accounts used to process, store or otherwise support Amexco Confidential information.

You <u>SHALL NOT</u>:

1. Use Amexco Confidential Information for your own benefit or the benefit of any third party, except to the extent necessary for the performance of your Job Duties;
2. Access Amexco Confidential Information unless required to as part of the performance of your Job Duties;
3. Access Amexco Confidential Information that does, or could contain any of the following types of information:
    - Your own account or related Amexco Confidential Information for any reason; or
    - An account or related Amexco Confidential Information if you personally know the account holder or customer in any way, whether from inside or outside of work.

    (Note: If you are ever required to access any of the above information as part of your Job Duties, you must promptly notify management <u>prior</u> to such access and provide any information necessary for management to determine if this is permissible);
4. Discuss Amexco Confidential Information in public places;
5. Reveal Amexco Confidential Information to any third party and/or to any individual except to the extent strictly necessary to perform your Job Duties;
6. Give your password to any person; or
7. Use another person's password or identification number.