

BANK OF AMERICA, N.A.
MERCHANT OPERATING GUIDE

Contents

1. Introduction	3
2. Card Networks.....	6
3. Accepting Card-Present Payments.....	10
4. Accepting Card-Not-Present Payments.....	20
5. Authorizations	24
6. Refunds and Exchanges.....	34
7. Data Security	38
8. Chargebacks, Retrievals and Other Debits or Adjustments.....	41
9. Settlement Procedures	48
10. Statements	49
11. Other Information.....	50
12. Definitions	51

OPERATING GUIDE

1. Introduction

1.1 Overview

- This Operating Guide forms part of your Agreement with us, and describes the procedures and methods for submitting Card Transactions for payment, obtaining Authorizations, responding to Chargebacks, and other aspects of the operations of the Merchant Services that we provide to you. Terms used in this Operating Guide but not defined have the meanings attributed to them in your Agreement.
- The Operating Guide seeks to provide you with a reference guide for accepting Card payments; however, you should consult the Card Network Rules for complete information and to ensure full compliance with them. They are designed to help you decrease your Chargeback liability and train your employees. (In the event we provide Authorization, processing or settlement services for transactions involving Cards other than Visa, Mastercard, Discover and American Express, you should also consult those independent Issuers' proprietary rules and regulations.)
- The requirements set forth in this Operating Guide will apply unless prohibited by law. You are responsible for following any additional or conflicting requirements imposed by your state or local jurisdiction. The Card Network Rules are made a part of your Agreement by this reference to them, and reference to your Agreement or the Terms and Conditions shall be deemed to include the Card Network Rules, unless stated otherwise. Capitalized terms not defined in your Agreement are defined in the applicable Card Network Rules.
- This Operating Guide references multiple payment types and methods of accepting payment. You may not have the capabilities or systems to accept all methods of payment referenced in this Operating Guide.
- Please note: notwithstanding anything in this Operating Guide to the contrary, you may be limited to accepting and processing only card present / in-person transactions; you may not be able to process *card-not-present* transactions.

This Operating Guide is designed to be used as a reference document and should be referred to if you have any questions on the acceptance of Card payments from your customers. Please review this Operating Guide in detail.

1.2 Contact Us

- If you have any questions on this Operating Guide or on the Merchant Services we provide to you, please visit bankofamerica.com/smallbusiness for Customer Service information.

Alternatively, please contact Customer Service at **888.BUSINESS (888.287.4637)**.

You may also write to us at:

Bank of America
P.O. Box 251118
Tampa, Florida 33622-5118

Please send any notifications that you are required to submit to us under this Operating Guide and/or in accordance with your Agreement to this address.

1.3 Your Information

Change in Your Legal Name or Business Structure

- You must call Customer Service or your Relationship Manager. Due to Form 1099-K reporting requirements, you must always report to us as soon as possible any change in your legal name and/or Taxpayer Identification Number ("TIN") information. **Failure to notify us in a**

timely manner of any change of this information may result in back-up withholding of your Settlement Funds or resulting issues with 1099-K reporting, for which we will not be liable or responsible.

Change in Company D/B/A Name, Address or Telephone/Fax Number, and website address

- To change your company or Location D/B/A name, address (or e-mail address) or telephone/ fax number, or website address please contact Customer Service for further instructions.

Change of Settlement Account Number

- If you change the Settlement Account in which you receive the deposits for your transactions, you must call Customer Service immediately to request the change. They will provide you with the documentation needed to initiate the update. Only an authorized representative of your business can update banking information. If you have direct relationships with any Card Networks such as American Express or Discover you are responsible for contacting them directly in order for those Card Networks to update your bank account information.

Change of Ownership

- If there is a change in ownership such as adding an owner or selling any portion of your business to another owner you must call Customer Service and request that this information be updated on your account.
- Entry into a loan or other agreement that may affect your Agreement with us.

Sale of Your Business

- In the event you sell any portion of your business it is important that you contact Customer Service so they can instruct you on the necessary procedures. In the event your business is sold, the new owner may need to submit an application to us so that any future liability is transferred to the new owner

Closing Your Business or Bankruptcy

- In the event you close or liquidate your business, it is important that you contact Customer Service so they can instruct you and ensure any billing is discontinued. You will still be responsible for any Chargebacks resulting from previous transactions when the business was open.
- Please notify us if you become party to a bankruptcy procedures.

Change in the Ways Cards are Accepted

- Please notify us in the event you change from a business that exclusively conducts *card-present* retail sales to one that accepts Card Transactions by mail, telephone or internet transactions, please notify us.

New Lines of Business, Products, or Services

- Please notify us in the event you add new lines of business that deliver goods and services that are different from when you originally applied for the Merchant Services or if you now offer products or services that are materially different than what you offered previously when you applied to receive the Merchant Services.

Changes in Billing Methodology

- In the event you change the way you bill Cardholders you need to notify us. This includes examples such as if you previously billed for the goods or services at the time of sale and now bill in installment, membership, recurring or subscription payments or now require a deposit for your products.

Changes in Card Processing Equipment

- In the event you change your equipment (for example, from a POS terminal to a third-party processing POS system) you need to notify us.
- You need to notify us if you discontinue use of some of your Merchant Equipment so that we can comply with the relevant security standards by deactivating terminal IDs.

Change of Information for Locations

- You must provide to us and keep current a list of all of your business Locations where you use the Merchant Services. You shall be liable to us under your Agreement for all Locations (including any failure of such Location to comply with any obligations applicable to you under your Agreement), without regard to whether such Locations are owned or leased by you.
- This list should state, for each Location:
 - (i) Physical address (no P.O. Box);
 - (ii) Mailing address;
 - (iii) Telephone number(s);
 - (iv) Fax number(s) (if any);
 - (v) Email address(es) (if any); and
 - (vi) Website.

You must update this list as changes to any of the categories of information listed above or changes to any of your Locations occur.

We retain the right to terminate your Agreement if you fail to notify us of any change to the information in your merchant profile.

Card Network Monitoring

- The Card Networks have established guidelines, merchant monitoring programs, and reports to track merchant activity, such as, but not limited to, excessive Credits, Chargebacks, reported fraud and increased deposit activity. In the event you exceed the guidelines, engage in practices that could circumvent such monitoring programs or submit suspicious transactions as identified by a Card Network or any related program or reports, you may be subject to: (i) operating procedure requirement modifications; (ii) Chargebacks and/or increased fees; (iii) settlement delay or withholding; (iv) termination of your Agreement; or (v) audit and imposition of fines.

2. Card Networks

2.1 Card Acceptance

- You may accept the Agreed Upon Card Types indicated in your Agreement and you will not seek Authorization for or submit a transaction of any other Card type until you receive notice from us that you are approved to accept such other Card type.
- Depending on your Agreement with us, the Agreed Upon Card Types may include the below Debit Networks:
 - (i) Accel;
 - (ii) AFFN;
 - (iii) Cualiance;
 - (iv) Interlink;
 - (v) Maestro;
 - (vi) Mastercard Debit ;
 - (vii) NYCE;
 - (viii) Pulse;
 - (ix) Shazam;
 - (x) Star;
 - (xi) Visa Debit (PIN Authenticated Visa debit); and
 - (xii) EBT.

EBT/SNAP (Electronic Benefits Transfer now known as “Supplemental Nutrition Assistance Program”)

- When carrying out your business, you may, depending on the products and services you offer, accept payment via EBT or SNAP Cards. Further information on this program is as below:
 - (i) SNAP is a program that provides food and other products for SNAP Cardholders.
 - (ii) To be qualified for a SNAP permit, your business must meet at least one of the following criteria:
 - a. Your business sells staple foods in the following four categories: (1) dairy; (2) breads, grains, and cereals; (3) fruits and vegetables; and (4) meat, fish, and poultry. At least two of these categories must include perishable foods; or
 - b. One or more staple foods account for over 50% of your gross retail sales.
 - (iii) You must be authorized by USDA Food and Nutrition Services in order to accept SNAP and provide benefits. Once registered you will receive a SNAP permit.
 - (iv) One the permit is received, you may be required to install either a special stand-alone terminal capable of accepting SNAP or an integrated terminal/system to enable acceptance.
 - (v) You will be paid by the SNAP program typically within two (2) Business Days.
 - (vi) Contact Customer Service to discuss enrolling in the program and the associated fees.
- You understand that if you do not, or no longer qualify for, the American Express OptBlue® Program Service for authorizing, processing and settling your American Express Card Transactions, your American Express Card Transaction will be settled (acquired) by American Express. American Express will provide you with its own agreement that governs those transactions. In this scenario, we may authorize your American Express Card Transactions, but the clearing and settlement process may be carried out by American Express, and all Chargebacks, fees and other payments may be payable by you to American Express.

Please be advised that you can modify the Card Networks and Debit Networks that are enabled for the processing of your Card Transactions by contacting Customer Service (e.g. if you do not intend to process American Express Card Transactions, you can opt out of this by contacting Customer Service).

Where we have approved your acceptance of American Express Cards and you submit American Express Card Transactions to us, by entering into your Agreement, you consent to our disclosure of your contact information (e.g. cellular telephone number, office address, etc.) to American Express for marketing purposes.

Please notify us if you do not want to be contacted by American Express for marketing purposes.

You acknowledge and agree that if we have not agreed to or do not acquire transactions for any Card type (i) we have no liability or responsibility whatsoever for the settlement of or disputes regarding those transactions and (ii) you will pursue directly with the related Card Network all claims and disputes regarding those transactions. You agree to pay us for per item processing, Authorization and other fees disclosed to you for any non-acquired transaction services you receive from us.

Bona Fide Transactions

- You may present for payment only valid charges that arise from a transaction between a bona fide Cardholder and your business. If you submit or attempt to submit Card Transactions that arise from sales between Cardholders and a different business than the one approved by us in your Agreement, then those transactions may be charged back, we may suspend or debit funds associated with all such transactions, and we may immediately terminate your account and your Agreement.
- Owners, partners, officers and employees of your business establishment, and the guarantors who signed your application form to us, are prohibited from submitting Card Transactions transacted on their own personal Cards, other than Card Transactions arising from bona fide purchases of goods or services in the ordinary course of your business. Such use in violation of your Agreement is deemed a cash advance, and cash advances are prohibited.

Factoring

- Factoring is considered Fraud and strictly prohibited. Factoring is the submission of Authorization requests by a merchant for Card Transactions transacted by another business. If you submit Card Transactions on behalf of another person, you will suffer any losses associated with the disputes of any such Card Transactions. Also, if any other fraud is involved, you could face criminal prosecution.

2.2 Card Network Rules

- You must comply at all times with all Card Network Rules applicable to all Cards accepted by you. You are responsible for reviewing the Card Network Rules from time to time and staying up to date with any changes. This includes the following obligations (which are expanded on in this Operating Guide):
 - (i) Except as otherwise agreed with us, you agree that you shall honor all valid Cards in accordance with the Card Network Rules without discrimination when properly presented for payment and not establish a minimum or maximum Card Transaction amount as a condition for honoring all Cards;
 - (ii) You agree not to accept any Card when you know, or should know, that acceptance of such Card may result in Fraud, where the Cardholder is not the authorized user, or where the Card Transaction does not result from a bona fide Card Transaction between you and the Cardholder;
 - (iii) You agree not to add any additional fees or charges to Card Transactions, unless expressly permitted under Applicable Law. If permitted, any such fee or charge must be included in the Card Transaction amount and not collected separately;
 - (iv) You agree to prominently and clearly disclose to Cardholders at all points of interaction your name and your Location, and ensure that the Cardholder is easily able to understand that you are responsible for the relevant Card Transaction, including the delivery of any goods (whether physical or digital) or provision of the services that are the subject of the Card Transaction; and
 - (v) You agree to display prominently on each of your premises, trading venues and/or websites where you accept Card Transactions, all applicable Card and Card Network identification, as required by and in accordance with, this Operating Guide and/or Card Network Rules.
- You must follow these rules when accepting Visa, Mastercard and Discover Cards. These rules are also required to be observed under the relevant rules of the various Debit Networks. Failure to comply with any of the Card Network Rules may result in fines or penalties.
 - (i) You may not impose a surcharge or fee for accepting a Debit Card;
 - (ii) You may not establish any special conditions for accepting a Card, other than those specifically permitted by the Card Network Rules;
 - (iii) You may not require the Cardholder to supply any personal information (e.g. home or business phone number; home or business address; or driver's license number) unless instructed by us. The exception to this is for mail/ telephone/internet order or delivery-

required transactions, or as otherwise permitted by Applicable Law. Any information that is supplied by the Cardholder must not be in plain view when mailed;

- (iv) You may not submit any Card Transaction representing the refinance or transfer of an existing Cardholder obligation deemed uncollectible, for example, a Card Transaction that has been previously charged back, or to cover a dishonored check;
- (v) You may not accept a Visa Consumer Credit Card or Commercial Visa Product, issued by a U.S. Issuer, to collect or refinance an existing debt without our approval. NOTE: Visa Consumer debit and Visa Business debit Card products, including prepaid card type may be accepted to collect or refinance an existing debt, with our prior approval and registration with Visa. You agree to reimburse us for our registration costs;
- (vi) You may not accept a Mastercard Card for payment of an existing consumer loan without our approval. NOTE: Mastercard Signature Debit or Mastercard Prepaid Card may be accepted for payment of an existing consumer loan, with our prior approval and registration with Mastercard. You agree to reimburse us for our registration costs;
- (vii) Any tax required to be collected must be included in the total transaction amount and may not be collected in cash;
- (viii) You may not accept Cards for cash equivalents, except as permitted by Card Network Rules;
- (ix) You may not accept Cards to verify the age of a Cardholder;
- (x) You may not accept Cards for purchases not specifically approved by the Cardholder;
- (xi) You may not accept Cards for damages, losses, penalties or fines of any kind, except as permitted under applicable Card Network Rules;
- (xii) You may not require a minimum Credit Card acceptance amount that exceeds \$10.00 and may not apply a minimum acceptance amount to Debit Card Transactions. Such minimum amount must be established for all Credit Cards regardless of Issuer or Card Network. Unless you are a federal government entity or an institution of higher learning, you may not establish a maximum amount as a condition for accepting a Card, except that for Discover Card Transactions, you may limit the maximum amount a Discover Cardholder may spend if, and only if, you have not received an Authorization approval code from the Issuer. Setting a minimum transaction amount limit for Debit Cards) is prohibited.

- **U.S. Merchants are permitted to engage in any of the following:**

- (i) You may direct customers to a particular brand or type of general purpose Card or a particular form of payment. You may also encourage customers who initially present a Visa Card to use a Card with a different network brand, a different type of Card or a different form of payment;
- (ii) You may provide a discount/incentive for a consumer to pay with cash, check, Credit Card, Debit Card, etc. however, you must clearly and conspicuously disclose the discount to consumers. Also, you must offer the discount to all consumers and you cannot discriminate based upon Card brand or Card Issuer. However, you may choose not to accept either U.S. issued Debit Cards or U.S. issued Credit Cards under the terms described in this Operating Guide;
- (iii) You may offer a discount or rebate, including an immediate discount or rebate at the point of sale;
- (iv) You may offer a free or discounted product, service or enhanced service;
- (v) You may offer an incentive, encouragement, or benefit;
- (vi) You may express a preference for the use of a particular brand or type of general purpose card or a particular form of payment;
- (vii) You may communicate to a customer the reasonably estimated or actual costs incurred by you when a customer uses a particular brand or type of general purpose Card or a particular form of payment or the relative costs of using different brands or types of general purpose Cards or different forms of payment;
- (viii) You will inform the Cardholder that you are responsible for the Card Transaction including your goods and services and for related customer service, dispute resolution and performance of the terms and conditions of the Card Transaction;
- (ix) You can accept Cards for charitable contributions (for non-profits);

- Additional information related to Card Network Rules can be found at the following websites:

- You may download “Visa Regulations” from Visa’s website at: <https://usa.visa.com/support/merchant.html>
- You may download “Mastercard Regulations” from Mastercard’s website: <http://www.mastercard.com/us/merchant/support/rules.html>
- For the American Express OptBlue Service only, you may download “American Express Merchant Operating Guide” from American Express’ website at: <http://www.americanexpress.com/merchantopguide>
- You may view information on Discover acceptance: <https://www.discoverglobalnetwork.com/en-us/partner-with-us/business-owners>
- You may access information on PayPal acceptance: <https://www.paypal.com/us/brc/>

3. Accepting Card-Present Payments

3.1 Overview

- This Section sets out the procedures required to accept Card Transactions, either through a Point-of-Sale (“POS”) terminal or via other *card-present* routes. This Section also includes information on how you can protect against potentially fraudulent transactions and the ways in which you and your staff can be aware of potential security issues when accepting Card Transactions.
- This Section primarily sets out information relevant to *card-present* Card Transactions. For *card-not-present* and e-commerce Card Transactions, please refer to Section 4 in this Operating Guide.
- **You are required to adhere to the procedures in Section 5 of this Operating Guide for information on the Authorization process for your Card Transactions with customers.**

3.2 Display of Cards Accepted

- You must prominently display appropriate Visa, Mastercard, Discover, and American Express and, if applicable, other Card Network decals and program Marks at each of your Locations, in catalogs, on websites and on other promotional materials as required by Card Network Rules. You may not indicate that Visa, Mastercard, Discover, American Express or any other Card Network endorses your goods or services.
- Your right to use the program Marks of the Card Networks terminates upon the earlier of:
 - (i) if and when your right to accept the Cards of the respective Card Network terminates (e.g. if your right to accept Discover Cards terminates, you are no longer permitted to use Discover Program Marks);
 - (ii) delivery of notice by us or the respective Card Network to you of the termination of the right to use the Mark(s) for that Card Network; or
 - (iii) termination of the license to use the program Marks by the respective Card Network to us.
- You must comply with all Card Network Rules regarding use of Marks owned by the Card Networks. Your use, display and reproduction of Card Network Marks in advertising, acceptance decals, signs, or otherwise must be in accordance with the guidelines and standards set by each respective Card Network.

Special Provisions for American Express Marks

- Whenever payment methods are communicated to customers, or when customers ask what payments are accepted, you must indicate your acceptance of the American Express Card and display the American Express Marks (including any Card application forms provided to you) as prominently and in the same manner as you do for any other Card or payment products.
- You must not use the American Express Marks in any way that injures or diminishes the goodwill associated with the American Express Marks, nor (without prior written consent from us) indicate that American Express endorse your goods or services. You shall only use the American Express Marks as permitted by your Agreement and you shall cease using the American Express Marks upon termination of your Agreement.
- You shall only use the American Express Marks as reasonably necessary to perform your obligations under your Agreement. The guidelines listed below apply to the Merchant’s use of the American Express “Blue Box” logo:
 - (i) The “Blue Box” logo must always be shown in the pre-approved “American Express blue” or, in one or two color communications, or black;
 - (ii) The space around the “Blue Box” must equal at least 1/3 the size of the box;
 - (iii) The “Blue Box” logo minimum size is 3/8" and 1/2" is the preferred size;
 - (iv) A minimum distance of 1-1/2 times the size of the “Blue Box” must be allowed between the “Blue Box” logo and another Mark.

- For additional guidelines on the use of the American Express Marks, you can visit the American Express website at www.americanexpress.com/decals.
- You must remove American Express Marks from your website and wherever else they are displayed upon termination of your Agreement or if you do not elect to accept or are not authorized to accept American Express Cards.

Special Provisions for Discover Marks

- You are prohibited from using the Discover Program Marks, as defined below, other than as expressly authorized in writing by us. **“Discover Program Marks”** means the brands, emblems, trademarks and/or logos that identify Discover Network Cards, including, without limitation, Diners Club International Cards, JCB, UnionPay, BCard, and Dinacard. You may use the Discover Program Marks only to promote the services covered by the Discover Program Marks by using them on decals, indoor and outdoor signs, advertising materials and marketing materials; provided that all such uses by you must be approved in advance by us in writing.
- You shall not use the Discover Program Marks other than as a part of the display of decals, signage, advertising and other forms depicting the Discover Program Marks that are provided to you by us or otherwise approved in advance in writing by us. You shall not use the Discover Program Marks in such a way that customers could believe that the products or services offered by you are sponsored or guaranteed by the owners of the Discover Program Marks. You recognize that you have no ownership rights in the Discover Program Marks. You shall not assign to any person any of the rights to use the Discover Program Marks.

3.3 Accepting Cards via POS terminals

- Under your Agreement, you are responsible for providing the necessary Merchant Equipment for the acceptance of Card Transactions. This includes all hardware equipment to be used in connection with receiving the Merchant Services from us (e.g. POS terminals, PIN entry devices, Card readers, Card scanners, etc.) and software platforms. You are required to notify us of any changes or modifications to your Merchant Equipment.
- Your acceptance of the Agreed Upon Card Types includes both Credit Cards and Debit Cards, and you may also choose to accept PIN Debit Cards. With PIN Debit, Cardholders are required to enter in a PIN in order to successfully complete the transaction. Some Cardholders prefer the additional security of entering in their PIN. This requires you to either have a terminal or system that can be faced towards the customer in order for them to enter their PIN or a separate PIN pad connected to their terminal or system that allows the entry of the PIN.
- Not all types of business are conducive to accepting PIN Debit. If the Card is not present or the location of the Credit Card terminal is not convenient to the Cardholder entering in their PIN then your business will not be able to accept PIN Debit Cards. If you choose not to accept PIN Debit then Debit Cards can typically be processed as a Mastercard or Visa Signature debit transaction without entering the PIN. If you need more information about accepting PIN Debit transactions please contact Customer Service.
- In this sub-section, we set out generic guidance on the use of a POS terminal to accept “Chip and PIN”, “Signature” and “Contactless” Card Transactions. This guidance does not relate to a specific model of POS terminal, but functionality across POS terminals are broadly similar.

Chip and PIN

1. Navigate to the functionality which permits you to input a new transaction.
2. Enter in the transaction amount according to the relevant prompt. The POS terminal may now request for the Cardholder to insert their Card into the Card reader slot on the POS terminal itself or on a separate connected Card reader.
3. The POS terminal may now request for the Cardholder to input their PIN. Request for the Cardholder to verify that the transaction amount is correct and to input their PIN and press the “Enter” or “Submit” key.
4. The POS terminal may then connect to the relevant payment network to authorize the Card Transaction. The timeframe required for this process depends on your connection to the payment network and the data traffic being processed by that payment network.

5. The POS terminal may then display “Authorized”, indicating that the Cardholder has the requisite funds for the payment transaction. **Please be advised that Authorization is not a guarantee of payment.** A receipt may then be printed. Please retain one copy for yourself and provide the Cardholder with another copy.
6. If the POS terminal returns an error message or otherwise declines the Card submitted, inform the Cardholder. Where the POS terminal displays a prompt to contact our Authorizations Centre, please contact us immediately and comply with our instructions.
7. Where providing goods, you may provide those goods to the Cardholder when Authorization is received. Remember to return the Card to the Cardholder.

If you accept Chip Cards on equipment not enabled for Chip Card acceptance based on Chips (and not the Magnetic Stripe), you (and not the Issuers of such Chip Cards) will be responsible for any counterfeit Card fraud regarding those Chip Card Transactions, pursuant to Mastercard, Visa, American Express and Discover Card Network Rules (“**EMV Liability Shift**”).

A similar EMV Liability Shift has already occurred for American Express Card Transactions as of October 17, 2015. For Automated Fuel Dispensers (“**AFDs**”), the EMV Liability Shifts for Visa, Mastercard and Discover will occur on October 1, 2020, and for American Express on October 17, 2020. Note: for Visa and Mastercard, the EMV Liability Shift for AFDs has already occurred as of October 1, 2017, with respect to the acceptance of Cards issued outside the U.S. region.

For unembossed Cards used to conduct *card-present* Transactions, Merchants must obtain Authorization responses electronically using a POS terminal. A Card Transaction involving an unembossed Card may be subject to dispute if you “key enters” Card information into a POS terminal and do not use the electronic Authorization procedures.

Mastercard MPOS

- Mastercard revised standards relate to the use of Mobile POS (“**MPOS**”) terminals. Merchants with less than \$100,000 in annual Mastercard transaction volume may use Chip-only MPOS terminals:
 - (i) That do not support Magnetic Stripe capture and cannot print a paper receipt; and
 - (ii) Have a contact chip reader and Magnetic Stripe-reading capability but does not support PIN as a Cardholder Verification Method (“**CVM**”) for Chip Card Transactions.
- Merchants with less than \$100,000 in annual Mastercard transaction volume may use MPOS terminals or Chip-only MPOS solutions that do not support electronic signature capture to complete a transaction without obtaining a CVM.

NOTE

Merchants with more than \$100,000 in annual transactions may use MPOS terminals if the MPOS terminal complies with Mastercard’s requirements for POS terminals or hybrid POS terminals (if Chip Cards are accepted).

Signature

- You may be required to accept a Card Transaction via verifying a Cardholder’s signature where the Card submitted for payment does not have a “Chip”. **You should prioritise the use of the “Chip and PIN” route for accepting a Card Transaction where the Card submitted for payment has a “Chip”.** This route for accepting Card Transactions has an additional risk as it is not as secure compared to a “Chip and PIN” payment transaction.
 1. Navigate to the functionality which permits you to input a new transaction.
 2. Enter in the transaction amount according to the relevant prompt. Ensure that the transaction amount is correct. The POS terminal may now request for the Card to be swiped on the POS terminal itself or on a separate connected Card reader. This may also arise where you opt to bypass PIN verification on a “Chip and PIN” payment transaction.

3. The POS terminal may then connect to the relevant payment network to authorize the Card Transaction. If the POS terminal returns an error message or otherwise declines the Card submitted, inform the Cardholder. Where the POS terminal displays a prompt to contact us, please contact Customer Service immediately and comply with our instructions.
4. The POS terminal may then print a receipt which requires the Cardholder's signature. Verify that the Card information is correctly reflected on the receipt.
5. Request that the Cardholder verify the transaction amount and sign the receipt where indicated.
6. Ensure that the Cardholder's signature on the terminal receipt matches the signature on the reverse of the Card. You may request the Cardholder to provide additional government-issued identification if you are unsure that the customer is the Cardholder
7. If there are no issues with the Cardholder's signature, submit the payment transaction on the POS terminal.
8. Where providing goods, you may now provide those goods to the Cardholder, returning his or her Card with a copy of the receipt. Please retain the signed receipt.

Contactless

- Your POS terminals may be equipped with the necessary functionality to accept contactless Card Transactions. In this route of accepting payments, Cardholders may utilise their contactless-enabled Cards or a mobile device (e.g. cellular telephone or wearable device) to pay for goods and services.
 1. Navigate to the functionality which permits you to input a new transaction.
 2. Enter in the transaction amount according to the relevant prompt. Ensure that the transaction amount is correct. The POS terminal or a connected contactless Card reader may now request for the contactless-enabled Card or mobile device to be in close proximity.
 3. The POS terminal may emit a sound indicating that it has captured the contactless-enabled Card or mobile device. **Please be advised that this does not indicate that the Card Transactions is authorized.** The POS terminal may request for a PIN entry in certain circumstances. This is a normal occurrence and may occur periodically as a security characteristic.
 4. The POS terminal may then connect to the relevant payment network to authorize the Card Transaction. If the POS terminal returns an error message or otherwise declines the Card submitted, inform the Cardholder.
 5. Where the POS terminal display indicates that the Card Transaction is authorized, it may print a receipt for the Cardholder. You may then provide this receipt to the Cardholder with the goods purchased.

Troubleshooting the acceptance of Cards using POS terminals

- In accepting Card Transactions via your POS terminal, you may encounter issues in the processing of such transactions. We set out general guidance below on what to do in the event that issues arise. Please be advised that you should rely on the instructions accompanying the model of your specific POS terminal in all cases.

(i) PIN entry issues

A Cardholder may incorrectly enter his or her PIN on the POS terminals when attempting a "Chip and PIN" transaction. In the event that the Cardholder incorrectly enters his or her PIN three times, the Card is automatically locked and cannot be used for any further transactions. You should advise the Cardholder to contact their issuing institution for further instructions and request for an alternative form of payment.

In the event that the Cardholder is unable to recall the PIN to enter on the POS terminal, his or her Card may have the functionality whereby PIN entry may be bypassed and the Card Transaction may proceed as a "Signature" transaction. In this situation, you should

exercise additional caution and verify the Cardholder's identity by reference to the signature on the reverse of the Card and/or requesting the Cardholder to provide a form of government-issued identification.

(ii) **Card reading issues**

Your POS terminal may be unable to correctly read the data residing on a Card. If attempting to process a "Chip and PIN" Card Transaction, ensure that the Card is inserted in the correct way and that there are no visible deformations or marks on the "Chip". If attempting to process a "Signature" Card Transaction, ensure that the magnetic strip on the reverse of the Card is not deformed or has excessive damage.

If your POS terminal is unable to correctly read or detect the Card, your POS terminal may provide for the option to enter the Primary Account Number ("**PAN**") via the POS terminal. Please refer to the instructions accompanying the model of your POS terminals for more information on this process. You should, if utilizing this procedure, also have a receipt of the Card used on a sales voucher with a signature by the Cardholder, and retain this to document that the Card was present for this transaction in the event that a chargeback is initiated. If the Card is entered manually, you are required to accept the risks involved if the transaction results in a Chargeback.

- If your terminal malfunctions, refer to your instruction Documentation, if necessary, or call Customer Service. The problem will either be corrected promptly or may require terminal programming or replacement.
- During the period in which your terminal is not functioning, remember to check it periodically since most terminal problems are temporary in nature and are quickly corrected. If a terminal is moved or if wires are disconnected, causing malfunction, call Customer Service immediately and follow their instructions. You may be responsible for any service charges incurred for reactivation of the terminal.

- **Until the terminal becomes operable, you must request another form of payment. A virtual terminal option is also offered that permits you to key transactions in to a software program. This may be an option that permits you to accept transactions when your primary terminal is not functioning. Please contact Customer Service for further information.**

Authorization procedure in the event of POS terminal failure

- All approved sales authorized via virtual terminal will be captured and deposited. These transaction do not need to be manually entered into your terminal or processing system.
- You may be subject to a Chargeback if you receive a referral and subsequently receive an approval. (For specific procedures on capturing Transaction Data electronically, refer to the terminal operating instructions/users guide.)
- If your POS terminal malfunctions for more than twenty-four (24) hours, contact Customer Service for further instructions on processing your transactions.

3.4 Protecting Against Card Fraud

- When accepting *card-present* Card payments, it is important to reduce the risk of fraudulent Card Transactions by ensuring that the Cards you accept are not cloned or otherwise used for illegal purposes. For these purposes, the Card must be carefully examined by you and your staff to determine whether it is a legitimate and valid Card. Please review the below characteristics of a Card prior to accepting such Card for a transaction.
- The name of the Card (e.g. Visa, Mastercard, Discover or American Express) should appear in bold letters on the Card. For all Visa and Mastercard Cards and for some Discover Cards, the Issuer (e.g. XYZ Bank, etc.) should also appear in bold letters on the Card. We have set out below the different security features of each type of Card that you may accept for payment.

Card Network	Security Features
Visa	<ul style="list-style-type: none">• The Visa Mark must appear in blue and gold on a white background in either the bottom right, top left, or top right corner.

	<ul style="list-style-type: none"> • Embossed/unembossed or printed account number on valid cards begins with “4” and all digits must be even, straight, and the same size. • The four to six digit Bank Identification Number (“BIN”) may be printed directly below the account number. This number should match exactly with the first four digits of the account number. • The expiration or “Good Thru” date should appear below the account number. • The “Mini-Dove” design hologram may appear on the back of the Card. The three-dimensional dove hologram should appear to move as you tilt the Card. • The magnetic-stripe is encoded with the Card’s identifying information. • The Card Verification Value 2 (“CVV2”) is a three-digit code that appears either in a white box to the right of the signature panel, or directly on the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in <i>card-not-present</i> Transactions to verify that customer is in possession of a valid Visa Card at the time of the sale. The signature panel must appear on the back of the card and contain an ultraviolet element that repeats the word “Visa®.” It may vary in length. The words “Authorized Signature” and “Not Valid Unless Signed” must appear above, below, or beside the signature panel. If someone tried to erase the signature panel; the word ‘VOID’ will be displayed. • Chip Cards contain a small embedded microchip that is virtually impossible to copy or counterfeit. Chip antenna for contactless cards, the interface can be an antenna embedded into the back of the Card and connected to the Chip. A contactless transaction works at terminals through the radio frequency wave between the Card and the terminal. • You are required to familiarize yourself with the new design by consulting the document entitled “Card Acceptance Guidelines for Visa Merchants and Chargeback Management Guidelines for Visa Merchants”. You may download the document from Visa’s website at http://www.visa.com/merchant or order a hardcopy to be mailed to you for a nominal charge by telephoning Visa fulfillment at 800-VISA-311.
Mastercard	<ul style="list-style-type: none"> • The Mastercard symbol appears on the front or back of the Card. • The global hologram is three dimensional with a repeat “Mastercard” printed in the background. In addition, the words “Classic”, “Preferred”, “Gold” or “Business” may appear. When rotated, the hologram will reflect light and appear to move. • Mastercard account numbers are sixteen (16) digits, and the first digit is always a five (5) or two (2). The first four digits of the account must be printed directly below the embossed number. • The signature panel is tamper evident with the word “Mastercard” printed in multiple colors at a 45° angle. For magnetic swiped Card Transactions, remember to compare the signature on the back of the Card with the Cardholder’s signature on the receipt. The four digits printed on the signature panel must match the last 4 digits of the account number, followed by the three digit indent printed CVC2 number. • A Chip may be present on the Card. The Cardholder will be prompted to enter a unique personal identification number or PIN when the Card is inserted into a Chip-capable payment terminal. PayPass® contactless payment technology may be present on Card. A signature is not required for PayPass® “tapped” transactions below a specified limit.
Discover Discover includes Discover, Diners Club International, JCB, UnionPay, BCard and Dinacard	<ul style="list-style-type: none"> • The Discover Mark may appear on the lower right corner of the front, back, or both sides of the Card. • Cards display a three-dimensional hologram on the front of the Card OR a three-dimensional holographic Magnetic Stripe on the back of the Card. Valid Cards do not display holograms on both front and back. • Card numbers may be embossed or unembossed and will appear on either the front or back of a Card. Card numbers begin with the number “6” and are composed of 16 digits that should be clear and uniform in size and spacing. • The Cardholder name, and if applicable, business name, may be embossed or unembossed and will appear on either the front or back of the Card. • The “Valid Thru” date may be embossed or unembossed and will appear on either the front or back of a Card in “mm/yy” format that indicates the last month in which the Card is valid. • The words “DISCOVER” or “DISCOVER NETWORK” appears on the front of the Card under an ultraviolet light. • The signature panel displays the words “DISCOVER” or “DISCOVER NETWORK” and may vary in size. Cards may contain a panel that includes an ultraviolet image of the word “DISCOVER.” An underprint of “void” on the signature panel becomes visible if erasure of the signature is attempted. • The last four digits of the Card Number may be displayed on the back of the Card and are commonly printed in reverse indent printing on the signature panel. • On embossed Cards, a security character, displayed as an embossed stylized “D” may appear on the front of the Card. • The three digit CID is printed on the back of the Card in a separate box to the right of the signature panel. <p>Note: Valid Cards may not always be rectangular in shape (e.g. Discover 2GO Cards). Certain valid unembossed Cards or contactless payment devices approved by us for use in accessing Card accounts (e.g. contactless stickers, key fobs, and mobile commerce devices) and to conduct contactless Card Transactions may not display the same features</p>

	<p>described above. Card expiration date and other features listed above are not displayed on such contactless payment devices.</p> <p>The features indicated below are found on valid contactless Chip payment devices approved for use in accessing Card accounts and to conduct contactless Card Transactions:</p> <ul style="list-style-type: none"> • Standard, plastic rectangular Cards that are also contactless Chip payment devices bear the security features described above. • Contactless Chip payment devices other than mobile payment devices bear the contactless indicator. • Contactless Magnetic Stripe payment devices bear the “Discover Zip” indicator
<p>Diners Club International</p>	<ul style="list-style-type: none"> • A “Diners Club International Acceptance” Mark appears in upper left corner. • Two-character alphanumeric code is printed in the lower right corner. • Embossed with a 14-digit account number (begins with 36). • Embossed 16-digit account number (begins with 30). • Embossed digits on the Card must be clear and uniform in size and spacing within groupings. • Embossed expiration data appears in “mm/yy” format and indicates the last month in which the Card is valid. <p>Note: Some valid Cards bearing a “Diners Club International Acceptance Mark” display a printed, unembossed Card number. If a Card Transaction involving a Diners Club International Card with an unembossed Card number cannot be completed by swiping the card through the POS terminal, the Card should not be accepted. If submitted, such Card Transaction may be subject to dispute.</p>
<p>UnionPay</p>	<ul style="list-style-type: none"> • A 16-digit Card number starting with “622,” “624,” “625,” “626,” or “628” is embossed on the front of the Card. • Embossed digits on the Card should be clear and uniform in size and spacing. • The embossed expiration date appears in “mm/yy” format and indicates the last month in which the Card is valid. • The Card contains a Magnetic Stripe. • A three-dimensional hologram image of “Heaven Temple” in the foreground with Chinese characters in the background appears on the front of all such Cards. The hologram reflects light as it is rotated. • “Valid Thru” and the Cardholder name (which may not be in English) are embossed on the front of the Card. • The CID appears on the upper right corner of the signature panel. <p>Note: Text on Cards bearing a “UnionPay Acceptance Mark” may not be printed in English.</p>
<p>JCB</p>	<ul style="list-style-type: none"> • Card numbers are made up of 16 digits, starting with “35” embossed or printed on the front of the Card. • Embossed digits on the Card should be clear and uniform in size and spacing within groupings. • The Cardholder name and, if applicable, business name embossed on the front of the Card. • A “JCB Acceptance Mark” appears on the front of the Card. • A three-dimensional hologram image of rising sun, rainbow, and “JCB” in micro lettering appears on either the front or the back of the Card. The hologram reflects light as it is rotated. • The embossed expiration date appears in “mm/yy” or “mm/dd/yy” format on the front of the Card and indicates the last month in which the Card is valid. • The Card contains a Magnetic Stripe on the back of the Card. • The name “JCB” appears in ultraviolet ink on the left bottom of the front of the Card when held under an ultraviolet light. • The first four digits of the Card number match the four-digit number pre-printed just below the embossed Card number of the front of the Card. • The first four digits of the Card number displayed on the signature panel on the back of the Card match the last four digits of the Card number that appear on the front of the Card. • The last four digits of the Card number on the back of the Card are followed by the three-digit CID. • An overprint on the signature panel reads “JCB” in two colors, blue and green. • Some Cards have an embedded integrated circuit chip on the front of the Card. • The words “Good Thru,” “Valid Dates,” “Valid Thru,” or “Expiration Date” must be printed near the expiration date. The corresponding words in the language of the country where the JCB Card is issued may also be printed. The

	<p>words “Month/Year” or the corresponding words in the language of the country where the JCB Card is issued may be printed above or below the expiration date.</p> <p>Note: Some valid Cards bearing the JCB Acceptance Mark will have a printed, unembossed Card number on the Card. If a Card Transaction involving a valid, JCB Card with an unembossed Card number cannot be completed by swiping the Card through the POS terminal, the Card should not be accepted. If you accept a Card that displays a printed, rather than embossed, Card number, you are required to obtain a Card imprint, the Card Transaction may be subject to dispute.</p>
American Express	<ul style="list-style-type: none"> • 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 any transaction receipt, must match. • Pre-printed Card identification numbers must always appear above the Card number on either the right or left edge of the Card. • Do not accept a Card outside the “Valid Dates”. • 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. • Some Cards have a Chip on which data is stored and used to conduct a Card Transaction. • Only the person whose name appears on an American Express Card is entitled to use it. Cards are not transferable. • The signature on the back of the Card must match the Cardholder’s signature on any transaction receipt (where a signature is used to verify the Cardholder’s identity), 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.

Expiration Dates

- At the point of sale, the Card should be carefully examined for its expiration date.
 - (i) When an expiration date is expressed in a month/year format, Card Transactions are valid through and including the last day of the month and year.
 - (ii) Do not accept a Card after the expiration date.

Valid Signature

The following does not apply to a Card Transaction that is processed with a PCI DSS-compliant Chip Card reading device with which you may process a Transaction without a Cardholder signature.

- Check the back of the Card. Ensure that the signature panel has not been disfigured or tampered with in any fashion (an altered signature panel may appear discolored, glued or painted, or show erasure marks on the surface).
- The signature on the back of the Card must compare favorably with the signature on the signed transaction receipt. The relevant transaction receipt must be signed by the Card presenter in the presence of your authorized representative (unless a *card-not-present* Transaction) and in the same format as the signature panel on the Card.
- The signature panels of Visa, Mastercard and Discover Cards have a three-digit number (CVV2/CVC2/CID) printed on the panel known as the Card Validation Code (“**CVC**”).
- Visa, Mastercard, Discover and American Express: If the signature panel on the Card is blank, in addition to requesting an Authorization, you must do all the following:
 - (i) Review positive identification bearing the Cardholder’s signature (such as a passport or driver’s license that has not expired) to validate the Cardholder’s identity;

- (ii) Require the Cardholder to sign the signature panel of the Card prior to completing the transaction; and
- (iii) When a Mastercard PayPass enabled key fob or mobile telephone is presented for payment, validating the customer's signature is not required.

American Express No PIN Program.

- You may participate in the American Express "No PIN Program". This No PIN Program allows establishments not to request a PIN from Cardholders on transaction receipts. To qualify for the No PIN Program, both the establishment and each charge must meet the following criteria:
 - (i) **Establishment Criteria.** If your establishment is classified in an industry that accepts in-person charges, then the establishment may participate in the No PIN Program with the exception of the following categories:
 - Merchants who do not conduct in-person charges (i.e. internet, mail order or telephone order);
 - Prohibited transactions as set forth in the American Express Card Network Rules or illegal transactions or activity;
 - "High risk" merchants (e.g. establishments whose business type has had historically high occurrences of fraud and disputed charges with American Express or as compared to other similarly situated merchants (or both); examples include internet electronic services or nightclubs/lounges) as determined by American Express in its sole discretion;
 - Merchants placed in American Express' Fraud Full Recourse Program.
 - (ii) **Charge Criteria:**
 - The amount or charge must meet the threshold established in American Express' country-specific policy;
 - The charge submission must include the appropriate indicator to reflect that the Card and the Cardholder were present at the point of sale;
 - The charge submission must include a valid approval.
- Under the No PIN Program, Chargebacks will not be exercised for such charges based solely on the establishment's failure to obtain the Cardholder's PIN at the point of sale.
- If a disproportionate amount or a number of disputed charges under the No PIN Program occur, you must cooperate to reduce the amount or number of disputed charges. If such efforts fail, you may be placed in American Express Chargeback programs (see American Express Card Network Rules regarding "chargeback programs"), or your establishment's participation in the No PIN Program may be modified or terminated. The established threshold for charges to qualify under the "No PIN Program" is \$50.00 or less.
- Note: Obtaining Cardholder signature on card-present Transactions is optional to complete a Charge Record, and at your discretion, unless required by Applicable Law.

Physical Security

- Physical security policies and procedures should also be implemented in your business. This may include ensuring that only specified staff members have access to POS terminals or can alter or set the programming of your POS terminals in any way.
- Additional security measures could include ensuring that POS terminals are always in view of staff members at the relevant service counters, and to ensure that the setup of the acceptance of payments facilitates security (e.g. ensuring that no other customers can have sight of another customer's PIN when entering such a PIN into a POS terminal).

Users Other Than Cardholders

- **A Cardholder may not authorize another individual to use his / her Card for purchases.** Be sure the signature on the Card matches with the one on the transaction receipt signed by the Cardholder.
- Furthermore, any Card having two signatures on the back panel is invalid and any sale made with this Card can result in a Chargeback.
- For Cards bearing a photograph of the Cardholder, ensure that the Cardholder appears to be the person depicted in the picture which appears on the Card.

Suspicious Transactions

- While not proof that a transaction is fraudulent, the following are some suggestions to assist you in preventing fraudulent transactions that could result in a Chargeback:

Ask yourself, is the customer:

- (i) Purchasing high-value or large amounts of merchandise with seemingly no concern for size, style, color, or price;
 - (ii) Asking no questions or refusing free delivery on large items (e.g. heavy appliances or televisions) or high-value purchases;
 - (iii) Trying to distract or rush sales associates during a transaction;
 - (iv) Making purchases, leaving the store, and then returning to make more purchases; and/or
 - (v) Making purchases either when the store opens or immediately before it closes.
- If you feel uncomfortable or suspicious about a Cardholder or Card Transaction, adhere to your procedures and respond accordingly.

If you use an electronic terminal and swipe the Card, make sure the account number displayed on the terminal and/or the transaction receipt matches the number on the Card. If you cannot or do not verify the account number and accept the sale, you are subject to a Chargeback and could be debited for the amount of the transaction. IF THE NUMBERS DO NOT MATCH, DO NOT ACCEPT THE CARD AS A FORM OF PAYMENT, EVEN THOUGH AN AUTHORIZATION APPROVAL CODE FOR THE MAGNETICALLY SWIPED CARD NUMBER MAY BE RECEIVED.

Any counterfeit Card fraud transactions (including any resulting from lost, stolen or never received Cards by the Cardholder) may result in Chargebacks for which you will be liable to us.

Fraud-Prone Merchandise Tips:

- (i) Gift cards, jewelry, video, stereo, computer and camera equipment, shoes and men's clothing are typically fraud-prone because they can easily be resold.
- (ii) Be suspicious of high dollar amounts and transactions with more than one fraud-prone item (e.g. two computers, three gold chains, etc.).

REMEMBER: An Authorization approval code only indicates the availability of a Cardholder's credit at the time of the transaction. It does not warrant that the person presenting the Card is the rightful Cardholder. If proper procedures are not followed at the time of the transaction, you are subject to a Chargeback and your account may be debited for the amount of the Card Transaction.

4. Accepting Card-Not-Present Payments

4.1 Overview

- This Section sets out the procedures required to accept *card-not-present* Transactions. These encompass payment transactions that may be processed over the internet (“**eCommerce transactions**”), or via mail order(s) or telephone order(s) (“**MOTO Transactions**”). We set out below the policies and procedures for accepting payments via eCommerce transactions and MOTO Transactions.
- This Section primarily sets out information relevant to *card-not-present* Transactions. For *card-present* Transactions, please refer to Section 3 in this Operating Guide. The procedures described in this Section 4, while they will not eliminate Chargebacks, are useful in reducing them and should be followed by you.
- **You are required to adhere to the procedures in Section 5 of this Operating Guide in relation to the Authorization process for your Card Transactions with customers.**

4.2 Card Acceptance

- You may only accept Cards for mail/telephone/internet orders provided they do not exceed the percentage of your total Card volume reflected on your application. Failure to adhere to this requirement may result in cancellation of your Agreement.
- Please be advised that mail, telephone, internet and other *card-not-present* Transactions have a substantially higher risk of Chargeback due to the fact that you will not have a PIN-verified Card Transaction or magnetically swiped Card Transaction and you will not have the Cardholder’s signature on the transaction receipt as you would in a face-to-face transaction.

General Requirements

- You may not submit a Card Transaction for processing until after the merchandise has been shipped or the service has been provided to the customer. (The Card Networks will permit the immediate billing of merchandise manufactured to the customer’s specifications (i.e. special/custom orders) provided the Cardholder has been advised of the billing details.)
- You should provide a copy of the relevant transaction receipt or invoice to the Cardholder at the time of delivery. You must also obtain proof of delivery of the goods or services to the address designated by the Cardholder (i.e. by getting “proof of delivery” from the delivery carrier).
- Notify the Cardholder of delivery time frames and special handling and/or cancellation policies. Merchandise shipping dates must be within seven (7) days of the date Authorization was obtained. If, after the order has been taken, additional delays will be incurred (e.g. out of stock), notify the Cardholder. If you have not shipped the product by the seventh day, you must reverse the original Authorization, then reauthorize the Card Transaction.
- **For Discover Cards:** Discover does not use an Electronic Commerce Indicator (as defined below). The amount of a Mail-Order/Telephone-Order Card Sale as represented in Sales Data may exceed the amount of the corresponding positive Authorization Response by a Tolerance Level of 15% if the amount in excess of the Authorization Response represents shipping costs.
- Merchants conducting internet transactions using Mastercard or Visa Cards must have special codes (an “**Electronic Commerce Indicator**”) added to their Authorization and settlement records. Failure to register as a merchant conducting internet transactions can result in fines imposed by the Card Networks.

4.3 eCommerce Transactions

- In your business, you may retail goods and services over the internet by using a website. In these circumstances, you must provide us with at least thirty (30) days’ prior written notice of any change in your website address before we start providing the Merchant Services to you (your “**Website**”) in respect of which the Merchant Services are to be provided.

General Requirements

- If you accept orders via the internet, your Website must include the following information in a prominent manner:
 - (i) Complete description of the goods or services offered;
 - (ii) Description of your merchandise return and Credit / Refund policy;
 - (iii) Customer service contact, including email address and/or telephone number;
 - (iv) Transaction currency (U.S. dollars, unless permission is otherwise received from servicers);
 - (v) Any applicable export or legal restrictions;
 - (vi) Delivery policy, including for split shipments (if applicable);
 - (vii) Consumer data privacy policy;
 - (viii) A description of the transaction security used on your website;
 - (ix) Your identity at all points of interaction with the Cardholder;
 - (x) Your address, including country;
 - (xi) Cancellation policy;
 - (xii) Date when charges will commence (if applicable); and
 - (xiii) Date any free trial period ends.

- You may not accept Card numbers through email over the internet.

The sale or disclosure of databases containing Cardholder account numbers, personal information, or other Card Transaction information to third parties is prohibited.

Acceptance of Terms and Conditions

- You must either include a click-to-accept button, check-box, or electronic signature acknowledgment to indicate that the customer or the Cardholder accepts the terms and conditions of the transaction or locate the terms and conditions on the checkout screen near the “Submit” button where the customer or the Cardholder completes the transaction.

Completion of the Transaction

- You must disclose certain information after the customer or Cardholder successfully submits their Card details on your Website(s). These include, but are not limited to:
 - (i) A receipt for the customer or Cardholder and a confirmation of the order placed or goods and/or services sold, including any arrangements for delivery. This may be delivered by way of e-mail; and
 - (ii) Information for customers or Cardholders on the procedure to rectify any inaccurate details on this receipt and/or confirmation (e.g. your contact information for customers or Cardholders).

Processing eCommerce Transactions

Payment gateway integration

- Prior to accepting eCommerce transactions, please ensure that your Website(s) are compatible with our payment gateway that is used for accepting Card details from your customers. You may be required to establish a separate designated account for the acceptance and processing of eCommerce transactions.

- Our payment gateway delivers a secure route to the acceptance of Card information and for the relay of such Card information in the processing of Card Transactions. Where Card details are submitted via our payment gateway, the customer’s or Cardholder’s Card is pre-authorized for the amount of that eCommerce transaction, and the full amount is authorized on dispatch of the good(s) ordered by that customer.

- Please be reminded that the Authorization process only indicates that there are sufficient funds in the customer's or Cardholder's account and that the relevant transaction amount being authorized is set aside for actual payment. It also only indicates that the Card being used is not reported as lost or stolen.
- Please refer to your Agreement to determine which Cards you can accept for payment when processing eCommerce transactions.

Security

- Any information relating to Cardholder data must be stored and transferred in a secure way. You are required to ensure that all Cardholder data is appropriately encrypted, and that your computer systems are protected with up-to-date anti-virus and anti-malware software. You must also have appropriate access control to your systems to prevent unauthorized intrusions and ensure that only individuals who require access are provided with access to your computer systems. Where you use your equipment and systems to process eCommerce transactions, you must ensure that such equipment and systems are compliant with the Payment Card Industry – Data Security Standards.
- The processing of eCommerce transactions may additionally involve customer authentication via Visa Secure, Mastercard SecureCode or American Express Safekey. These authentication systems may require your customers and Cardholders to authenticate identities through the use of two-factor authentication (i.e. “2FA”). This may require your customers and Cardholders to input an additional code or other security password when submitting Card details online.
- You should also be aware of indicators of potential fraudulent activity (e.g. multiple transactions from the same Card number or from the same country or issuing institution, or where the transaction involves high volumes of items that are easily re-sold), and the procedures for reducing the potential for Fraud (e.g. ensuring that Refunds are provided to the Card used for the original transaction, or ensuring that the high-value items ordered are delivered to the stated billing address).
- Please refer to Section 7 (Data Security) in this Operating Guide for further information on payment security.

Additional Requirements for eCommerce Transactions

- You agree to develop and maintain a point of presence on the internet at your expense. You will be responsible for all costs of connectivity and communication between you, the internet and us. You agree to utilize Secure Sockets Layer (“SSL”) or other secure compatible encryption method acceptable to us in providing your eCommerce transactions to us for Authorization, processing and settlement.

Discover Protocol for internet Transactions

- Each internet Discover Card Transaction accepted by you and submitted to us shall comply with Discover standards, including, without limitation, Discover standards governing the formatting, transmission and encryption of data, referred to as the “designated protocol”. You shall accept only those internet Discover Card Transactions that are encrypted in accordance with the designated protocol. As of the date of this Operating Guide, the designated protocol for the encryption of data is SSL.
- We may, at our discretion, withhold Settlement Funds until security standards can be verified. However, the designated protocol, including any specifications with respect to data encryption, may change at any time upon thirty (30) days advance written notice. You shall not accept any internet Discover Card Transaction unless the transaction is sent by means of a browser which supports the designated protocol.

4.4 Mail Order / Telephone Order Transactions

- The below procedures should be adhered to when accepting mail order / telephone order transactions (otherwise referred to as “MOTO” transactions):
 - (i) Obtain the expiration date of Card;
 - (ii) For mail orders, write “MO”; for telephone orders, write “TO” on the Cardholder's signature line;
 - (iii) For telephone orders, it is recommended that written verification of the sale be requested from the Cardholder (sent by mail or fax);
 - (iv) If feasible, obtain and keep a copy of the Cardholder's signature on file on a form authorizing you to submit telephone and mail order transactions;

- (v) You may not require a Cardholder to complete a postcard or other document that displays the Cardholder's Card number in clear view when mailed.

4.5 Address Verification Service

- AVS (and other fraud mitigation tools such as Verified by Visa®, Mastercard® SecureCode, Discover Protect Buy, American Express® SafeKey Card Validation Codes and Card Identification) does not guarantee against Chargebacks, but used properly, it assists you in reducing the risk of fraud by confirming whether certain elements of the billing address provided by your customer match the billing address maintained by the Issuer. AVS also may help you avoid incurring additional interchange expenses.
- AVS is a separate process from obtaining an Authorization and will provide a separate response. A Card Transaction may be authorized regardless of the AVS response. It is your responsibility to monitor the AVS responses and use the information provided to avoid high-risk transactions.
- The below procedures should be adhered to ensure the security of payment transactions for *card-not-present* Transactions and reduce the possibility of you experiencing Chargebacks:
 - (i) You should utilize the AVS for all *card-not-present* Transactions (see note below). AVS is specifically required for all Discover *card-not-present* Transactions, and **if you do not receive a positive match through AVS for a Discover *card-not-present* transaction, you may not process that Card Transaction. If you do not have AVS, contact us immediately.**
 - (ii) You should obtain the 3 or 4 digit Card Verification Code number and include it with each Authorization request. Discover Card Network Rules specifically require that you submit the Card Verification Code with the Authorization request for all Discover *card-not-present* Transactions.

5. Authorizations

5.1 Overview

- This Section sets out the procedures you should adhere to in relation to the Authorization of Card Transactions. **Please be reminded that Authorization of a Card Transaction does not guarantee payment, and that it only indicates that, at the time of the transaction, the Card has not been reported as lost or stolen, and that there are sufficient funds available.**

5.2 Authorization of Card Transactions

General Rules

- Each Authorization request you submit to us (e.g. via your POS terminal or for eCommerce transactions) must fully comply with the applicable provisions of your Agreement. Submission of an Authorization request that does not fully comply may result in an Assessment of additional fees to you (if permitted under, and subject to, your Agreement), a declined Authorization response or a Chargeback to you.

An Authorization approval code only indicates the availability of funds on an account at the time the Authorization is requested. It does not warrant that the person presenting the Card is the rightful Cardholder, nor is it a promise or guarantee that you will not be subject to a Chargeback and/or adjustment. You must obtain an Authorization approval code from us for all transactions.

- Failure to obtain an Authorization approval code for a sales transaction may result in a Chargeback and/or the termination of your Agreement. Authorization approval codes can be obtained through your POS terminal. Fees (if any) related to Authorizations will be charged per each request for an Authorization approval code, whether or not the transaction is approved.
- **For card-present Transactions:** It is highly recommended that you use your electronic authorization device to capture Card data using the POS terminal by inserting the Card (Chip Card), swiping the Card (Magnetic Stripe) or tapping/waving the Card (contactless).
- **For card-not-present Transactions:** You must obtain the three-digit Card Verification Code on the back of the Card (or the four-digit Card Verification Code on the front of American Express Cards) and include this code with each *card-not-present* Authorization request unless the transaction is a recurring transaction. However, for recurring transaction Authorizations you submit the Card Verification Code only with the first Authorization request, not with subsequent recurring transaction Authorization requests.
- Do not attempt to obtain an Authorization approval code provided by someone other than us except as described in relation to “Authorization by Third Party Vendors” as described in this Operating Guide. If a Cardholder or another service provider provides you with either an Authorization approval code or with a telephone number for obtaining Authorizations, the Authorization approval code you receive may not be valid. Even if the transaction is initially processed and funded, it may be charged back at a later date. Also, if you receive a purported Authorization approval code from someone other than us, we will not have the supporting records and will be unable to verify that you received the Authorization if that is later questioned in a Chargeback.
- If you utilize AVS, you must review the AVS response separately from the Authorization response and make your own decision about whether to accept the transaction. A transaction can receive an Authorization approval code from the Issuer even if AVS is unavailable or reflects that the address provided to you does not match the billing address on file at the Issuer. If the authorized Cardholder disputes such a transaction, you will be responsible for the resulting Chargeback.
- If you receive a referral response to an attempted Authorization for any Card type, please ask for another form of payment. After receiving a referral response you may not attempt another Authorization on the same Card through your POS terminal.
- If you fail to obtain an Authorization approval code or if you submit a Card Transaction after receiving a decline (even if a subsequent Authorization attempt results in an Authorization approval code), your transaction may result in a Chargeback and may be assessed fines or fees by the Card Networks for which you will be responsible. To avoid these costs and related Chargebacks, always obtain an Authorization approval code directly from your terminal before submitting a Card Transaction for settlement.
- You may not attempt to obtain multiple Authorizations for a single transaction, except when incremental Authorizations are allowed. Refer to the discussion on Customer Activated Terminals and Self-Service Terminals in this Operating Guide and the American Express Merchant Operating Guide (www.americanexpress.com/merchantopguide) with respect to American Express Card transactions regarding additional provisions for specific industries. If a sale is declined, do not take alternative measures with the same Card to obtain an approval of the sale

from other Authorization sources. Instead, request another form of payment. If you accept and process a transaction that was declined, or attempt multi-transactions and/or multi-Authorizations, you are subject to a Chargeback, Card Network fines and/or cancellation of your Agreement. Do not discuss reason for decline with a Cardholder; rather refer them to the customer service number on the back of the Card.

- Any requests for Authorization which do not lead to a request for the Issuer to allocate funds for settlement within the timing specified by the applicable Card Network Rules after such request for Authorization will automatically expire.
- **If you have been classified by Discover as having a “Discover Direct Strategic Relationship” with Discover, we will not acquire your Discover transactions and they will be subject to your agreement with Discover. We may authorize your transactions with Discover Card, however, other aspects of processing of your Card Transactions with Discover Cards will be based on your direct relationship with Discover. You may also be responsible for all Assessments, Chargebacks or other fees payable to Discover**

NOTE: We will not acquire any Card Transactions that are subject to a separate agreement or relationship with a particular Card Network relating to the direct acquiring of Card Transactions (“**External Card Transactions**”). Those External Card Transactions will be subject to your agreement with such Card Network(s). You acknowledge and agree that if we have not agreed to or do not acquire Card Transactions for a Card type: (i) we will have no liability or responsibility for the settlement of or disputes regarding those transactions; and (ii) you shall pursue directly with the related Card Network all claims and disputes regarding those transactions.

Authorization via Electronic Devices

- If you use an electronic terminal (e.g. a POS terminal) to obtain an Authorization approval code, all sales should be authorized through this equipment. Authorizations through other methods may result in additional charges to you. In the event your terminal is not functioning then you may be able to use a virtual terminal to conduct a transaction until your terminal is functioning. Please contact Customer Service with any questions.

Authorization via Telephone

- We do not offer authorization by telephone. In the event the Cardholder has an issue with their transaction, please request another form of payment and request that they call the Card Issuer 800 number on the back of their Card.

Authorization via Third-Party Authorization Systems

- If you have contracted with another Authorization network to obtain Credit Card Authorization, liability resulting from discrepancies with that network must be resolved between you and that network.
- If an Authorization provided by a third-party Authorization system is challenged in a Chargeback, you must obtain proof (e.g. third-party Authorization logs) from the Authorization source and submit it to us within the time frame specified on the Chargeback documentation.

IF YOU CONTRACTED TO USE ONE OF OUR AUTHORIZATION SERVICES, YOU MUST NOT USE ANOTHER THIRD-PARTY AUTHORIZATION SYSTEM WITHOUT VERIFYING THEY ARE PROPERLY REGISTERED. THIS CAN BE DONE BY NOTIFYING CUSTOMER SERVICE AND HAVING THEM CHECK THE REGISTRATION STATUS. OTHERWISE, WE WILL BE UNABLE TO SUCCESSFULLY RESEARCH AND DEFEND ANY AUTHORIZATION RELATED CHARGEBACKS ON YOUR BEHALF. THIS DELAY WILL SIGNIFICANTLY DECREASE YOUR TIME TO RESEARCH AND PROVIDE PROOF OF AUTHORIZATION, THUS REDUCING YOUR OPPORTUNITY TO REVERSE A CHARGEBACK.

Authorization via Third-Party Vendors

- You must confirm our approval prior to using any vendor that is providing services that stores, processes, or transmits Cardholder data. This includes, but is not limited to: Authorization, encryption key/software application loading, terminal driving/servicing (remote servicing), and shopping carts. This can be done by notifying Customer Service and having them check the registration status.
- You are responsible for assisting us in collecting any information that we may require on Third Party Vendors that you use (e.g. associated with our due diligence processes on Third Party Vendors). You are responsible for any registration fees incurred in this process.
- If you utilize another Authorization network, you will be responsible for the downgrade of any transactions to a higher-cost interchange that result from a mismatch of information to our systems and those of third-party Authorization networks.

- If you use a third-party Authorization network, you must also comply with this Section 5 of this Operating Guide.

Authorization Timeframes

- Please note the below Authorization response validity timeframes. These timeframes provide an indication to you and your customers on when Card Transactions are settled and when payment can be received by you:
 - (i) For **Mastercard**, a positive Authorization response remains valid for:
 - a. Seven (7) days for electronic processed transactions that are coded as final or undefined Authorizations.
 - b. Thirty (30) days for those coded as pre-Authorizations.
 - (ii) **Visa** has introduced a single point of reference for the length of time an estimate/initial Authorization is valid to complete the transaction:
 - a. Lodging, vehicle rental, cruise lines: Thirty-one (31) days from day of initial Authorization approval.
 - b. Commuter transportation, bus, railway merchants: Seven (7) days (in the U.S. three (3) days) from the date of initial Authorization approval.
 - c. Other rental merchant categories: Seven (7) days from day of initial Authorization approval.
 - d. Other *card-present* Transactions: Day of the approval (same as transaction date).
 - e. Other *card-not-present* Transactions: Seven (7) days from day of initial Authorization approval.
 - (iii) A **Discover** positive Authorization response remains valid for:
 - a. Seven (7) days and ten (10) days for **Discover** electronic processed transactions subject to the following exception.
 - b. A positive Authorization response for Discover will remain valid for thirty (30) days for the following industries - car rental, airline and passenger railway, lodging and other Travel and Entertainment (“T&E”) categories.
 - (iv) A positive Authorization response for **American Express**:
 - a. Seven (7) Days for Non-T&E electronic processed transactions
 - b. American Express T&E positive Authorizations are good for thirty (30) days.

5.3 Authorization of Special Card Transactions

Delayed Deliveries

- In a delayed delivery transaction where a Cardholder makes a deposit toward the full amount of the sale, you should process two separate Card Transactions, the first for a deposit and the second for payment of the balance upon delivery of the merchandise or the performance of the services.
- The procedure for each Card Network is set out below:
 - (i) Visa
 - You must obtain an Authorization for each Card Transaction on each transaction date.
 - You must ensure that separate Authorization approval codes are assigned to each Card Transaction, respectively.
 - (ii) Mastercard:
 - For Mastercard transactions, you must obtain an Authorization for each Card Transaction on each transaction date.

NOTE:

For Visa and Mastercard transactions, if delivery is more than twenty-five (25) days after the original transaction date and the initial Authorization request (as opposed to the thirty (30) days in Discover transactions), you should reauthorize the unprocessed portion of the transaction prior to delivery. If the transaction is declined, contact the Cardholder and request another form of payment.

- (iii) Discover:

- You shall submit Authorization requests you receive and await receipt of the Authorization response prior to completing the Card Transaction.
- A positive Authorization response will remain valid for thirty (30) calendar days from the date of the Authorization response for Card Transactions in the car rental industry, airline and passenger railway industries, the lodging industry and other travel MCCs, including passenger transport and all international Card Transactions.
- A positive Authorization response will remain valid for ten (10) calendar days from the date of the Authorization response for Card Transactions in all other industries and MCCs.
- In addition, you must utilize AVS at the time of the “balance” Authorization, and you must obtain proof of delivery upon delivery of the services/merchandise purchased.
- You may not submit sales data relating to the “balance” to us for processing until the merchandise/ service purchased has been completely delivered.

(iv) American Express:

- For American Express Card Transactions, you must clearly disclose your intent and obtain written consent from the Cardholder to perform a delayed delivery transaction before you request an Authorization.
 - You must obtain a separate Authorization approval for each delayed delivery transaction on their respective charge dates and clearly indicate on each record that the charge is either for the deposit or for the balance of the transaction.
 - You must submit the delayed delivery transaction record for the balance of the purchase only after the items have been shipped, provided or services rendered.
 - For deposits, submission must be on the date the Cardholder agreed to pay for the deposit for the purchase.
 - For balances, submission must be on the date the items are shipped, provided or services rendered.
 - You must submit and authorize each delayed delivery transaction under the same Merchant Account Number and treat deposits on the Card no differently than you treat deposits on all other payment products.
- If delivery is longer than the allowable timeframes after the initial Authorization request, per payment type, the Authorization must be reversed for the unused portion and a new Authorization obtained for the remaining amount prior to delivery:

- (i) Seven (7) days (Mastercard, Visa, American Express; and
- (ii) Ten (10) days (Discover Network and PayPal transactions).

Pre-Authorization for T&E and Restaurant Merchants

- If you are a business engaged in providing travel and/or entertainment (i.e. “T&E”) services (e.g. car rentals, hotels, motels, etc.) or a restaurant business, and engage in the practice of “pre-Authorization”, you must comply with the following general procedures:
 - (i) You must notify the Cardholder of the dollar amount you intend to pre-authorize.
 - (ii) A hotel, motel, or car rental merchant may obtain an estimated Visa, Mastercard or Discover Authorization at the time of check-in.
 - (iii) If you receive a decline on a transaction, you must wait twenty-four (24) hours before attempting to reauthorize. If you reauthorize prior to this time frame and receive an approval, you may be subject to a Chargeback and a fine imposed by the Card Networks.
 - (iv) With the exception of Mastercard Card Transactions, hotels, motels, and car rental merchants are allowed up to a 15% variance above the amount authorized. If the final amount charged to the Cardholder exceeds the original estimate by more than 15% above the pre-Authorization, you must authorize any additional amounts, and all incremental Authorization approval codes must be written in the Authorization area along with the date of Authorization and the amount authorized.
 - (v) The Card Network Rules provide that certain establishments' services are permitted to submit a pre-Authorization of up to a 20% (instead of 15%) above the amount authorized. If the final amount exceeds the amount pre-authorized by more than 20%, you must authorize the additional amount.

NOTE: For Mastercard Card Transactions, the 20% amount tolerance between Authorization and clearing for tipping is only permissible for *card-present* Magnetic Stripe or contact Chip Card Transactions with either a signature Cardholder verification method or no Cardholder verification method. Estimating the Authorization amount to include a tip is prohibited. The Authorization request should include only the amount associated with the bill presented to the consumer.

- (vi) You must obtain an Authorization for the initial estimated charges and then monitor the charges to ensure that the actual charges made do not exceed the estimated charges. If the actual charges exceed the amount of the initial estimated Authorization (and any subsequent estimated Authorizations), then you must secure a positive Authorization for the additional amount.

NOTE: Subsequent Authorizations should only be for the additional amount of total charges and must not include amounts already authorized.

- (vii) The estimated amount of any pre-Authorization for lodging accommodations must be based on:

- (a) The intended length of stay;
- (b) The room rate;
- (c) Applicable taxes and service charges; and/or
- (d) Other miscellaneous charges as dictated by experience.

- (viii) If an Authorization request is declined, no charges occurring after that date will be accepted for that Cardholder.

- (ix) With the exception of Mastercard Card Transactions, you do not need to obtain a final Authorization if the total sum of charges (the final amount) does not exceed 20% of the previously authorized charges. For Discover, you need not obtain a final authorization at the end of the vehicle rental period if the final amount of the Cardholder's charges does not exceed 115% of the sum of the charges estimated by you with respect to which you obtained an Authorization response.

- (x) Restaurants must not add an estimated tip amount to the Authorization request beyond the value of the goods provided, or services rendered, plus any applicable tax.

- (xi) **VEHICLE RENTAL PROVIDERS MAY NOT INCLUDE POTENTIAL VEHICLE DAMAGE OR INSURANCE DEDUCTIBLES IN ANY PRE-AUTHORIZATIONS.**

Merchants in the Lodging Industry

Lodging Rules

- There are additional rules and requirements that apply to merchants in the lodging industry for practices, including, but not limited to, guaranteed reservations and charges for no shows, advance deposits, overbookings, and priority check out. Failure to do so could result in additional charges or termination of your Agreement.

- (i) **Written confirmation of guaranteed reservations:** You must provide the Cardholder with written confirmation of a guaranteed reservation. The confirmation must contain:

- Cardholder's name as it appears on the Card, if present;
- Card number, if truncated where required by Applicable Law and Card expiration date if present, unless prohibited by Applicable Law;
- Reservation confirmation number;
- Anticipated arrival date and length of stay;
- The cancellation policy in its entirety, inclusive of the date and time the cancellation privileges expire; and
- Any other pertinent details related to the reserved accommodations.

- (ii) **Cancellation of guaranteed reservations:** If a Cardholder requests a cancellation in accordance with your cancellation policy and specified time frames, you must provide the Cardholder with a cancellation number and instructions to retain a record of it. If a Cardholder requests a written confirmation of the cancellation, you must forward this confirmation within three (3) Business Days of the Cardholder's request. The cancellation confirmation must contain: Cardholder's reference that charges were placed on the Card, if applicable, or a guarantee that a "no-show" charge will not be placed on the Card. The information to be recorded is as below:

- Cardholder's name as it appears on the Card, if present;
- Card number, truncated as required by Applicable Law to you or us;
- Card expiration date, if present, unless prohibited by Applicable Law to you or us;

- Reservation cancellation number;
- Date of cancellation;
- The name of your employee that processed the cancellation; and
- Any other pertinent information related to the reserved accommodations.

Lodging Service Programs

- In the event you are a lodging merchant and wish to participate in Visa's and/or Mastercard's lodging services programs, please contact your sales representative or relationship manager for details and to obtain information on the appropriate Visa and Mastercard requirements.

Advance Payment Charges

- Please follow the procedures set out in this Section if you permit or require Cardholders to make advance payment charges for:
 - (i) Custom orders (for example, orders for goods to be manufactured to a customer's specifications);
 - (ii) Ticketing for events or entertainment (for example, sporting events or concerts);
 - (iii) Tuition, room, board, and other mandatory fees (for example, library or other students services fees at universities);
 - (iv) Tickets for airlines, rail lines, cruise lines, lodging, and other travel-related services (for example, tours or guided expeditions);
 - (v) Vehicle rentals; or
 - (vi) In-store merchandise not immediately available (for example, merchandise pre-purchased for an upcoming sale event or merchandise on layaway).
- **For all advance payment transactions:**
 - (i) State your full cancellation and refund policies;
 - (ii) Clearly disclose your intention to receive advance payment;
 - (iii) Before you request an Authorization, do obtain written consent from the Cardholder to bill the Card for an advance payment charge; the Cardholder's consent must include (1) a detailed description of the goods or services to be provided, and (2) his or her agreement to all of the terms of the sale, including price, any cancellation or refund policies, and the expected delivery date of the goods or services;
 - (iv) Obtain an Authorization approval; and
 - (v) If you cannot deliver the goods or services (for example, because custom-ordered merchandise cannot be fulfilled) and cannot make other arrangements, do immediately issue a credit for the full amount of the advance payment charge.

- **For card-not-present Transactions involving an advance payment:**

Within twenty-four (24) hours of the advance charge being authorized (**or, in the case of a transaction using a Visa Card, at the time of the payment**), provide the Cardholder with written confirmation (for example, by e-mail or facsimile) that an advance payment charge has been made, the written confirmation must include:

- a detailed description of the goods or services to be provided;
- the amount of the charge;
- the confirmation number (if applicable);
- the details of any cancellation or refund policies; and
- the expected delivery date of the goods or services.

Recurring Transactions and Preauthorized Orders

- If you process recurring transactions and charge a Cardholder's account periodically for recurring goods or services (e.g. yearly subscriptions, annual membership fees, etc.), the Cardholder is required to complete and deliver to you a Cardholder approval for such goods or services to be charged to his account.
- The approval must at least specify the Cardholder's name, address, account number and expiration date, the transaction amounts, the timing or frequency of recurring charges and the duration of time for which the Cardholder's permission is granted. For Discover transactions, the

approval must also include the total amount of recurring charges to be billed to the Cardholder's account, including taxes and tips and your Merchant Account Number.

- If the recurring transaction is renewed, the Cardholder must complete and deliver to you a subsequent written request for the continuation of such goods or services to be charged to the Cardholder's account. **You may not complete a recurring transaction after receiving a cancellation notice from the Cardholder or Issuer or after a request for Authorization has been denied.**
- If we or you have terminated your Agreement, you may not submit Authorization requests or sales data for recurring transactions that are due after the termination date of your Agreement.
- You must obtain an Authorization for each Card Transaction. A positive Authorization response for one recurring transaction Card Transaction is not a guarantee that any future recurring transaction Authorization request will be approved or paid.
- **For all Discover recurring transactions:** You should submit the three-digit Card identification number with the first Authorization request, but not subsequent Authorization requests. Discover Card Network Rules specifically require that you follow this CID procedure for Discover recurring transactions.
- **For American Express recurring transactions:** You should periodically verify with Cardholders that their information (e.g. Card number, expiration date, billing address) is still accurate. This will improve the likelihood of obtaining an approval to an Authorization request. The cancellation of an American Express Card constitutes immediate cancellation of that Cardholder's consent for recurring Charges. American Express will not have any liability from such cancellation. If an American Express Card is cancelled or a Cardholder withdraws consent to recurring charges, you are responsible for arranging another form of payment with the Cardholder.
- The method to secure consent for recurring charges must contain a disclosure that you may receive updated Card account information from the Issuer. You must retain evidence of consent to receive updated Card account information from the Issuer for twenty-four (24) months from the date you submit the last recurring billing charges. If you offer Cardholders the option to make recurring billing charges, you must:
 - (i) Ensure that your process for cancellation of recurring billing is simple and expeditious;
 - (ii) 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 Cardholder;
 - (iii) Within twenty-four (24) hours of incurring the first recurring billing charge, provide the Cardholder written confirmation (e.g. email or facsimile) of such charge, including all material terms of the option and details of your cancellation/refund policy; and
 - (iv) Where the material terms of the option change after submission of the first recurring billing charge, promptly notify the Cardholder in writing of such change and obtain the Cardholder's express written consent to the new terms prior to submitting another recurring billing charge.
- All recurring transactions or preauthorized orders may not include partial payments for goods or services purchased in a single transaction.
- You may not impose a finance charge in connection with a recurring transaction or preauthorized order.
- If you process recurring payment transactions, the "Recurring Payment Indicator" must be included in each Authorization request, and as applicable, each batch submission entry. Penalties can be assessed by the Card Networks for failure to use the "Recurring Payment Indicator".

Installment Payments

- If you process multiple payments for a single purchase of goods or services over a period of time based on an agreement between a Cardholder and your business (e.g. a car payment or furniture purchase) please follow the procedures set out below:
 - (i) Do obtain written Cardholder approval for goods or services to be charged on an instalment basis to the Cardholder's account at the time of the first transaction. Approval must at least specify:
 - Terms of service.
 - Timing of delivery to Cardholder.
 - Transaction amount.
 - Total purchase price.
 - Terms of future payments, including dates, amounts, currency, cancellation and refund policies.

- Any associated charges, including shipping and handling charges and any applicable taxes.
- (ii) The instalment transaction amount must be less than the total price of the merchandise or services purchased (may include interest charges, except in the US Region) and must be applied to the total obligation.
- (iii) Do obtain an Authorization for each Card Transaction.
- (iv) Contact the Cardholder in writing if Authorization is declined and allow at least seven (7) calendar days for payment by other means.
- (v) Provide the following to the Cardholder within three (3) Business Days if they cancel within the terms of the cancellation policy:
 - Cancellation or refund confirmation in writing.
 - Credit transaction receipt for the amount specified in the cancellation policy.
- (vi) Process a refund for the full amount paid if unable to adhere to the terms of the sale or service.
- (vii) Do include the instalment payment indicator in the authorization request.
- (viii) Do not impose a convenience fee in connection with an instalment payment.
- (ix) Do not process instalment transactions at intervals less than:
 - Seven (7) calendar days.
 - The monthly anniversary of the shipment date for the U.S. region.

Customer Activated Terminals and Self-Service Terminals

- Transactions processed at customer-activated terminals and self-service terminals have specific requirements for processing. Prior to conducting “Customer Activated Terminal” (“**CAT**”) transactions or “Self-Service Terminal” transactions for Mastercard, Visa or Discover you must contact us for approval and further instructions, rules and requirements that apply to such transactions. Failure to do so could result in additional charges or termination of your Agreement.
- **Customer Activated Terminals for American Express Transactions:** Charges for purchases at your CATs must include:
 - (i) Full Magnetic Stripe data stream or chip Card data in all Authorization requests; and
 - (ii) CAT indicator on all Authorization requests and submissions.

American Express will not be liable for actual or alleged fraudulent charges occurring through CATs and will have the right to Chargeback for those charges.

Cash Over (also known as Cash Back) Transactions

- “**Cash Over**” transactions are transactions which permit customers to obtain cash above the amount of a particular sale transaction.
- Please contact Customer Service to inquire about the possibility of offering Cash Over transactions.

Telecommunications Transactions

- Telecommunication Card Transactions occur when a telephone service provider is paid directly using a Card for individual local or long-distance telephone calls. (**NOTE:** Pre-paid telephone service cards are not and do not give rise to Telecommunication Card Transactions).
- **Prior to conducting Telecommunication Card Transactions you must contact us for approval and further instructions, rules and requirements. Failure to do so could result in additional charges or termination of your Agreement.**

5.4 Modification of Authorizations

Partial Authorization

- Partial Authorization provides an alternative to a declined transaction by permitting an Issuer to return an Authorization approval for a partial amount, an amount equal to or less than the transaction amount requested by the merchant when the available Card balance is not sufficient to approve the transaction in full. The Cardholder is able to use up the remaining funds on the Card and select another form of payment (i.e. another Card, cash, check) for the remaining balance of the transaction.
- In the event that you wish to support the partial Authorization functionality, you must contact us for additional rules and requirements.
- Please refer to the below for Card Network-specific details on partial Authorizations:
 - (i) **For Discover Credit Cards or Debit Cards:** Partial Authorization support is optional for *card-not-present* Transactions.
 - (ii) **For Mastercard transactions:** Partial Authorization is optional for batch-authorized electronic commerce transactions, mail order and telephone order transactions, and recurring transactions.
 - (iii) **For Visa transactions:** Partial Authorization is optional, except for automated fuel dispenser and PIN Debit Transactions with cash-back.
- If you support partial Authorizations, a partial Authorization indicator must be included in each Authorization request.
- The transaction sent for settlement must be no more than the amount approved in the partial Authorization response.

Authorization Reversals

- An Authorization reversal must be submitted if the Authorization is no longer needed, a partial amount of the total authorized is submitted for the settled transaction, or the Cardholder elects not to complete the purchase.
- An Authorization reversal may only be submitted if the transaction has not settled. Once the transaction has settled, only a Credit or Refund can occur.

Sale Reversals

- You may request to reverse sales processed from time to time which were either submitted in error by you or a result of fraudulent activity.
- **By requesting that we process sale reversals, you understand and accept that although the sales are being reversed by us, you bear all responsibility to respond to any Chargebacks received for reversed sales. Failure by you to respond within an appropriate timeframe will cause a duplicate debit of the same amount from your Settlement Account by the reversal of the sale and the Chargeback.**

Discover Procedure for Request for Cancellation of Authorization

- If a Discover Card Transaction is cancelled or the amount of the transaction changes following your receipt of Authorization for the sale, you must process an Authorization reversal via your POS terminal. An Authorization may be cancelled at any time within ten (10) days of your receipt of the Authorization, but must be cancelled before the sales data relating to the transaction is submitted to us, after which the Authorization cannot be changed.

Cash Payments by and Cash Disbursements to Cardholders

You must not accept any direct payments from Cardholders for Card Transactions relating to charges for merchandise or services; it is the right of the Issuer to receive such payments. You may not make any cash disbursements or cash advances to a Cardholder as part of a Card Transaction unless you are a financial institution that has received express written authorization from Bank of America, N.A. Merchant Services, in advance. For Discover, cash advances in authorized jurisdictions other than the United States may be conducted in an originating currency provided that cash advances may be subject to dispute and/or other fees.

6. Refunds and Exchanges

6.1 Overview

- You may experience a situation where you are required to process a Refund or exchange for a customer who has paid utilizing a Card.
- When you process a Refund, the relevant transaction amount being refunded is debited from your Settlement Account while the Cardholder receives that transaction amount returned to the Card used for that transaction.
- You are required to adhere to the requirements and procedures in this Section 6 of this Operating Guide when processing any Refunds or exchanges to your customers.

6.2 Refunding Card Transactions

- Please ensure that you only process a Refund where you have provided a Cardholder with goods and services and only in relation to the Card used by that Cardholder for this transaction.
- Unless required by Applicable Law, you are not permitted to provide a Refund in cash to a Cardholder where that Cardholder utilizes a Card for the transaction the subject of the Refund Request. Any Refund Request is to be processed in the same currency as the original payment transaction.
- We may cease providing you with the Merchant Services in the event you breach these requirements and/or the requirements under your Agreement. Any non-compliance is also a breach of your Agreement.

Refunds Using Your POS Terminal

- When using your POS terminal to process a Refund Request please adhere to the instructions accompanying the specific model of your POS terminal when processing a Refund Request. You may have designated only specific members of staff to have the authority to process Refund Requests (e.g. via the use of a “Supervisor” PIN or Authorization device).
- You are required to issue a receipt to the Cardholder when you process a Refund Request.
- You should adhere to the below rules when processing Refunds:
 - (i) You must select “Credit” or “Refund” on your device, then key, swipe or insert the Card and enter the Refund amount. Your terminal may authorize the Refund Request. Provide your customer with a Refund receipt.
 - (ii) All Refunds should be deposited with your daily transactions and not held for deposit at a later date.
 - (iii) You cannot process a credit transaction that does not correspond to a previous sale / purchase transaction for the original Card Transaction (e.g. as evidenced on a transaction receipt).
 - (iv) Full Refunds must be for the exact dollar amount of the original transaction including tax, handling charges, etc. (You must identify the shipping and handling charges incurred.) The Refund amount may not be for more than the original Card Transaction amount.
 - (v) All dollar amounts and other handwritten information must be clearly written.
 - (vi) **You should not credit an account that differs from the account used for the original transaction.**
 - (vii) Never give cash or check Refunds or other consideration for Card Transactions, with the exception of the following types of Visa transactions only:

- Visa Easy Payment Service Transaction (Visa's 'no signature required' program);
- A gift purchased as a MOTO transaction; or
- Visa prepaid Card Transaction if the Cardholder states that the Visa prepaid Card has been discarded.

(viii) You cannot intentionally submit a sale and an offsetting Credit at a later date solely for the purpose of debiting and crediting your own or a customer's account.

(ix) You are responsible for paying all Refunds submitted to us on your account. We assume no responsibility for verifying any Credits or Refunds.

(x) Do not process a Credit transaction once a Chargeback is received. Credits issued after a Chargeback has been received may not be recoverable, and you will be financially responsible for the Credit as well as the Chargeback.

(xi) **YOU ARE RESPONSIBLE TO SECURE YOUR TERMINALS AND TO INSTITUTE APPROPRIATE CONTROLS TO PREVENT EMPLOYEES OR OTHERS FROM SUBMITTING CREDITS THAT DO NOT REFLECT BONA FIDE RETURNS OR REIMBURSEMENTS OF PRIOR TRANSACTIONS.**

(xii) **For Discover transactions only:** Include the last 4 digits of the merchant identification number.

- If unable to process the Refund Request to the same Card number, you may either:

(i) Process the Refund to a secondary Card number, if available, and if a transaction receipt or other proof of purchase exists, and either:

- The original Card number is unavailable (account is closed, transferred, reported lost/stolen);
- An Authorization request for the Refund to the original Card number receives a "Declined" response.

(ii) Refund the Card Transaction amount through alternate means (cash, check, in-store credit, or prepaid card), if any of the following conditions apply:

- The Cardholder does not have a transaction receipt or other proof of purchase.
- The customer is not the original Cardholder and is returning a gift.
- The Cardholder claims that the Visa Prepaid Card used for the original purchase has been discarded.
- The Authorization request for a Refund to the original or secondary Visa.
- Card number receives a "Declined" response.

Refunds Processed for American Express Transactions

- There are additional requirements for a Refund for purchases or payments made on an American Express Card. **To issue a Refund, you must:**

(i) Compare the last four digits on the relevant transaction receipt against the Card presented (when applicable).

(ii) Have the Cardholder sign the Refund transaction receipt (when applicable).

(iii) Provide a copy of the Refund transaction receipt to the Cardholder.

- You must not issue a Refund when there is no corresponding charge, nor issue a Refund in exchange for cash (subject to the below) or other consideration from a Cardholder. You must submit all Refunds under the establishment where the Refund originated. A Refund must be issued in the currency in which the original charge was submitted to us. You must issue Refunds to the Card used to make the original purchase; however, if the Refund is for the return of a gift by someone other than the Cardholder who made the original purchase, apply your usual Refund policy.

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

- (i) For all Cards except prepaid Cards, advise the Cardholder that you must issue the Refund to that Card. If the Cardholder has questions, advise him or her to call the customer service number on the back of the Card in question.
 - (ii) If the inactive or unavailable Card is a prepaid Card, apply your usual policy for returns.
- If you issue a Refund, American Express will not return the discount or any other Fees or Assessments previously applied on the corresponding charge. The discount on Chargebacks will not be returned.

6.3 Return Policy Recommendations

- Your return and cancellation policies must be fair and clearly disclosed at the time of sale in compliance with Applicable Law. Your policies must be conveyed to the Cardholder prior to completion of the charge and printed on a copy of a receipt. Your Refund policy for purchases on the American Express Card must be at least as favorable as your Refund policy for purchases made with other payment products or other payment methods.
- Examples of Refund policies that should be clearly visible to the cardholder
 - (i) “Full refund if returned within seven (7) days”: This policy is relevant when you accept returns for Refunds and specify for how many days after the receipt date that a Refund is available.
 - (ii) “In-store credit only”: Your establishment takes returned merchandise and gives the Cardholder an in-store credit for the value of the returned merchandise.
 - (iii) “Exchanges Only”: Your establishment is willing to exchange returned merchandise for similar merchandise that is equal in price to the amount of the original transaction.
 - (iv) “No refunds or returns or exchanges”: Your establishment does not issue Refunds and does not accept returned merchandise or merchandise exchanges.
- Provide clear return instructions for your customers, including the following information:
 - (i) Customer service telephone number.
 - (ii) Reference number for the return.
 - (iii) Expected processing time for the Refund.
 - (iv) Return address, preferably on a pre-formatted shipping label (if applicable).
- You must submit all Credits to us within seven (7) days of determining that a Refund is due.

American Express Return Policy for Prepaid Products

- If your return policy for the purchase of prepaid products is different from your standard return policy, you must ensure that such prepaid product-specific return policy is clearly disclosed to the Cardholder at the time of purchase in accordance with Applicable Law and also coded to print on all transaction receipts you provide to Cardholders.

6.4 Cancellation Policy Recommendations

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

6.5 Exchanges

- No additional documentation is necessary for a straightforward exchange; just adhere to your standard company policy.
- For an uneven exchange, complete a credit transaction for the total amount of only the merchandise returned. The Cardholder’s account will be credited for that amount. Then, process a new Card Transaction for the total amount of any new merchandise purchased.

6.6 Refund Reversals

- You may submit a request to attempt to reverse Refunds from time to time (a “**Refund Reversal**”). There is no guarantee that a Refund Reversal will be successful, and if unsuccessful, the reversal attempt will be returned to you as a “**non-compliance chargeback**”.
- **You are wholly responsible for all Chargebacks and related Fees, including non-compliance chargebacks for failed Refund Reversals. By requesting that we process Refund Reversals, you understand and accept the risks and agree to bear the financial responsibility for all Chargebacks and Fees.**

6.7 Additional Guidance

- If you limit Refund / exchange terms or impose other specific conditions for Card Transactions, the words “No Exchange, No Refund,” etc. must be clearly printed (in 1/4" letters) on the relevant transaction receipt near or above the Cardholder’s signature. The Cardholder’s copy, as well as your copy, must clearly show this information.
- During a liquidation and/or closure of any of your outlets, Locations and/or businesses, you must post signs clearly visible to customers stating that “All Sales Are Final,” and stamp the relevant transaction receipt(s) with a notice that “All Sales Are Final”.

A disclosure does not eliminate your liability for a Chargeback. Consumer protection laws and Card Network Rules frequently allow the Cardholder to dispute these items notwithstanding such disclosures.

7. Data Security

THE FOLLOWING IS IMPORTANT INFORMATION REGARDING THE PROTECTION OF CARDHOLDER DATA. PLEASE REVIEW CAREFULLY. YOUR OBLIGATIONS IN THIS SECTION INCLUDE RESPONSIBILITY FOR POTENTIALLY SIGNIFICANT FEES, FINES AND ASSESSMENTS.

7.1 Payment Card Industry Data Security Standards

- As part of your obligation to comply with Card Network Rules, you are required to comply with the Payment Card Industry Data Security Standards (“PCI DSS”).
- PCI DSS compliance is focused on Merchant Systems where Cardholder data can be accessed, processed, stored, or transmitted, including external connections into your network, connections to and from the authorization and settlement environment (e.g. connections for employee access or for devices such as firewalls and routers), and data repositories outside of the authorization and settlement environment. Information about PCI DSS can be found at www.pcisecuritystandards.org.
- You also are solely responsible for ensuring that all Merchant Providers, Merchant Systems, Third Parties, services provided by Third Parties, Merchant Equipment, and Software that you use in connection with Card Transactions comply with Card Network Rules, including PCI DSS.

7.2 Security Policies and Procedures

- You are responsible for establishing and maintaining security policies and procedures that prevent unauthorized access to, disclosure of, and use of Cardholder data. As part of this obligation you must implement:
 - (i) all steps required to comply with PCI DSS, including ensuring all Merchant Providers, Merchant Systems, Third Parties, Third-Party Services, Merchant Equipment, and Software you use in connection with your payment processing comply with PCI DSS;
 - (ii) appropriate controls to limit access to, and render unreadable prior to discarding, all records containing Cardholder account numbers, Card imprints, and other Cardholder data, including all Sensitive Authentication Data; and
 - (iii) firewalls, passwords, and other appropriate physical, administrative, and technical safeguards to protect against unauthorized access to your Merchant Systems, the Merchant Services, Software, and Cardholder data by your employees, contractors, Merchant Providers, customers, and other Third Parties (including instituting appropriate controls to prevent submission of sales and credits / returns that are not bona-fide transactions).
- You are also required to, in accordance with your Agreement that you entered into with us, ensure that you and your Merchant Providers comply with:
 - (i) the Visa Account Information Security Program;
 - (ii) the Mastercard Site Data Protection Program;
 - (iii) the Discover Network’s Information Security & Compliance; and
 - (iv) any relevant program established by any other applicable Card Network.
- You are required to demonstrate such compliance to us on our request and only use services, Merchant Providers, and Merchant Equipment that have been certified as PCI DSS compliant by the Card Networks.

In entering into your Agreement, you represent, warrant and undertake that no Security Breach relating to Transaction Data processed by you or on your behalf has occurred before, and remains unremedied on, the date on which your Agreement was executed by you and us. You must notify us immediately if this is not accurate.

7.3 Merchant Providers

- You must ensure that Merchant Providers comply with your Agreement (including provisions requiring security of Cardholder data), Card Network Rules, and Applicable Law.
- Before you engage any Merchant Provider, you must provide to us in writing the Merchant Provider’s legal name, contact information, and intended function. You cannot use or allow the use of any Merchant Provider, or provide any Merchant Provider access to any Cardholder data, Bank Systems, or Merchant Services, until you receive our approval and, if required, confirmation of our registration of that Merchant Provider with applicable Card Networks.
- You are responsible for all our costs and expenses associated with our review, approval, certification, recertification, and registration of Merchant Providers. In addition, you are responsible to us for your Merchant Providers’ acts and omissions related to your Agreement.

7.4 Secure Data

- You are responsible for:
 - (i) Keeping safe and confidential your passwords, Merchant Account information (including account numbers), security questions and answers, login details, and other information that could enable access to your Merchant Account or the Merchant Services; and
 - (ii) Restricting access to such information, and to the Merchant Services and your Merchant Account, to authorized personnel. You will immediately notify us of any unauthorized disclosure or use of any password, login details, or other account access information.
- You shall **not** at any time “store” (as defined under PCI DSS):
 - (i) a Card's verification value in the Card's Magnetic Stripe, on the Card, in or next to its signature panel, or in the Card's Magnetic Stripe image in a Chip application;
 - (ii) a PIN verification value in a Card's Magnetic Stripe;
 - (iii) the full contents of any track from a Card's Magnetic Stripe (on the Card, in a chip or elsewhere); or
 - (iv) any other data (including any Sensitive Authentication Data) that any of the Card Networks mandate from time to time as data that cannot be stored.
- You must notify us of all Persons who have access to Cardholder data on your behalf (i.e. store, process or otherwise transmit Cardholder data). You acknowledge such Persons are required by the Card Networks to be registered, and you shall cooperate with us in completing such registration and be responsible for all fees imposed by the Card Networks in connection with such registration.

7.5 Information We May Require

- You must provide us information (including responses to any questionnaire provided to you) that we or any Card Network requests regarding your compliance with Card Network Rules, including PCI DSS, or Applicable Law.
- As part of this obligation, you must provide us any information that we or any Card Network requests concerning any Compromised Data Event or suspicious transactions. We may share any such information with Card Networks, our Affiliates, our service providers, and government agencies.
- In addition, in the event of a Compromised Data Event or if requested by any Card Network, we, our representatives, or any forensic examiner approved by the PCI Security Standards Council, LLC may conduct remote electronic scans of Merchant Systems, including scans of IP addresses associated with your access to the Merchant Services. You must promptly cooperate to facilitate such scans and you are responsible for all related costs, expenses, and other amounts.
- Subject to the requirements of PCI DSS, you shall retain accurate copies of all Transaction Data for a minimum period of eighteen (18) months from the date of the relevant Card Transaction, Chargeback, Retro-Charge or Representment to which it relates.
- You are required to provide us with copies of such Transaction Data relating to any Transaction or Chargeback, Retro-Charge or Representment as we may request, in each case in such format as specified by us and within seven (7) days of such request.

7.6 Compromised Data Events

General Requirements

- If you become aware of any Compromised Data Event, you must at your expense:
 - (i) Contact us (and, as required under Card Network Rules, each Card Network) immediately and in no event more than twenty-four (24) hours after becoming aware of the Compromised Data Event;
 - (ii) Do not alter or destroy any related records, and must maintain complete and accurate documentation regarding any modifications made to any records;
 - (iii) Perform or cause to be performed an independent investigation of the Compromised Data Event, including a forensics analysis performed by a certified forensic vendor acceptable to us and the Card Networks (e.g. a PFI) no longer than twenty-four (24) hours following your suspected or actual discovery of that Compromised Data Event, and provide a copy of the certified forensic vendor's final report to us and the Card Networks;
 - (iv) Take (or cause to be taken) any acts that we or any Card Network recommends or requires;

- (v) Cooperate with us in the investigation and resolution of the Compromised Data Event and share with us any information related to the Compromised Data Event, including any information related to your or any Card Network's investigation of the Compromised Data Event; and
 - (vi) Not, without our prior written consent, take any action, or fail to take any action, which prejudices our rights under your Agreement (if you do so, it will be at your own risk, liability, and expense).
- In addition, at any time we and any Card Network may engage at your expense a forensic vendor to:
 - (i) investigate the Compromised Data Event;
 - (ii) examine the Merchant Systems and your and each Merchant Provider's procedures and records; and
 - (iii) issue a written report of its findings.

Merchant Provider's Compromised Data Events

- If a Merchant Provider experiences or is connected with a Compromised Data Event, you must require such Merchant Provider to comply with the requirements of your Agreement. If such Merchant Provider fails to do so, please be advised that we or the Card Networks may at your expense:
 - (i) Retain a certified forensic vendor acceptable to us and the Card Networks to perform an independent investigation, including a forensics analysis performed in accordance with Card Network Rules;
 - (ii) Provide a copy of the certified forensic vendor's final report regarding the Compromised Data Event and any related information to the Card Networks; and
 - (iii) Perform or cause to be performed, including on your behalf and any Merchant Provider's behalf, any actions recommended by any such investigation.

8. Chargebacks, Retrievals and Other Debits or Adjustments

8.1 Overview

- Generally, both the Cardholder and the Issuer have the right to question or dispute a transaction. If such questions or disputes are not resolved, a Chargeback may occur, and this Section of this Operating Guide describes the procedures that you should adhere to in the event of Chargebacks.
- As a result of a Chargeback, we will debit your Settlement Account or Settlement Funds for the amount of each Chargeback. As such, it is strongly recommended that, whenever possible, you contact the Cardholder directly to resolve a disputed transaction or Chargeback, unless the dispute involves a Discover Cardholder, in which case Discover Card Network Rules expressly prohibit you from contacting the Discover Cardholder regarding the dispute.
- You are responsible for all Chargebacks, our Chargeback fees, and related costs arising from your Card Transactions.

8.2 Chargeback Process

- Regardless of whether you respond to a transaction records request, a Chargeback may be debited to your Settlement Account for numerous reasons (see below). If the Issuer submits a Chargeback, we will send you a Chargeback notification, which may also include a request for transaction records.

Due to the short time requirements imposed by Visa, Mastercard, Discover and American Express, it is extremely important that you respond to a Chargeback notification and transaction records request within the timeframe as indicated on the Merchant Portal.

- Do not process a credit transaction once a Chargeback is received; the Issuer will credit the Cardholder's account. A Credit issued after a Chargeback has been received may not be recoverable, and you may be financially responsible for the Credit as well as the Chargeback.
- If the information you provide is both timely and, in our sole discretion, sufficient to warrant a representment of the transaction and/or reversal of the Chargeback, we will do so on your behalf. However, representment and/or reversal is/are ultimately contingent upon the Issuer and/or Cardholder accepting the transaction under applicable Card Network guidelines. Representment or reversal is not a guarantee that the Chargeback has been resolved in your favor.
 - (i) **For Visa Chargebacks:** If we reverse the Chargeback and represent the transaction to the Issuer, the Issuer, at its sole discretion, may elect to submit the matter for arbitration before Visa.
 - (ii) **For Mastercard Chargebacks:** If we reverse the Chargeback and represent the transaction to the Issuer, the Issuer, at its sole discretion, may elect to resubmit the Chargeback. In such event, at our discretion, we will debit your Settlement Account or Settlement Funds for the Chargeback. However, if you feel strongly that it is an invalid Chargeback, we may, on your behalf and at your request, submit the matter for arbitration before Mastercard.
 - (iii) **For Discover Chargebacks:** If Discover rejects our representment request and you feel strongly that the Chargeback is invalid, we may, at our discretion and on your behalf and at your request, submit the matter for dispute arbitration before Discover.
 - (iv) **For American Express Chargebacks:** You may request a Chargeback reversal if the Chargeback was applied in error. In order for your request to be considered, you must have responded to the original inquiry within the specified timeframe, request the Chargeback reversal no later than twenty (20) days after the date of the Chargeback, and provide all supporting transaction records to substantiate the error. If a Chargeback is applied, the Chargeback reversal can only be requested if you prove that you already issued a Credit to the Cardholder for the amount of the disputed charge.

- If the Chargeback is not disputed within the applicable time limits set forth by Visa, Mastercard or Discover Card Network Rules, as applicable, reversal rights are forfeited. Our only alternative, for Visa and Mastercard non-fraud Chargeback reason codes, is to attempt a “good faith collection” to the Issuer on your behalf. This process can take up to six (6) months and must meet the Issuer’s criteria (e.g. at or above a set dollar amount). Good faith collection attempts are not a guarantee that any funds will be collected on your behalf. Issuers normally charge good faith collection fees, which are deducted from the transaction amount if accepted in addition to any processing fees that are charged by us.
- **Please be advised that you will be responsible for all fees and charges imposed by the Card Networks in relation to any Chargebacks you receive, including any fees and charges incurred due to any dispute of a Chargeback. Any such fees and charges will be debited from your Settlement Account or Settlement Funds, in addition to the Chargeback.**

NOTE:

Visa and Mastercard Card Network Rules require that a merchant make a good faith attempt and be willing and able to resolve any disputes directly with the Cardholder.

Discover Card Network Rules and Regulations, however, prohibit you and/or us from contacting the Cardholder directly regarding dispute(s) or any other matter, except as required for acceptance of Discover transactions, and require you and/or us to submit any responses to dispute notices directly to Discover.

Due to Card Network Rules, you may not re-bill a Cardholder after a Chargeback is received for that transaction, even with Cardholder Authorization.

- We strongly recommend that you include a detailed rebuttal letter along with all pertinent documents when responding to a transaction records request or a Chargeback notification (e.g. rental agreement, relevant portion of the invoice or transaction receipt (in particular, the portion signed by the Cardholder and the area where the Authorization approval codes, with amounts and dates, are located)).
- Due to the short timeframes and the supporting documentation necessary to successfully (and permanently) reverse a Chargeback in your favor, we strongly recommend the following:
 - (i) Avoid Chargebacks by adhering to the guidelines and procedures outlined in this Operating Guide;
 - (ii) If you do receive a Chargeback, investigate, and if you dispute the Chargeback, submit the appropriate transaction records within the required time frame;
 - (iii) Whenever possible, contact the Cardholder directly to resolve the dispute, unless the dispute relates to a Discover Cardholder, in which case direct contact with the Discover Cardholder regarding the dispute is prohibited by Discover Card Network Rules;
 - (iv) If you have any questions, call Customer Service.

8.3 Chargeback Reasons

- This Section outlines the most common types of Chargebacks. This list is not exhaustive. For ease of understanding, we have combined like Chargebacks into six groupings. We have included recommendations on how to reduce the risk of Chargebacks within each group. These are recommendations only, and do not guarantee that you will be able to prevent Chargebacks.

Authorization Issues: Proper Authorization procedures were not followed and valid Authorization was not obtained.

- The following scenarios could cause an Authorization-related Chargeback to occur:
 - (i) Authorization not obtained;
 - (ii) Authorization was declined;
 - (iii) Transaction processed with an expired card and Authorization was not obtained;
 - (iv) Transaction was processed with an invalid account number and Authorization was not obtained;

(v) Card Recovery Bulletin (i.e. CRB) or Exception File was not checked (transactions below floor limit).

- To reduce your risk of receiving an Authorization Related Chargeback:
 - (i) Pre-notify the Cardholder of billings within ten (10) days;
 - (ii) American Express customers have the option to receive written notification of the recurring transaction at least (10) days prior to submitting, or any time the charge amount exceeds a maximum amount that has been set by the Cardholder;
 - (iii) Obtain valid Authorization on the day of the transaction;
 - (iv) *Card-present* Transactions: Authorization must be obtained on the transaction date for the amount settled;
 - (v) *Card-not-present* Transactions: Authorization must be obtained on the transaction date for the amount settled. However, if merchandise is being shipped, Authorization must be obtained within seven (7) calendar days of the transaction ship date;
 - (vi) If a referral or declined response is received, then request another form of payment from the Cardholder;
 - (vii) "Pick-up" response indicates that the Issuer is requesting that the Card be retained and returned back to them. The Card should not be accepted for payment. Additionally, you can choose to retain the Credit Card and send it to us so that we can arrange for its return to the Issuer;
 - (viii) Merchants should not exceed any predetermined thresholds for specific terminal types as specified by each Card Network.

Cancellations and Returns: Credit was not processed properly or the Cardholder has cancelled and/or returned items.

- The following scenarios could cause a cancellation and return-related Chargeback to occur:
 - (i) Cardholder received damaged or defective merchandise;
 - (ii) Cardholder continued to be billed for cancelled recurring transaction;
 - (iii) Credit transaction was not processed.
- To reduce your risk of receiving a cancellation and return-related Chargeback:
 - (i) Issue Credits to the Cardholder on the same account as the purchase in a timely manner;
 - (ii) Do not issue Credits to the Cardholder in the form of cash, check or in store/merchandise credit as we may not be able to recoup your funds in the event the transaction is charged back;
 - (iii) Ensure customers are fully aware of the conditions for recurring transactions. Cancel recurring billings as soon as notification is received from the Cardholder or as a Chargeback, and issue the appropriate Credit as needed to the Cardholder in a timely manner;
 - (iv) Pre-notify the Cardholder of billings within ten (10) days (domestic) and fifteen (15) (international) prior to billing, allowing the Cardholder time to cancel the transaction;
 - (v) Provide proper disclosure of your refund policy for returned/cancelled merchandise, or services to the Cardholder at the time of transaction in accordance with Applicable Law;
 - (vi) For *card-present* Transactions, ensure that the Cardholder signs the relevant transaction receipt(s) containing such disclosure(s);
 - (vii) If applicable, the words "NO EXCHANGE, NO REFUND," etc. must be clearly printed in 1/4" lettering on the relevant transaction receipt near or above the Cardholder signature;
 - (viii) For eCommerce transactions, provide the relevant disclosure on your website on the same page as the "check out", requiring the Cardholder to click to accept it prior to completion of the transaction;
 - (ix) For *card-not-present* Transactions, provide your cancellation policy at the time of the transaction;
 - (x) Provide cancellation numbers to Cardholder's when lodging services are cancelled;
 - (xi) Ensure delivery of the merchandise or services ordered to the Cardholder.

Fraud: Transactions that the Cardholder claims are unauthorized; the account number is no longer in use or is fictitious, or the Merchant was identified as "high risk." "High risk" Merchants include, for example, establishments whose business type has had historically high occurrences of fraud and disputed charges with American Express or as compared to other similarly situated merchants (or both); examples include internet electronic services or nightclubs/lounges). "High risk" Merchants may also be designated by the relevant Card Networks from time to time.

- The following scenarios could cause a Fraud-related Chargeback to occur:

- (i) Multiple transactions were completed with a single Card without the Cardholder's permission;
- (ii) Counterfeit Card was utilized and proper acceptance procedures were not followed;
- (iii) Authorization was obtained; however, full track data was not transmitted;
- (iv) Cardholder states that they did not authorize or participate in the transaction.

Mastercard has already implemented a contactless Chip and PIN liability shift for lost, stolen and Never Received Issue (“NRI”) fraud since April 21, 2017 (effective October 1, 2020 for AFDs for U.S.-issued cards). If the contactless Card or access device is PIN-preferring but the terminal does not support online PIN validation and lost, stolen or NRI fraud occurs at the point of sale, you will be liable for the Fraud, provided that the transaction was above the applicable CVM limit.

- To reduce your risk of receiving a Fraud-related Chargeback:

(i) *Card-present* Transactions:

- Pre-notify the Cardholder of billings within ten (10) days.
- American Express customers have the option to receive written notification of the recurring transaction at least (10) days prior to submitting, or any time the charge amount exceeds a maximum amount that has been set by the Cardholder.
- Obtain an Authorization for all transactions.
- If you are utilizing an electronic device to capture Card data information, swipe, dip or wave all Card Transactions through your electronic Authorization device to capture Cardholder information. When applicable, ensure the displayed Cardholder number matches the number on the Card.
- You should avoid keying the Card data into your electronic authorization device unless you are unable to capture the Card data through one of the above methods. If you do not key the Card data into your electronic authorization device, it is highly recommended that you also key in the 3 or 4 digit CVC.
- Use POS terminals (or other Card acceptance equipment) that can accept Chip Cards based on their Chips, not their Magnetic Stripes.
- Obtain the Cardholder signature for all transactions; ensure the signature on the signed transaction receipt matches the signature on the back of the Card.
- Process all transactions one time and do not batch out transactions multiple times.
- Educate staff on procedures to eliminate point of sale Fraud.

(ii) *Card-not-present* transactions:

- Participation in recommended fraud mitigation tools:
 - (a) Verified by Visa Program.
 - (b) Mastercard SecureCode.
 - (c) Discover Protect Program.
 - (d) American Express SafeKey Program.
 - (e) Address Verification Services.
 - (f) Use Card Verification Code.

NOTE: While transactions utilizing these tools may still be disputed, the service may assist you with your decision to accept the Card for the transaction.

- Ensure you ship to the AVS-confirmed address (bill to and ship to should match).
 - Obtain Authorization for all transactions.
 - Ensure merchant descriptor matches the name of the business and is displayed correctly on the Cardholder statement.
 - Ensure descriptor includes correct business address and a valid customer service number.
- American Express offers fraud mitigation tools for both *card-present* Transactions and *card-not-present* Transactions to help verify that a charge is valid. These tools help you mitigate the risk of Fraud at the point of sale, but are not a guarantee that a

charge is in fact valid or bona fide, or that you will not be subject to a Chargeback. For optimal use of the tools, please visit American Express' Fraud Prevention Information at: www.americanexpress.com/fraudinfo

Cardholder Disputes: Merchandise or services not received by the Cardholder, merchandise defective or not as described.

- The following scenarios could cause a Cardholder dispute Chargeback to occur:
 - (i) Services were not provided or merchandise was not received by the Cardholder;
 - (ii) The Cardholder was charged prior to merchandise being shipped or merchandise was not received by agreed upon delivery date or location;
 - (iii) Cardholder received merchandise that was defective, damaged or unsuited for the purpose sold, or did not match the description on the transaction documentation/verbal description presented at the time of purchase;
 - (iv) Cardholder paid with an alternate means and their Card was also billed for the same transaction;
 - (v) Cardholder cancelled service or merchandise and their Card was billed;
 - (vi) Cardholder billed for a transaction that was not part of the original transaction document;
 - (vii) The Cardholder claims to have been sold counterfeit goods;
 - (viii) The Cardholder claims the terms of sale were misrepresented by the merchant.

- To reduce your risk of receiving a Cardholder dispute-related Chargeback:
 - (i) Provide services or merchandise as agreed upon and described to the Cardholder; clearly indicate the expected delivery date on the sales receipt or invoice;
 - (ii) Contact the Cardholder in writing if the merchandise or service cannot be provided or is delayed, and offer the Cardholder the option to cancel if your internal policies allow;
 - (iii) In the event that the Cardholder received defective merchandise or the merchandise received was not as described, resolve the issue with the Cardholder at first contact;
 - (iv) If the merchandise is being picked up by the Cardholder, have them sign for the merchandise after inspection that it was received in good condition;
 - (v) Do not charge the Cardholder until the merchandise has been shipped, ship according to the agreed upon terms and obtain signed proof of delivery from the Cardholder;
 - (vi) If unable to provide services or merchandise, issue a Credit to Cardholder in a timely manner;
 - (vii) Accept only one form of payment per transaction and ensure the Cardholder is only billed once per transaction;
 - (viii) Do not bill Cardholder for loss, theft or damages unless authorized by the Cardholder;
 - (ix) Ensure that the service or merchandise provided is clearly described.

Processing Errors: Error was made when transaction was processed or it was billed incorrectly.

- The following scenarios could cause a processing error Chargeback to occur:
 - (i) Transaction was not deposited within the Card Network specified timeframe;
 - (ii) Transaction was to be processed in a currency other than the currency used to settle the transaction;
 - (iii) The account number or transaction amount utilized in the transaction was incorrectly entered;
 - (iv) A single transaction was processed more than once to the Cardholder's account;
 - (v) Cardholder initially presented Card as payment for the transaction; however Cardholder decided to use an alternate form of payment;
 - (vi) Limited amount or self-service terminal transaction was processed for an amount which is over the pre-determined limit.

- To reduce your risk of receiving a processing error-related Chargeback:
 - (i) Process all transactions within the Card Network specified timeframes;
 - (ii) Ensure all transactions are processed accurately and only one time;

NOTE: In the event that a transaction was processed more than once; immediately issue or contact us to issue voids, transaction reversals or Credits.

- (iii) Ensure that credit transaction receipts are processed as Credits and sale transaction receipts are processed as sales;
- (iv) Ensure all transactions received a valid Authorization approval code prior to processing the transaction and obtain a legible transaction receipt that is signed where the Magnetic Stripe of a Card is swiped;
- (v) Do not alter transaction records or make any adjustments unless the Cardholder has been contacted and agrees to any modifications of the transaction amount;
- (vi) Ensure limited amount, self-service and automated fuel dispenser terminals are set properly to conform to the pre-determined limits.

Chargebacks due to non-receipt of information description: Failure to respond to a retrieval request or the Cardholder does not recognize the transactions.

- The following scenarios could cause such Chargebacks to occur:
 - (i) The transaction records required were not provided to fulfill the retrieval request;
 - (ii) The retrieval request was fulfilled with illegible transaction records or was an invalid fulfillment (incorrect transaction records or the transaction records did not contain required information that may include a signature);
 - (iii) The Cardholder does not recognize or is unfamiliar with the transaction due to the merchant name and/or Location not matching the name and/or location where the transaction took place.

- To reduce your risk of receiving such Chargebacks:
 - (i) Provide a clear and legible copy of the relevant transaction records that contains all required data elements within the required timeframe that is specified on the retrieval request;
 - (ii) Ensure that the most recognizable merchant name, Location and/or Customer Service phone number is provided on all transactions;
 - (iii) Retain copies of all transaction records for the required timeframe that is specified by each Card Network;
 - (iv) Develop efficient methods to retrieve transaction records to maximize ability to fulfill request.

8.4 Summary (Deposit) Adjustments / Electronic Rejects

- Occasionally, it is necessary to adjust the dollar amount of your summaries/submissions (deposits) and credit or debit your Settlement Account or Settlement Funds accordingly. The following is a list of the most frequent reasons for summary (deposit) adjustments/electronic rejects:
 - (i) Your summary reflected an arithmetic error;
 - (ii) Submitted sales not included in your Agreement (e.g. American Express);
 - (iii) The dollar amount is unreadable/ illegible;
 - (iv) The Cardholder's account number is unreadable /illegible;
 - (v) Card number is incorrect/ incomplete;
 - (vi) Summary indicated Credits, but no Credits were submitted.

8.5 Disputing Other Debits and Summary Adjustments

- In order to quickly resolve disputed debits and summary adjustments, it is extremely important that the items listed in this Section be sent to the address listed on the notification.

- If the transaction is over thirty (30) calendar days old, you must reauthorize and obtain a valid Authorization approval code.

- A clear and legible copy of the relevant transaction receipt containing the following should be obtained from your files:

- (i) Date of sale/Credit;
 - (ii) Cardholder's account number, name and signature;
 - (iii) Total amount of the sale and description of goods and services; and
 - (iv) Date and Authorization approval code.
- Include a dated cover letter detailing the reasons for requesting a review of the debit or summary adjustment and transaction records to support your dispute. (You should retain a copy of the correspondence and all transaction records for your files.) If the inquiry is related to prior correspondence, be sure to include the control number we previously used. Immediately send the relevant transaction records to the contact details indicated on the notification letter.
 - If you have any questions, please call Customer Service. If a representative informs you that additional transaction records are required in order to fully review the item, please immediately submit your rebuttal and the relevant transaction records to the address listed on the debit notification.

8.6 Record Retention Requirements

- **For Visa, Mastercard:** You must securely retain legible copies of all transaction records or be able to reproduce them for a period of thirteen (13) months from the date of each transaction and a period of five (5) years for the retention of transaction records related to healthcare.
- **For Discover:** You must securely retain legible copies of all transaction records for the longer of: (i) 365 days; or (ii) the resolution of any pending or threatened disputes, claims, disagreements or litigation involving the Card Transaction. You must also keep images or other copies of transaction records for no less than three (3) years from the date of the Discover Card Transaction.
- **For American Express:** You must submit Credit transactions to your processor for payment. You must securely retain legible copies of all transaction records for twenty-four (24) months from the date you submitted the corresponding Credit.

9. Settlement Procedures

9.1 Overview

- This Section describes the procedure and timeframes within which we settle payments due to you for Card Transactions you submit to us. Please be advised that the timeframes indicated below are subject to change, and we may (but are not required to) notify you of any such changes prior to implementation.

9.2 Submission Timeframes

- All Card Transactions must be properly completed and submitted daily. If you have not received payment for submitted Card Transactions after one (1) week from your normal payment date, contact Customer Service. Late submission of Card Transactions may result in additional Fees and/or in a Chargeback to you.
- You must confirm that your equipment has transmitted your Card Transactions to us at least once daily.** Even if your equipment is designed or programmed to close and submit Card Transactions without your intervention, it is ultimately your responsibility to confirm that your Card Transactions have been transmitted to us for processing.

9.3 “Special Process” Transactions

- Special processing involves submitting Card Transactions for processing later than the recommended timeframe for submission. Special processing presents a very high risk of Chargebacks and higher interchange and Fees. **You are wholly responsible for Chargebacks and related Fees. By requesting special processing, you understand and accept the risks and agree to bear the financial responsibility for all Chargebacks and Fees.**

9.4 Settlement Timeframes

- We will settle with you for each Card Transaction acquired and accepted by us under your Agreement. You may be eligible for either Same Day or Standard Day Funding. The following grid identifies the cutoff times and when funding will show up in your account as designated by you as the account to be credited and debited in relation to Card Transactions, Fees, Chargebacks and other amounts in connection with your Agreement:

Funding Frequency	Funding cut-off time	Funding Post Time	Day Received/Day Funded
Same-Day Funding (funding is memo-posted into Merchant account)	1:30 AM EST	4:00 AM EST	Monday / Monday
	5:30 AM EST	8:00 AM EST	Tuesday / Tuesday
	9:30 AM EST	12:00 PM EST	Wednesday / Wednesday
	1:30 PM EST	4:00 PM EST	Thursday / Thursday
	5:30 PM EST	8:00 PM EST	Friday / Friday
	8:30 PM EST	11:00 PM EST	Saturday / Saturday Sunday / Sunday

Funding Frequency	Funding cut-off time	Funding Post Time	Day Received/Day Funded
Standard Day Funding (funding is hard-posted into Merchant account)	8:30 PM EST	11:00 AM EST (next day)	Monday / Tuesday
			Tuesday / Wednesday
			Wednesday / Thursday
			Thursday / Friday
			Friday / Monday
			Saturday / Monday Sunday / Monday

10. Statements

10.1 Overview

- Your Statements will be available for you to access on your Merchant Portal, (accessed at bankofamerica.com/smallbusiness) on a monthly basis using the log-in details you registered with in your application to us. We will not deliver paper-based Statements to you. Please review your Statements carefully.

10.2 Issues on Your Statement

- If you notice any issues or discrepancies on your Statement, please notify us in writing, detailing such errors within sixty (60) days of such Statement being available to you for access. We will effect adjustments remedying any errors on Statements, in our discretion.
- Please be advised that if you do not provide us with such written notice in this timeframe, we will not have any obligation or liability to investigate or correct such error, or to effect any related adjustment, absent any willful misconduct by us.

11. Other Information

11.1 IRS Reporting and Back-Up Withholding

- On an annual basis, we are required to send you a “Form 1099” showing total payment processing volume and report the same amounts to the IRS. This is required for all merchants above a certain dollar threshold in processing volume.
- In the event you or your business becomes subject to back-up withholding please notify us immediately in order for us to comply with the IRS requirements.

11.2 Lost / Recovered Cards

- If a Card is left behind and remains unclaimed, you should call the appropriate Card Network’s customer service team via the number below and they will instruct you on how to handle it:
 - (i) **Visa:** 1-800-336-8472
 - (ii) **Mastercard:** 1-800-826-2181
 - (iii) **Discover:** 1-800-DISCOVER (1-800-347-2683)
 - (iv) **American Express:** 1-800-992-3404

12. Definitions

As used in this Operating Guide, the following terms have the following meanings:

Address Verification Service (AVS): A service for verifying a Cardholder's address, primarily for *card-not-present* Transactions.

American Express: American Express Travel Related Services Company, Inc.

American Express OptBlue® Program Service: OptBlue allows Bank of America to set pricing, process transactions, fund, statement and support American Express transactions for a merchant. Merchants must process less than USD 1 million dollars in American Express volume annually and not be part of a franchise that has a direct relationship with American Express.

Authorization: Approval by, or on behalf of, the Issuer to validate a Card Transaction; or in the case of EBT Card Transactions, the issuing state or related EBT service provider to validate an EBT Card Transaction. Authorization, including an Authorization approval code, indicates only the availability of credit, funds, or EBT Benefits at the time the Authorization is requested; it does not indicate that the person presenting the Card is the rightful Cardholder and it does not promise, indicate, or suggest that you will not be subject to a Chargeback, an adjustment, or other Fees and Third Party Based Fees.

card-not-present Transaction: A transaction that occurs when the Card is not present at the point-of-sale, including internet, mail-order, and telephone-order Card Transactions.

card-present Transaction: A transaction that occurs when the Card is present at the point-of-sale.

Card Verification Codes: A three-digit value printed in the signature panel of most Cards and a four-digit value printed on the front of an American Express Card. Visa's Card Verification Code is known as CVV2; Mastercard's Card Verification Code is known as CVC2; and Discover's Card Verification Code is known as a CID (and can also be referred to as a security code).

Chip: An integrated microchip embedded on a Card containing Cardholder account information.

Credit: A refund or price adjustment given for a previous purchase transaction, including for the return of merchandise by a Cardholder.

Discover: DFS Services LLC, its subsidiaries and affiliates, and each of its and their respective successors or assigns.

Documentation: The operational documents, technical integration requirements and documentation, user manuals, help files, and other implementation overviews, integration guidelines, sandbox guidelines, and other documentation that we provide or make available, in written or electronic form, in connection with any Software or service, as modified by us from time to time.

Electronic Benefit Transfer (EBT): An electronic benefits transfer system used to deliver certain government provided benefits (such benefits, "EBT Benefits") to customers, including cash benefits and benefits offered by the United States Department of Agriculture, Food and Nutrition Service; the Supplemental Nutrition Assistance Program; and the Special Supplemental Nutrition Program for Women, Infants, and Children.

EMV: The global standard for Chip Card based payments developed by Europay, Mastercard, and Visa.

Magnetic Stripe: A stripe of magnetic information affixed to the back of a plastic Credit Card or Debit Card. The Magnetic Stripe contains essential Cardholder and account information.

Mastercard: Mastercard International Incorporated, its subsidiaries and affiliates, and each of its and their respective successors or assigns.

Merchant Account: An account we establish for each of your Locations for accounting and billing purposes in connection with the Merchant Services.

Merchant Account Number (MID): A number that numerically identifies each Merchant Account.

OptBlue: American Express program that allows the merchant acquirer (Bank of America, N.A.) to set pricing, process transactions, settle payment and provide support for American Express transactions

Representment: a transaction to reverse a Chargeback by the re-submission of the original transaction after you have successfully challenged a Chargeback.

Retro-Charge: a transaction to reverse a Refund that the Cardholder was not entitled to.

Third Party (Third Parties): Any third party individual(s) or entity(ies) other than you or us.

Third Party Based Fees: Fees, fines, assessments, penalties, obligations, liabilities, adjustments, and other charges and amounts a Card Network, Issuer, or other Third Party imposes, establishes, or sets, and all related costs and expenses. The term "Third Party Based Fees" includes all Data Compromise Losses and all Chargebacks.

Visa: Visa Inc. its subsidiaries and affiliates, and each of its and their respective successors or assigns.