Operating Guide

February 2016

Table of Contents

Chapter

1

About Your Card Program

Thank you for your choosing us as your Servicer. This Operating Guide contains instructions for processing card transactions with us and minimizing the risk of fraud to your business.

This guide is a part of the Agreement with us. Please familiarize yourself with this guide as you are the first line of defense against fraud. Failure to comply with these guidelines and suggestions may be considered a breach of the Agreement and may result in financial loss to your business. In the event that compliance with this Operating Guide would cause you to violate applicable Payment Network Regulations and/or Laws, you should comply with such applicable Payment Network Regulations and/or Laws.

Throughout this guide terms that have specific meaning to the Card industry are noted with initially capitalized letters (e.g., Credit Card, Card Present Transactions). If you are not familiar with these terms, refer to Appendix A, *Glossary* for definitions.

TYPES OF CARDS

Types of Cards include:

- **Credit Card:** A Credit Card is issued by a financial institution or other Credit Card company (called the Issuer) that extends a line of credit to the Cardholder. A Credit Card allows the Cardholder to borrow money against the credit line and to repay the funds with interest if the Balance is carried over from month to month. Visa and MasterCard Credit Cards (often referred to as "Bank Cards") are issued by banks, while American Express, Discover Network, and other Credit Cards may be issued by the Card company itself or in some instances by other financial institutions. There are many Issuers that offer Discover Network, Visa and MasterCard Credit Cards, making it possible for a Cardholder to have several different Credit Cards, each of which represents its own line of credit.

- **Debit Card:** A Debit Card is issued by a financial institution. Purchases made with Debit Cards result in the immediate withdrawal of funds from the Cardholder's bank account. Debit Cards do not represent a line of credit; they can only be used to the extent the Cardholder has available funds in the account associated with the Debit Card. Discover Network, Visa and MasterCard offer Debit Cards in addition to Credit Cards. Debit Cards that are processed on Credit Card Association networks are typically signature-based Debit Cards, while Debit Cards that are processed on EFT Networks are generally Personal Identification Number (PIN)-based Debit Cards.

- **Automated Teller Machine (ATM) Card:** An ATM Card is a plastic card issued by a financial institution that allows a Cardholder to withdraw funds, make deposits, make purchases, or perform other banking functions against the Cardholder's bank account through an ATM or POS Device.

- **Electronic Gift Cards (EGC):** EGCs are issued by Companies at a set dollar amount for future purchases. When a Cardholder uses an EGC to make a purchase, the Transaction total is deducted from the value remaining on the Card until the pre-paid amount is spent.
- **Electronic Benefits Transfer (EBT) Cards:** EBT Cards are Cards used by a Cardholder to purchase qualifying goods or services from a Company using government-funded benefits loaded onto the Card. EBT Cards are used like Debit or ATM Cards (requiring a PIN). When an EBT Card is used to make a purchase, the Transaction total is deducted from the value remaining in the Cardholder's account until the pre-paid amount is spent.

ABOUT TRANSACTION PROCESSING

To accept Credit Cards, Debit Cards or other Cards for payment, you process the Transactions through a POS Device and/or with point-of-sale software. A group of Transactions is called a Batch, and the process of sending these Transactions to us is called Settlement.

When you settle a Batch, information for each Transaction is sent to clearing networks across the country and sometimes around the world. Based on each Card number, we send information about a Transaction to the corresponding Issuer so they can charge the Cardholder. Then, funds for the Transaction are deposited into your Demand Deposit Account (DDA). Refer to Chapter 2, *Processing Transactions*, for specific details about processing Transactions.

In exchange for these services, you are charged a percentage of each Transaction (known as a Discount), along with Transaction fees, Authorization fees, and any other fees specified in the Agreement. Fees are deducted from your DDA on either a monthly or a daily basis.

When a Cardholder does not agree with a Transaction posted to his or her account, the Cardholder can contact the Issuer and initiate a dispute. In this case, the Transaction amount is debited from your DDA and we send you a Chargeback notice. In order to protect your rights, it is important that you respond promptly to any Chargeback notice you receive. Refer to Chapter 6, *Retrieval Requests & Chargebacks*, for a detailed explanation of this process.

GENERAL OPERATING GUIDELINES

When you process Transactions, it is important to keep the following general guidelines in mind:

- **Do Not Set Restrictions on Card Transactions:** Discover Network, Visa and MasterCard prohibit setting a minimum or maximum purchase amount except that you are permitted to set a minimum purchase amount of up to $10 for Credit Card Transactions and, if you are a government agency or institution of higher education, you may set a maximum purchase amount for Credit Card Transactions. Discover Network, Visa and MasterCard permit adding a surcharge to a Credit Card Transaction amount, subject to specific conditions and requirements. You may give a discount from your standard pricing or offer an in-kind incentive for payment by cash, Credit Card, Debit Card or any other method of payment. Card customers are frequently among your best customers due to their available lines of credit, purchasing freedom, and their tendency to spend more than cash customers.

- **Do Not Discriminate:** You must honor all valid Cards within your acceptance categories when properly presented for payment, without discrimination, unless Laws expressly require otherwise. You must maintain a policy that does not discriminate, unless Laws expressly require otherwise, among Cardholders seeking to make purchases with a particular brand of Card accepted by you.

- **Keep Passwords Secure:** Keep all passwords that allow you to access our databases or services secure. Remember, you are responsible for the actions of anyone who uses your password. If you believe your password has been compromised or shared with an unauthorized user, please contact us immediately.

- **Protect Cardholder Privacy:** You may only require a Cardholder's personal information if it is necessary to complete a Transaction (such as a delivery address and/or telephone number for Card Not Present

Transactions) or if the Voice Authorization Center specifically requests it. You may not refuse to complete an otherwise valid Card Transaction just because a Cardholder refuses to provide additional identification or information. Discover Network, Visa and MasterCard regulations prohibit listing a Cardholder's personal information on the Transaction Receipt because it can expose a Cardholder to increased risk of fraud. You must not use any Servicer's systems, including, but not limited to, custom fields or any other unprotected fields within Service's systems, to collect, transmit, or store any sensitive or confidential data, including, but not limited to, personal unique identifiers, including, but not limited to, Primary Account Numbers (PAN), Card expiration dates, track data, Card Identification Numbers, Card Validation Codes, Social Security numbers, Personal Identification Numbers, individually identifiable health information, or other private data of customers or cardholders. You must not, and must not cause Servicer to, violate applicable requirements of the Payment Card Industry (PCI) Data Security Standard, including Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection Program (SDP) and the Discover Information Security & Compliance (DISC) program.

- **Plan Ahead for Fees and Chargebacks:** Maintain sufficient funds in your DDA to cover all fees, Chargebacks, or any other adjustments that may occur. Monthly fees are debited from your DDA near the beginning of each month for the prior month's activity. We recommend that you keep five percent (5%) of your average monthly processing volume available in your account to cover monthly fees and the possibility of Chargebacks. Keep in mind that this is only a recommendation and your business may require additional available funds. For example, businesses that conduct high-risk Transactions (such as Card Not Present or those with future delivery of products or services) should consider maintaining a higher percentage of their average monthly processing volume in their account.

- **Keep Cardholder Data Secure:** Keep all Transaction Receipts in a locked area that is accessible only to select personnel. When you dispose of Transaction Receipts after the designated retention period, make sure that account numbers and Imprints are rendered unreadable, as criminals can commit fraud with even a few pieces of Cardholder data. Your customers will not only appreciate your concern and consideration, but will also gain confidence in your service and integrity.

- **Perform Regular Audits:** In addition to balancing daily receipts, compare Transaction Receipts to the register tape to ensure that they match. Periodic reviews help identify potential problems associated with a specific register or sales associate. Remember, it is your responsibility to address inconsistencies and educate your staff.

- **Know Your Third Party Vendors:** If you use software or other services (such as an online "shopping cart") provided by a third party or value-added reseller (VAR), you may be impacted by and financially liable for security breaches or system failures by the third party vendor. Be sure to acquaint yourself with the third party vendors' requirements and limitations so you can minimize disruption in service and protect yourself from unauthorized access. It is your responsibility to ensure that all Cardholder information (including that accessed or maintained by your third party vendor) is stored in an encrypted and secure environment. You are responsible for ensuring that any third party vendors that you engage are registered with the Payment Networks prior to the performance of any contracted services on your behalf. Additionally, you are responsible for notifying Servicer of any third party vendors registered or VARs used by you.

- **Security Program Compliance:** You, and any third party vendors that you utilize, must comply with all applicable requirements of the Payment Card Industry (PCI) Data Security Standard, including Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection Program (SDP) and the Discover Information Security & Compliance (DISC) program. You must remain in compliance with these standards as they change.

- **Data Compromise:** Notify us immediately, and in any event within twenty-four (24) hours, if you know or suspect that Cardholder information has been accessed or used without authorization, even if this compromise involves a third party vendor. You must take immediate steps to preserve all business records, logs and electronic evidence and contact local law enforcement authorities (including the local FBI and U.S. Secret Service). You must work with us to rectify any issues that result, including providing us (and

obtaining any waivers necessary to provide us with) all relevant information to verify your ability to prevent future data incidents in a manner consistent with the Agreement.

- **Interchange:** Interchange qualification requirements, as defined by the Credit Card Associations, affect the Company's fees or surcharges owed for Transactions. Company will pay a higher discount rate, higher fees, and surcharges for Transactions that do not meet the best rate qualification criteria or have been processed in a manner other than for which the Company was approved.
- **Display of Card Marks.** Unless otherwise informed by Servicer, you must prominently display the most current versions of the Credit Card Association's and EFT Network's names, symbols, and/or service marks, as appropriate, at or near the POS Device as may be required or requested by the Payment Networks. For Companies that accept Cards for Electronic Commerce Transactions, you must display such names, symbols and/or service marks on Internet payment screens. You may also display such marks on promotional materials to inform the public that such Credit Cards and Debit Cards will be honored at your place(s) of business. Company's use of such marks must comply with the requirements of each mark's owner. Company's right to use or display such marks will continue only so long as the Agreement remains in effect and such right will automatically terminate upon termination of the Agreement. Company must remove the marks immediately upon termination.
- **Prohibited Transactions.** A Company must not: (a) submit for payment into interchange any Transaction that (i) arises from the dishonor of a Cardholder's personal check, (ii) arises from the acceptance of a Card at a POS Device that dispenses scrip, (iii) is illegal, or (iv) is otherwise prohibited herein or in the Payment Network Regulations; (b) accept Cardholder payments for previous Card charges incurred at the Company location; (c) accept a Card to collect or refinance an existing debt that has been deemed uncollectible by the Company providing the associated goods or services; or (d) accept Cards at POS Devices that dispense scrip.
- **Marketing; Opt-out.** Elavon seeks to provide you with updated information regarding the products and services that we offer to you. In addition to our traditional methods of communication, we may also reach out to you via mobile text messaging and email messages. By providing your mobile phone number and/or e-mail address in your Company Application, you authorize Servicer to use that information to contact you about your account and to market additional products/services to you. You are not required to provide your mobile phone number and/or e-mail address in connection with your Company Application, and, if you do, you may elect not to receive such communications from Servicer in the future by contacting Servicer at optout@elavon.com.

ADDITIONAL SERVICES

In addition to the traditional Card processing services offered, we also provide the following services:

- **Acceptance of American Express, Discover Network, Diners, JCB, and/or UnionPay Cards:** If Servicer provides authorization and/or data capture services to Company for American Express, Discover Network, Diners, JCB, and/or UnionPay Transactions, Company agrees to the following provisions, in addition to the other provisions set forth in the Operating Guide. If Card Processing Fees are indicated for Discover Network on your Company Application or Schedule A (Schedule of Fees) to the Agreement, as applicable, then Servicer provides full authorization, processing and settlement services for Discover Network Transactions and the Company's Discover Network Transactions must comply with the provisions of the Operating Guide; otherwise, Servicer provides only authorization and/or data capture services for Discover Network Transactions.
- **Address Verification Service (AVS):** Allows a Company to help prevent fraud by verifying a Cardholder's billing address prior to completing a Card Not Present Transaction.
- **MerchantConnect:** Allows a Company to manage Transaction data from multiple locations or multiple company accounts via any standard web browser (e.g., Internet Explorer) using a web-based Transaction reporting and reconciliation system.

- **Automated Customer Service (ACS):** Allows a Company to view detailed reports of Transaction activity, statement detail, Card type history, and qualification detail using a desktop reporting and accounting reconciliation application.
- **Dynamic Currency Conversion (DCC):** Allows a Company to offer international Cardholders in the United States the option at the point-of-sale to pay in their home currency rather than in U.S. Dollars.
- **Electronic Check Services (ECS):** Allows a Company to convert paper checks and other payment information into electronic Transactions, eliminating the need to manually deposit checks at a bank. ECS provides you and your Customers with efficient, easy, and secure bank account payment processing. Refer to the separate *Electronic Check Service Merchant Operating Guide (ECS MOG)* for additional information on electronic processing of checks using ECS.
- **Electronic Gift Card (EGC) Services:** Allows a Company to sell Electronic Gift Cards redeemable for in-store merchandise or services. EGCs provide Customers with another form of payment while encouraging repeat shopping.
- **Electronic Benefits Transfer (EBT) Service:** Allows electronic transfer of government funds to individuals through the use of a plastic debit-like Card and a PIN. The federal government requires all states to distribute food stamps and cash benefits in this manner.
- **Hospitality Services:** Allows a Company operating in the hotel and hospitality industry to process Transactions for lodging accommodations.
- **Petroleum Services:** Allows a Company to process petroleum-related Transactions including Satellite Services, SmartLink Services, Voyager Card Acceptance and Wright Express Card Acceptance.
- **Fanfare Loyalty and Gift Card Services:** Allows a Company to establish and operate a Customer loyalty program and/or a gift card program, including a Customer-facing website, through which the Company can create and manage marketing campaigns and promotional offerings to Customers.
- **Services in Canada:** Allows Companies operating in Canada to process Transactions subject to the requirements set forth herein and in the Agreement.

Please contact us if you are interested in any of these services.

Chapter

2

Processing Transactions

This Chapter explains the two steps involved in the Transaction process—Authorization and Settlement— as well as the different types of Transactions.

COMPANY COMPLIANCE

1. **Settlement of Transactions**. Subject to the other provisions of the Agreement and subject to Company's compliance with the terms of the Agreement and the Payment Network Regulations, Servicer will process Transactions daily, and if Company maintains its DDA with Member, provisional credit for Transactions (less recoupment of any Chargebacks, returns, adjustments, fees, fines, penalties, assessments from the Payment Networks and other amounts due to Servicer under the Agreement) may be available as soon as the next banking day after the banking day on which Servicer a process the Transactions. Regardless of where Company maintains its DDA, Company acknowledges and agrees that Servicer may use either "direct" (ACH debit authority pursuant to which Chargebacks, returns, adjustments, fees, fines, penalties, assessments and charges from the Payment Networks and other amounts due to Servicer under the Agreement are debited from the DDA) or "net" (pursuant to which Chargebacks, returns, adjustments, fees, fines, penalties, assessments and charges from the Payment Networks and other amounts due to Servicer under the Agreement are netted from Transaction proceeds) methods to recover any amounts owed by Company to Servicer under the Agreement. To the extent required, Company authorizes and appoints Servicer to act as Company's agent to collect Transaction amounts from the Customer, the Issuer or the Customer's financial institution.

2. **Deposits**. Company acknowledges that its obligation to Servicer for all amounts owed under the Agreement arises out of the same transaction as Servicer's obligation to deposit funds to the DDA and such amounts are owed in the ordinary course of business.

3. **Provisional Credit**. Company acknowledges that all credits for funds provided to it are provisional and subject to reversal in the event that Servicer does not receive payment of corresponding settlement amounts from the Payment Networks. Company further acknowledges that all credits are subject to adjustments for inaccuracies and errors (including rejects) and Chargebacks in accordance with the Agreement and the Payment Network Regulations, whether or not a Transaction is charged back by the Issuer or Customer. Company authorizes Servicer to initiate reversal or adjustment (debit or credit) entries and to initiate or suspend such entries in accordance with the Agreement as may be necessary to grant or reverse provisional

credit for any Transaction. Further, Servicer may delay Company-issued Cardholder credits for up to five (5) business days for accounting verification. Cardholder credits issued by Company to PIN-Debit Cards will not be subject to this delay.

4. **Chargebacks**. Company agrees to accept for Chargeback, and will be liable to Servicer in the amount of any Transaction disputed by the Cardholder or Issuer for any reason under the Payment Network Regulations. Company authorizes Servicer to offset from funds due Company or to debit the DDA or the Reserve Account for the amount of all Chargebacks. Company will fully cooperate with Servicer in complying with the Payment Network Regulations regarding all Chargebacks.

5. **Original Transaction Receipts**. Under no circumstances will Servicer be responsible for processing returns, refunds, or adjustments related to Transactions not originally processed by Servicer.

6. **Demand Deposit Account**. Company will maintain sufficient funds in the DDA to accommodate all Transactions contemplated by the Agreement and all Chargebacks, returns, adjustments, fees, fines, penalties, assessments from the Payment Networks and other payments due under the Agreement. Servicer has the right to delay, within its reasonable discretion, crediting the DDA with funds related to Transactions in order to investigate any Transactions related to suspicious or fraudulent activity or funds for Transactions for which Servicer has not received funding from the applicable Payment Networks. Servicer will endeavor to investigate or process any delayed Transactions expeditiously and will endeavor to notify Company if any Transactions are delayed for more than 48 hours.

7. **Asserted Errors**. It is the responsibility of Company to reconcile the statements regarding Transaction activity received from Servicer, any Payment Network, and any third party vendors with the statements Company receives for Company's DDA.

    a. Company must promptly examine all statements relating to the DDA and promptly notify Servicer in writing of any errors in the statement Company received from Servicer. Company's written notice must include:

        i. Company name and account number;

        ii. The dollar amount of the asserted error;

        iii. A description of the asserted error; and

        iv. An explanation of why Company believes an error exists and the cause of it, if known.

    b. The written notice described above must be received by Servicer within forty-five (45) days of the date of the Servicer statement containing the asserted error. If Company fails to provide such notice to Servicer within said forty-five (45) days, Servicer will not be liable to Company for any errors Company asserts at a later date. Company may not make any claim against Servicer for any loss or expense relating to any asserted error for forty-five (45) days immediately following Servicer's receipt of Company's written notice. During that forty-five (45) day period, Servicer:

        i. Will be entitled to investigate the asserted error, and Company will not incur any cost or expense in connection with the asserted error without notifying Servicer, and

        ii. Notify Company of its proposed resolution of the asserted error.

8. **Fraud Monitoring.** Company is solely responsible for monitoring its Transactions. Servicer is under no duty to monitor Company's Transactions for fraudulent or other suspicious activity.

9. **Use of Trademarks**. Company will use and display the Payment Networks' marks as may be required or requested by the Payment Networks, and will display such marks in accordance with the standards for use established by the Payment Networks. Company's right to use all such marks will terminate upon termination of the Agreement or upon notice by a Payment Network to discontinue such use. Company's use of promotional materials provided by the Payment Networks will not indicate, directly or indirectly, that such Payment Networks endorse any goods or services other than their own and Company may not refer to any Payment Networks in stating eligibility for Company's products or services.

10. **Accuracy of Information**. Company must promptly notify Servicer in writing of any material changes to the information provided in the Company Application, in the bid process if applicable, or otherwise in the Agreement, including, without limitation, any additional location or new facility at which Company desires to use the Servicer Services, the form of entity (e.g., partnership, corporation, etc.), change in control, material changes to the type of goods and services provided and/or payments accepted, and how Transactions are completed (e.g., by telephone, mail, electronic commerce, or in person at Company's place of business). The notice must be received by Servicer at least ten (10) business days prior to the change. Company will promptly provide any additional information reasonably requested by Servicer. Servicer has the right to rely upon written instructions submitted by Company to request changes to Company's business information. Company may request written confirmation of Servicer's consent to the changes to the Company's business information.

11. **Transaction Receipts**. Company is solely responsible for all Transactions and Transaction Receipts until such time as the Transaction Receipts have been received and validated by Servicer. Company will maintain sufficient "backup" information and data (e.g., Transaction Receipts or detailed reporting) with respect to Transactions and will provide such information and data to Servicer upon request in order to reconstruct any information or data lost due to any malfunction of Company's or Servicer's systems. Servicer is under no duty to recreate lost Transactions or Transaction Receipts unless such loss results from Servicer's breach of the Agreement.

AUTHORIZATION

The first step in processing a Transaction is to request Authorization from the Issuer to accept a Card for payment. Company must obtain an Authorization Code before completing any Transaction. An Authorization request is made via one of the following two methods:

- **Electronic Authorization:** The Company swipes a Card through or manually enters a Card number into a POS Device. Then, the POS Device sends the Transaction information electronically to the Issuer for Authorization.
- **Voice Authorization:** The Company calls the Voice Authorization Center, which then communicates the Transaction information electronically to the Issuer. An operator or an interactive voice response (IVR) unit provides the Company with the Authorization Code given by the Issuer. Voice Authorization toll-free telephone numbers are located on a sticker on your POS Device. If there is not a Voice Authorization sticker on your POS Device, contact merchant services.

Most Authorizations are requested electronically. Voice Authorization is usually used if a Company does not have a working POS Device or if the Issuer requests additional information during Electronic Authorization.

An Authorization request is required for every Transaction to determine if:

- The Card number is valid;
- The Card has been reported lost or stolen; and/or
- Sufficient credit or funds are available.

Receipt of an Approval Code in response to an Authorization request does not:

- Guarantee that the Company will receive final payment for a Transaction;
- Guarantee that the Cardholder will not dispute the Transaction later (all Card Transactions are subject to Chargebacks even when an Approval Code has been obtained);
- Protect you from Chargebacks for unauthorized Transactions or disputes regarding the quality of goods or services; or
- Waive any provision of the Agreement or otherwise validate a fraudulent Transaction or a Transaction involving the use of an expired Card.

Company will follow any instructions received during Authorization. Upon receipt of an Authorization Code, Company may consummate only the Transaction authorized and must note the Authorization Code on the Transaction Receipt. In any case in which a Transaction is completed without imprinting the Card, the Company, whether or not an Authorization Code is obtained, will be deemed to warrant the true identity of the Customer as the Cardholder.

THE ELECTRONIC AUTHORIZATION PROCESS

The following diagram describes the Electronic Authorization process:

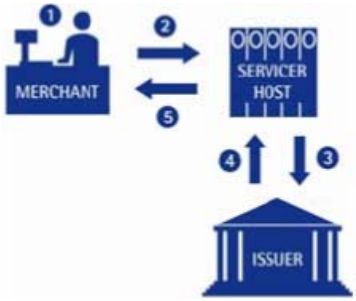

Figure 2-1. Authorization Process

1. **Authorization of Purchase:** The Transaction process begins when a Cardholder wants to buy goods or services using a Card. Before the Transaction can be completed, the Company must receive an Approval Code from the Issuer.
2. **Servicer Host:** The Company's POS Device sends the Transaction data to the Servicer Host to verify the MID, to read the Card number, and to route the information to the appropriate Issuer.
3. **Issuer:** The Servicer Host sends the information to the Issuer through the Discover Network, Visa, or MasterCard network, or directly to other Issuer networks (e.g., American Express). The Issuer determines whether the Transaction should be approved and sends one of the following responses back to the Servicer, who then forwards it to the Company:

    - **Approval Code:** Credit or funds are available to complete the sale and that the Card has not been reported lost, stolen, or otherwise invalid. The Company may complete the Transaction.
    - **Declined Code:** The Issuer does not approve the Transaction. The Company should ask for another form of payment and should not resubmit that Card for Authorization.
    - **Declined Pick-Up:** The Issuer does not approve the Transaction and requests that the Card not be returned to the Cardholder. The Card should be cut lengthwise without damaging the Magnetic Stripe and sent, along with the MID, Company address, and the date of the incident, to:

      Exception Processing

ATTN: Card Pick Up
Elavon, Inc.
7300 Chapman Highway
Knoxville, TN 37920

- **"Referral" or "Call Auth":** The Issuer requests the Company to call the Voice Authorization Center, which will either provide an Approval Code or ask the Company to request additional information from the Cardholder (e.g., mother's maiden name). The Voice Authorization Center will provide this information to the Issuer who will either approve or decline the Transaction.

4. **Servicer Host:** The Servicer Host receives the response from the Issuer and routes it to the Company.
5. **Company:** The Company receives the Issuer's response from the Servicer Host and follows the appropriate steps to complete the Transaction.

FULL AND PARTIAL AUTHORIZATION REVERSALS

For any approved amount received pursuant to an Authorization request that will not be included in a Transaction presentment for Settlement, a full or partial authorization reversal must be processed by the Company:

- Within 24 hours of the original Authorization request for Card Present Transactions; and
- Within 72 hours of the original Authorization request for Card Not Present Transactions.

This requirement does not apply if the Company is properly identified with any one of the following MCCs:

- MCCs 3351 through 3441 (Car Rental Agencies);
- MCCs 3501 through 3999 (Lodging—Hotels, Motels, Resorts);
- MCC 4411 (Cruise Lines);
- MCC 7011 (Lodging—Hotels, Motels, Resorts—not elsewhere classified); and
- MCC 7512 (automobile Rental Agency—not elsewhere classified).

SETTLEMENT

The final step in processing a Transaction is Settlement, which occurs when the Company sends all of its Card Transactions to Servicer to receive payment. During Settlement, the Company is paid and Cardholders are billed for previously-approved Transactions.

NOTE: *This process can take two or more business days (excluding holidays) unless you are set up for delayed funding.*

The following diagram describes the Settlement process:

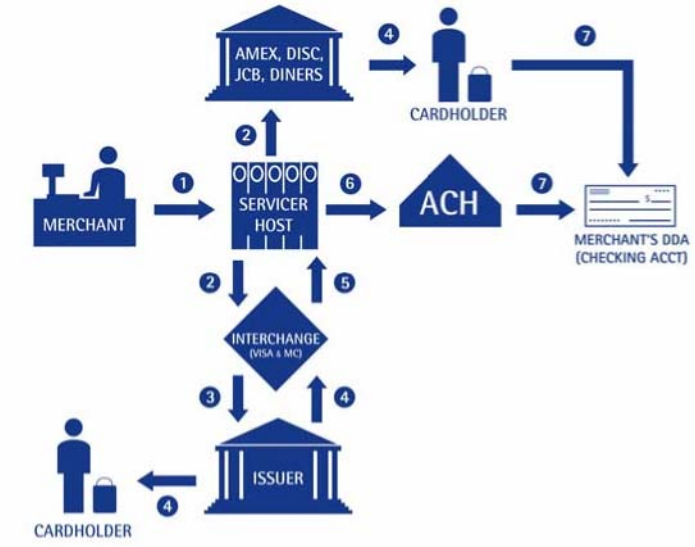

Figure 2-2. Settlement Process

PAYING THE COMPANY FOR TRANSACTIONS

1. **Company:** Sends all approved, un-settled Transactions (known as the open Batch) in the POS Device to the Servicer Host to close or settle the Batch.
2. **Servicer Host:** Sends Visa and MasterCard Card Transactions (and, if applicable, Discover Network Transactions) to Interchange and other Card Transactions to the appropriate Issuer (e.g., American Express Transactions to American Express). If the Transactions are not sent to Interchange, go to step 4.
3. **Interchange:** Sends Transaction data to the appropriate Issuer.
4. **Issuer:** Posts the Transaction to the Cardholder's account. The Issuer either sends to Interchange the difference between the Transaction amount and the Interchange fee charged to the Servicer, or sends the funds to the Company's DDA (see step 7).
5. **Interchange:** Sends the difference between the Transaction amount and the Interchange Fees to the Servicer Host.
6. **Servicer Host:** Sends a message to the Automated Clearing House (ACH) to pay the Company for the Transactions.
7. **Automated Clearing House (ACH):** Sends the funds from Servicer to the Company's DDA via electronic transfer. Fees are debited from the Company's DDA on a monthly or daily basis.

TRANSACTION PROCESSING PROCEDURES

Follow these guidelines when you process Transactions:

- Keep the Card in your hand until you complete the Transaction; the Card is required in several Transaction processing steps.
- If your POS Device displays "Referral" or "Call Auth" during a Transaction, call your toll-free Voice Authorization telephone number (located on a sticker on your POS Device) and follow the operator's instructions.
- If you receive an Approval Code, but are still suspicious about the Cardholder, Card, or circumstances of the Transaction, call for a Code 10 Authorization and follow the operator's instructions. Refer to Chapter 5, *Code 10 Procedures*, for additional information.

- Use a ballpoint pen for steps that require handwritten information. Never use a marker or a pencil to write on a Transaction Receipt.
- Do not write additional information (e.g., Cardholder's telephone number, address, driver's license number, Social Security number) on any Transaction Receipt.

To process a Transaction, follow these steps:

1. **Follow all Prompts and Enter all Data Elements.** You must include required elements to receive approval for Transactions and you can include optional data elements to qualify for better Interchange rates.

   For example: Under the current data requirements, Visa Business, Visa Corporate, and Visa Purchasing Card Transactions must include sales tax information to qualify for the Level II Interchange Rate, where applicable. Purchasing Cards only qualify if the customer code is also included in the Transaction.

2. **Make Sure the Card is Valid.** Check the Card's expiration date and other features to ensure that the Card is valid. Refer to Chapter 4, *Identifying Valid Cards* for validation information. Refer to Chapter 4, *Preventing Card Fraud* for additional loss-prevention information.

3. **Swipe the Card Through the POS Device.** If the Card is successfully swiped, the POS Device may prompt you to enter the last four digits of the Card number. This process compares the account number in the Magnetic Stripe with the account number embossed on the Card.

   If the POS Device cannot read the Magnetic Stripe, press the appropriate key to initiate a manual Transaction. When you are prompted by the POS Device, enter the Card number and expiration date embossed on the front of the Card. Make an Imprint of the Card on a paper Transaction Receipt to prove that the Card was present during the Transaction. Keep the Imprinted Transaction Receipt with the electronically printed Transaction Receipt from the POS Device.

   Ensure that the paper Transaction Receipt contains all of the information related to the Transaction, such as the Transaction amount, Transaction Date, Company information, Authorization Code, and Cardholder's signature.

4. **Enter the Amount of the Transaction.** When prompted by the POS Device, enter the amount of the Transaction using the numeric key pad. You do not need to include a decimal point.

   For Example: Enter $125.00 by pressing the **1-2-5-0-0** keys consecutively, and then pressing the **ENTER** key. The POS Device displays a message that indicates when the Transaction is being processed for Authorization.

5. **Obtain the Authorization Code.** If the Transaction is approved, the Approval Code prints on the Transaction Receipt. If a printer is not present, the POS Device displays the Approval Code. If you have to Imprint the Card, remember to record the Approval Code on the Transaction Receipt.

   If the Transaction is declined, the POS Device displays "Declined" or "Declined-Pick-Up". In these cases, you should ask for another form of payment.

   If the POS Device displays a "Referral" or "Call Auth" message, call the toll-free Voice Authorization telephone number (located on a sticker on your POS Device) and follow the operator's instructions. If you receive an Approval Code, you must enter it into your POS Device to complete the Transaction. If Authorization is declined, the Voice Authorization Center may ask you to retain the Card. If this occurs, follow the operator's instructions. A reward may be paid for the return of a Card at the Voice Authorization Center's request.

6. **Have the Cardholder Sign the Transaction Receipt, and then Compare Signatures.** In Card Present Transactions, Transaction Receipts must be signed by the Cardholder unless otherwise specified under separate criteria for a Credit Card Association program (e.g., No Signature Required Programs). Compare the signature on the Transaction Receipt with the signature on the back of the Card. If you cannot tell whether the signatures are similar, ask to see another form of identification and compare the second signature with the others. You may also compare the appearance of the Cardholder with the picture on his or her identification cards. Company must <u>not</u> honor any Card if: (i) the Card has expired; (ii) the signature on the Transaction Receipt does not correspond with the signature on the Card or if the signature panel on

the Card is blank, or uses language to the effect of "see id"; or (iii) the account number embossed on the Card does not match the account number on the Card's magnetic stripe. If you are still suspicious of the Transaction or the Cardholder, you may perform a Code 10 Authorization. Refer to Chapter 4, *Identifying Valid Cards* for more information.

7. **Return the Card and the Customer Copy of the Transaction Receipt to the Cardholder.** When the Transaction is complete, return the Card to the Cardholder, along with the Customer copy of the Transaction Receipt. Keep the Company copy of the Transaction Receipt for your records.

TRANSACTION PROCESSING RESTRICTIONS

Surcharges. Discover Network, Visa and MasterCard permit Companies in the U.S. to add a surcharge to a Credit Card Transaction amount, subject to their respective Credit Card Rules. As a result, if permitted, Company may add an amount to the posted price of goods or services Company offers as a condition of paying with a Discover Network, Visa and MasterCard Credit Card. If Company is permitted to and elects to apply a surcharge to its Discover Network, Visa and MasterCard Credit Card Transactions, Company must abide by all Payment Network Regulations applicable to surcharging, including, but not limited to, any advance notice requirements. In addition, Company may be required to register with Discover Network, Visa and/or MasterCard prior to surcharging any Credit Card Transactions. Registration requirements are set forth in the applicable Credit Card Rules and may be available through the applicable Payment Network websites. This paragraph does not prohibit Company from offering a discount or in-kind incentive to induce a person to pay by cash, Credit Card, Debit Card or any other method of payment.

Return Policy. Company must properly disclose to the Cardholder, at the time of the Transaction and in accordance with the Card Rules, any limitation Company has on accepting returned merchandise.

No Claim Against Cardholder. Unless Servicer refuses to accept a Transaction Receipt or revokes their prior acceptance of a Transaction Receipt (after receipt of a Chargeback or otherwise): (i) Company will not have any claim against, or right to receive payment from, a Cardholder in any Transaction; and (ii) Company will not accept any payments from a Cardholder relating to previous charges for merchandise or services included in a Transaction Receipt, and if Company receives such payments, Company will promptly remit them to Servicer.

TRANSACTION RECEIPTS

A Transaction Receipt is a paper or electronic record of the purchase of goods or services from a Company by a Cardholder using a Card. You must provide the Cardholder with a Transaction Receipt for his or her personal records.

Transaction Receipts are required for all Transaction types and must be retained for a minimum of two (2) years (or such longer period as the Card Rules or the Laws may require). Transaction Receipts should be stored in a safe, secure area and organized in chronological order by Transaction Date.

ELECTRONIC TRANSACTION COMPONENTS

An Electronic Transaction Receipt must contain the following information:

- Transaction Date
- Total Transaction amount, including applicable taxes, fees and any adjustments or credits
- Transaction Type (e.g., cash, debit, credit, etc.)
- Description of the goods and/or services purchased
- Card account number (must be truncated on the Cardholder copy) including the specific payment brand (e.g., Visa, MasterCard or Discover)
- Space for Cardholder signature for Card Present Transactions
- Authorization Code
- Company name and location

- Location code (i.e., POS Device or MID issued by Servicer)
- Special return or refund terms printed in close proximity to the Cardholder signature line on the Transaction Receipt, if restricted
- Indication of who will receive each copy of the Transaction Receipt (e.g., Company Copy, Bank Copy, and Cardholder Copy).

REPRODUCTION OF INFORMATION

For Card Present Transactions, if the following information embossed or printed on the Card is not legibly imprinted on the Transaction Receipt, Company will legibly reproduce on the Transaction Receipt the: (i) Cardholder's name; (ii) Card account number; (iii) Card expiration date; and (iv) Company's name and place of business.

TRUNCATION

- **Cardholder's Copy of the Transaction Receipt**. The Card account number and expiration date must be truncated on all Cardholder copies of Transaction Receipts and other paperwork provided to the Cardholder. Truncated digits should be replaced with a fill character such as "x," "*," or "#," and not with blank spaces or numeric characters. All POS Devices must suppress all but the last four (4) digits of the Card account number and the entire expiration date on the Cardholder's copy of the Transaction Receipt generated from electronic (including Cardholder-activated) POS Devices. These truncation rules do not apply to Transactions in which the only way to record a Card account number and expiration date is in handwriting or by making an Imprint or copy of the Card.
- **Company's Copy of the Transaction Receipt.** The Company's copy of the Transaction Receipt must suppress the entire expiration date. The Company may also have an obligation to suppress or truncate other information on the Company's copy of the Transaction Receipt under state or federal laws.

UNREADABLE MAGNETIC STRIPES

For Card Present Transactions, if Company authorizes and presents Transactions electronically and Company's POS Device is unable to read the Magnetic Stripe on the Card, Company must generate a manual Transaction Receipt containing the information set forth below under "Manual Transaction Components," in addition to key-entering the Transaction into the POS Device for processing.

MANUAL TRANSACTION COMPONENTS

A manual Transaction Receipt must contain the following information:

- Physical Imprint of the Card (not a photocopy)
- Identification of the Transaction type (sale, credit/refund, etc.)
- Transaction Date
- Total Transaction amount
- Cardholder signature
- Authorization Code
- Company name and location
- POS Device or MID
- Description of the merchandise or service purchased
- Special return or refund terms printed in close proximity to the Cardholder signature line on the Transaction Receipt
- Salesperson's initials or department number

NOTE: *If the Cardholder presents an unembossed Card and the POS Device cannot read the Magnetic Stripe then the Company must request another form of payment. Manual Transaction Receipts are prohibited on Transactions involving an unembossed Card.*

DELIVERY OF TRANSACTION RECEIPTS

The Company must provide a complete and legible copy of the Transaction Receipt to the Cardholder in the following manner:

- **Card Present Transactions:** Provide the Transaction Receipt to the Cardholder at the time of the Transaction.
- **Card Not Present Transactions:** Provide the Transaction Receipt to the Cardholder in either electronic (e.g., e-mail, fax) or paper (e.g., handwritten, POS Device-generated) format. Electronic Commerce Transaction Receipts must not include the Card's account number.

ELECTRONIC TRANSMISSION OF TRANSACTION RECEIPTS TO SERVICER

If Company utilizes electronic Authorization and/or data capture services, Company will enter the data related to Transactions into a POS Device and settle the Transactions and transmit the data to Servicer or its designated agent in the form specified by Servicer no later than the close of business on the date the Transactions are completed. If Servicer requests a copy of a Transaction Receipt, Credit Transaction Receipt, or other Transaction evidence, Company must provide it within the time frame specified in the request.

MULTIPLE TRANSACTION RECEIPTS

Company will include a description and total amount of goods and services purchased in a single Transaction on a single Transaction Receipt unless: (i) partial payment is entered on the Transaction Receipt and the balance of the Transaction amount is paid in cash or by check at the time of the Transaction; or (ii) a Transaction Receipt represents an advance deposit in a Transaction completed in accordance with the Agreement and the Card Rules.

DEPOSITS

Company must execute one Transaction Receipt when processing the deposit Transaction and a second Transaction Receipt upon processing the balance of the Transaction. Company will note the words "deposit" or "balance" on the applicable Transaction Receipt, as appropriate. Company will not deposit the Transaction Receipt labeled "balance" until the goods have been delivered to the Cardholder or until Company has fully performed the services.

FUTURE DELIVERY

Company represents and warrants to Servicer that Company will not rely on any proceeds or credit resulting from future delivery Transactions to purchase or furnish goods or services. Company will maintain sufficient working capital to provide for the delivery of goods or services at the agreed upon future date, independent of any credit or proceeds resulting from Transaction Receipts or other Credit Transaction Receipts in connection with future delivery Transactions.

PROCESSING CARD NOT PRESENT TRANSACTIONS

Card Not Present Transactions include Mail Order (MO), Telephone Order (TO), and Electronic Commerce (EC) Transactions. These Transactions occur when the Card is not physically presented to the Company at the time of a sale. You must be authorized by us to process Card Not Present Transactions.

If more than twenty percent (20%) of your Transactions are MO/TO, you must apply for a separate MID for those Transactions. If more than one percent (1%) of your Transactions are Electronic Commerce orders, you must also apply for a separate MID for those Transactions.

MAIL ORDER/TELEPHONE ORDER (MO/TO)

Company understands that Transactions processed via MO/TO are high risk and subject to a higher incidence of Chargebacks. Company is liable for all Chargebacks and losses related to MO/TO Transactions. Company may be required to use an address verification service ("**AVS**") on MO/TO Transactions. AVS is not a guarantee of payment and the use of AVS will not waive any provision of the Agreement or validate a fraudulent Transaction. Company will obtain the expiration date of the Card for a MO/TO Transaction and submit the expiration date when requesting Authorization of the Transaction. For MO/TO Transactions, Company will type or print legibly on the signature line of the Transaction Receipt the following applicable words or letters: telephone order or "TO," or mail order or "MO," as appropriate. Servicer recommends that Company obtain a signed Transaction Receipt or other proof of delivery signed by Cardholder for MO/TO Transactions.

ELECTRONIC COMMERCE (EC)

Company may process Electronic Commerce Transactions only if the Transactions have been encrypted by Servicer or a third party vendor acceptable to Servicer. Company understands that Transactions processed via the Internet are high risk and subject to a higher incidence of Chargebacks. Company is liable for all Chargebacks and losses related to Electronic Commerce Transactions, whether or not such Transactions have been encrypted. Encryption is not a guarantee of payment and does not waive any provision of the Agreement or otherwise validate a fraudulent Transaction. Servicer recommends that Company obtain a signed Transaction Receipt or other proof of delivery signed by the Cardholder for all Electronic Commerce Transactions. All communication costs and compliance with Laws related to Electronic Commerce Transactions will be Company's responsibility. Company understands that Servicer will not manage the telecommunications link for Electronic Commerce Transactions and that it is Company's responsibility to manage that link. Company authorizes Servicer to perform an annual audit and examination of Company's website and such other due diligence review as required by the Payment Network Regulations for Electronic Commerce Companies.

Requirements. Company's website must contain all of the following information: (a) prominently display the name of the Company; (b) prominently identify the name of the Company as displayed on the website as both the Company and as the name that will appear on the Cardholder statement; (c) display Company name information as prominently as any other information depicted on the website, other than images of the products or services being offered for sale; (d) complete description of the goods or services offered; (e) returned merchandise and refund policy; (f) customer service contacts, including electronic mail address and/or telephone number; (g) complete address (street address, city, state, zip code, and country) of the permanent establishment of the Company's business; (h) complete address of the permanent establishment of the Company's business on either the checkout screen (which displays the total purchase amount) or within the sequence of website pages presented to the Cardholder during the checkout process; (i) Transaction currency (such as U.S. or Canadian dollars); (j) export or legal restrictions, if known; (k) delivery policy; (l) Customer data privacy policy; and (m) Company's method of Transaction security such as Secure Sockets layer (SSL) or 3-D Secure. If Company stores Card account numbers, expiration dates, or other personal Cardholder data in a database, Company must follow the applicable Payment Network Regulations on securing such data. Company may not retain or store CVV2/CVC2/CID data after authorization for record keeping or additional authorization processing. A Company must not refuse to complete an Electronic Commerce Transaction solely because the Cardholder does not have a digital certificate or other secured protocol.

Shipped Goods. For goods to be shipped on Electronic Commerce Transactions, Company may obtain authorization up to seven (7) days prior to the shipment date. Company need not obtain a second authorization if the Transaction Receipt amount is within fifteen percent (15%) of the authorized amount, provided the additional amount represents shipping costs.

Card Not Present Transactions pose a higher risk of fraud and Chargebacks, so it is important that you take precaution in processing these Transactions. Follow these guidelines **prior** to processing a Card Not Present Transaction, as applicable:

- Use a ballpoint pen when handwritten information is required. Never use a marker or pencil when writing on a Transaction Receipt.
- Obtain the following information from the Cardholder, if needed:
  - Cardholder's billing address
  - Shipping address, if different from billing address
  - Cardholder's telephone number
  - Cardholder's account number
  - Card expiration date
  - CVV2/CVC2/CID number
  - Purchaser's name (in lieu of Cardholder signature)

NOTE: *You must not retain or record the CVV2/CVC2/CID data element beyond the original Authorization request. Further, the CVV2/CVC2/CID data element must not be printed on the Transaction Receipt or on any document given to the Cardholder.*

In addition to the Transaction Receipt requirements set out in Chapter 2, *Processing Transactions*, a Card Not Present Transaction Receipt must also contain:

- Company online address
- Customer service contact, including telephone number

Do not settle a Transaction before shipping the goods. This increases the risk of a Chargeback to the Company and is prohibited by the Agreement.

Do not retain magnetic stripe data except for first time use.

MANUAL TRANSACTION RECEIPTS FOR CARD NOT PRESENT TRANSACTIONS

Follow these steps for manual Transaction Receipts:

1. **Write the Cardholder's Name and Card Number on the Transaction Receipt.** Refer to Chapter 2, *Processing Transactions – Electronic Transaction Components* for information on Transaction Receipt requirements. In addition to the electronic Transaction components requirements, a manual Transaction Receipt for a Card Not Present Transaction may include the full Card account number and expiration date and must include the Cardholder's billing address (and shipping address, if different) and telephone number. Do not record CVV2/CVC2/CID data elements on the Transaction Receipt.
2. **Record the Order Type on the Transaction Receipt.** Write one of the following on the signature line of the Transaction Receipt:
   - "Mail Order"
   - "Telephone Order"
   - "Internet"

POS DEVICE GENERATED RECEIPTS

If you are using a POS Device to generate a Transaction Receipt for a Card Not Present Transaction, enter the Transaction into the device by following these steps:

1. Press the appropriate key on your POS Device to initiate the Transaction.
2. When prompted, enter the Card number.

3. When prompted again, enter the Card expiration date.
4. Finally, when prompted, enter the Transaction amount.
5. Record the Authorization Code on the Transaction Receipt. Refer to Chapter 2, *Processing Transactions – Transaction Receipts* for more information.

CARD IDENTIFICATION NUMBER AND ADDRESS VERIFICATION SERVICE

The use of CVV2/CVC2/CID and AVS can lessen your risk of Chargebacks by providing you with additional information to assist with your decision on whether or not to process a Card Not Present Transaction.

NOTE: *The use of CVV2/CVC2/CID and AVS will not relieve you of liability for Chargebacks. Remember, you bear the risk of loss associated with any Chargeback.*

If you are using these services, follow the next two steps **prior** to processing a Transaction.

1. **Verify the Card Identification Number (CVV2/CVC2/CID) Printed on the Front or Back of the Card (at the end of the Card Account Number in the Signature Panel), as Applicable to the Specific Card Type.** If your POS Device is set up for CVV2/CVC2/CID and if the CVV2/CVC2/CID number is provided at the time of Authorization, the Issuer returns either a "match" or a "no match" response. "Match" means it is more likely that the Card is present and in the hands of the Cardholder at the time of the Transaction. "No match" means you should consider whether or not to process the Transaction. Even though you receive an Approval Code with a "no match" response, the Approval Code is not a guarantee of payment. The decision to process a Transaction, regardless of the response received, is up to you, because you are responsible for any risk associated with processing a Transaction.

   NOTE: *You must not retain or record the CVV2/CVC2/CID data element beyond the original Authorization request. Further, the CVV2/CVC2/CID data element must not be printed on the Transaction Receipt or on any document given to the Cardholder.*

   Most Customers do not know where the CVV2/CVC2/CID code is located on the Card. To assist a Customer, have him or her locate the last three (or four) alphanumeric characters in the signature panel on the back of his or her Card for Discover Network, Visa or MasterCard Card types or on the front of his or her Card for American Express Card types.

   Refer to Chapter 4, *Unique Card Characteristics*, for more details concerning the Card Identification Number. The following table sets forth CVV2/CVC2 response codes.

Code	Definition
Space	CVV2 processing not requested
M	CVV2/CVC2 Match
N	CVV2/CVC2 not matched
P	Not processed
S	CVV2 should be printed on the card, but it was indicated that the value was not present
U	Issuer does not support CVV2
X	Service provider did not respond

2. **Verify the Cardholder's Address by Using the Address Verification Service (AVS).** If your POS Device is set up for AVS, it prompts you to enter the numeric portion of the Cardholder's billing address and the five digit zip code to verify that the individual providing the Card account number is the Cardholder. The AVS result code indicates whether the address given by the Cardholder matches (exactly, partially, or not at all) the address that the Issuer has on file for the Card. "Exactly" means it is more likely that the Card is being used by the authorized Cardholder. "Partially" or "not at all"

means you should consider whether or not to process the Transaction. The decision to process a Transaction, regardless of the response received, is up to you, as you are responsible for any risk associated with processing a Transaction. Even though you will receive an Approval Code following a "no match" response, the Approval Code is not a guarantee of payment. The following table sets forth AVS response codes.

Code	Definition
A	Address (street) matches - ZIP Code does not
B	Street address match, postal code in wrong format (international issuer)
C	Street address and postal code in wrong formats
D	Street address and postal code match (international issuer)
E	Error response for Merchant Category Code (SIC)
G	Card issued by a non-U.S. issuer that does not participate in the AVS system
I	Address information not verified by international issuer
M	Street address and postal code match (international issuer)
N	No match on address (street) or ZIP Code
O	No response sent
P	Postal codes match, Street address not verified due to incompatible formats
R	Retry, system is unavailable or timed out
S	Service not supported by issuer
U	Address information is unavailable (domestic issuer)
W	Nine-digit ZIP Code matches - Address (street) does not match
X	Exact AVS Match
Y	Address (Street) and five digit Zip match
Z	Five-digit zip matches - address (street) does not match

NOTE: *For more information about CVV2/CVC2/CID and AVS, contact merchant services.*

For more information about processing Card Not Present Transactions, call the following numbers:

- MC (MasterCard) Assist: (800) 622-7747
- Visa's Company Assistance Service: (800) 847-2750
- American Express: (800) 528-2121
- Discover Network: (800) 347-1111

The information provided by calling these numbers may allow you to verify a Cardholder's address and obtain the Issuer's telephone number.

PAPER DRAFTS

We supply you with the materials and forms that you need to process Discover Network, Visa or MasterCard Transactions using paper drafts. You must maintain a supply of these materials. Refer to Chapter 29, *Supplies* for more information.

Before you process a paper draft, please follow the guidelines under *Transaction Processing Procedures* earlier in this Chapter.

To correctly process a paper Transaction Receipt, follow these steps:

1. **Make Sure the Card is Valid.** Check the Card's expiration date and other features to ensure that the card is valid. Refer to Chapter 4, *Identifying Valid Cards* for validation information. Refer to Chapter 4, *Preventing Card Fraud* for additional loss-prevention information.

2. **Imprint the Transaction Receipt.** Make a legible Imprint of the Card on all copies of the Transaction Receipt.
3. **Call for Authorization.** Call the Voice Authorization number provided on the sticker on your POS Device and have the following information available:
   - Card account number
   - MID
   - Amount of sale (dollars and cents)
   - Card expiration date
4. **Write the Approval Code in the Space Provided on the Transaction Receipt.** The Approval Code is required.
5. **Have the Cardholder Sign the Transaction Receipt, and then Compare Signatures.** Compare the signature on the Transaction Receipt with the signature on the back of the Card. If you cannot tell whether the signatures are similar, ask to see another form of identification and compare the second signature with the others. You may also compare the appearance of the Cardholder with the picture on his or her identification cards. If you are still suspicious of the Transaction or the Cardholder, you may perform a Code 10 Authorization. Refer to Chapter 4, *Identifying Valid Cards* for more information.
6. **Return the Card and the Cardholder Copy of the Transaction Receipt to the Cardholder.** When the Transaction is complete, return the Card to the Cardholder, along with the Cardholder copy of the Transaction Receipt. Make sure to keep the Company copy of the Transaction Receipt for your records.
7. **Storage of Paper Drafts.** It is important to keep copies of your Transaction Receipts in a safe place, filed by Transaction Date. This is especially important for quickly locating a receipt if questions arise. The PCI Data Security Standard sets out the requirements on how to handle the storage of paper drafts that contain Cardholder information.

   Visit **http://www.pcisecuritystandards.org/security_standards/pci_dss.shtml** or contact Customer Service at 1-800-725-1243 for more information.

PROCESSING CREDIT TRANSACTIONS

Credit Transaction Receipt. Company must issue a Credit Transaction Receipt, instead of issuing cash or a check, as a refund for any previous Transaction. Servicer will debit the DDA for the total face amount of each Credit Transaction Receipt submitted to Servicer. Company must not submit a Credit Transaction Receipt relating to any Transaction Receipt not originally submitted to Servicer, and Company must not submit a Credit Transaction Receipt that exceeds the amount of the original Transaction Receipt. Company must, within the time period specified by applicable Laws or the Card Rules, whichever time period is shorter, provide Servicer with a Credit Transaction Receipt for every return of goods or forgiveness of debt for services that was the subject of a previous Transaction in accordance with the Card Rules.

Revocation of Credit. Servicer may, in its reasonable discretion, refuse to accept any Credit Transaction Receipt for processing.

Reprocessing. Company must not resubmit or reprocess any Transaction that has been charged back.

RETURNS AND EXCHANGES

Refunds for a Transaction must be processed by issuing a credit to the Card on which the original purchase was made. You must also prepare a Credit Transaction Receipt for the amount of credit issued. Do not refund a Card purchase with cash or check. Do not refund cash or check purchases to a Card.

If you have a special policy regarding returns or refunds, make sure that the policy is:

- Clearly posted at the point-of-sale

- Printed on the Transaction Receipt using letters approximately ¼ inch high and in close proximity to the signature line

If you are processing an even exchange, no action is necessary. However, if an exchange involves merchandise of greater or lesser value, you must issue a Transaction Receipt or a Credit Transaction Receipt for the difference. If you prefer, you may instead give a full refund to the Cardholder for the original Transaction amount and process the exchange as a new Transaction.

Additional Requirements Applicable To Debit Card, PIN-Authorized Debit Card and Prepaid Card Transactions

With respect to Debit Card, PIN-authorized Debit Card, and Prepaid Card Transactions, Companies operating in the Merchant Category Codes in the table below must:

1. For all Card Present Transactions occurring at an attended POS Device or at a Cardholder-activated POS Device identified with MCC 5542 (Automated Fuel Dispensers), support partial approvals;
2. For all Transactions, support full and partial reversals; and
3. For all Card Present Transactions occurring at an attended POS Device and conducted with a Prepaid Card, support account balance responses;

each as further described below.

MCC
4111 Transportation—Suburban and Local Commuter Passenger, including Ferries
4812 Telecommunication Equipment including Telephone Sales
4814 Telecommunication Services
4816 Computer Network/Information Services
4899 Cable, Satellite, and Other Pay Television and Radio Services
5111 Stationery, Office Supplies
5200 Home Supply Warehouse Stores
5300 Wholesale Clubs
5310 Discount Stores
5311 Department Stores
5331 Variety Stores
5399 Miscellaneous General Merchandise Stores
5411 Grocery Stores, Supermarkets
5499 Miscellaneous Food Stores — Convenience Stores, Markets, Specialty Stores and Vending Machines
5541 Service Stations (with or without Ancillary Services)
5542 Fuel Dispenser, Automated
5732 Electronic Sales
5734 Computer Software Stores
5735 Record Shops
5812 Eating Places, Restaurants
5814 Fast Food Restaurants
5912 Drug Stores, Pharmacies
5921 Package Stores, Beer, Wine, and Liquor
5941 Sporting Goods Stores
5942 Book Stores

5943 Office, School Supply and Stationery Stores
5964 Direct Marketing—Catalog Merchants
5965 Direct Marketing—Combination Catalog—Retail Merchants
5966 Direct Marketing—Outbound Telemarketing Merchants
5967 Direct Marketing—Inbound Telemarketing Merchants
5969 Direct Marketing—Other Direct Marketers—not elsewhere classified
5999 Miscellaneous and Specialty Retail Stores
7829 Motion Picture-Video Tape Production-Distribution
7832 Motion Picture Theaters
7841 Video Entertainment Rental Stores
7996 Amusement Parks, Carnivals, Circuses, Fortune Tellers
7997 Clubs—Country Membership
7999 Recreation services—not elsewhere classified
8011 Doctors — not elsewhere classified
8021 Dentists, Orthodontists
8041 Chiropractors
8042 Optometrists, Ophthalmologists
8043 Opticians, Optical Goods, and Eyeglasses
8062 Hospitals
8099 Health Practitioners, Medical Services — not elsewhere classified
8999 Professional Services—not elsewhere classified
9399 Government Services —not elsewhere classified

Partial Approvals. When a Debit Card, PIN-authorized Debit Card, or Prepaid Card Authorization request is sent, the issuer can respond with an approval amount less than the requested amount. When the approved amount is less than the originally requested amount, Company should prompt the Customer to pay the difference with another form of payment. If the Customer does not wish to proceed with all or part of the Transaction (or if the Transaction "times out"), the Company must initiate an authorization reversal Transaction.

Full and Partial Authorization Reversals. An "authorization reversal" is a real-time Transaction initiated when the Customer decides that it does not want to proceed with the Transaction or if the Company cannot complete the Transaction for any reason (e.g., the item is out of stock, the Transaction "times out" while waiting for the Authorization response, etc.). To initiate an authorization reversal, the Transaction must have already been authorized but not submitted for Settlement. If the Transaction has already been submitted for clearing, then the Company should initiate a void, refund, or other similar Transaction so that the Customer's open-to-buy is freed up and the available balance is restored. A partial authorization reversal should be initiated whenever the Company determines that the final Transaction amount will be less than the amount of the Authorization.

Authorization reversals must be processed by the Company within 24 hours of the original Authorization request for Card Present Transactions and within 72 hours of the original Authorization Request for Card Not Present Transactions; provided, however, that Companies in hotel, lodging, cruise line and vehicle rentals are exempt from this requirement.

Account Balance Response. For some Prepaid Cards, the Issuer is required to include the remaining available balance on the Cardholder's account in the Authorization response message. If the remaining available balance is included, the Company must print it on the Transaction Receipt or display it on a Customer facing POS Device.

ADDITIONAL REQUIREMENTS APPLICABLE TO PIN-AUTHORIZED DEBIT CARD TRANSACTIONS

Debit Card Rules. Company will comply with and be bound by the Debit Card Rules, which are incorporated by this reference as if fully set forth herein. Except as otherwise provided below, Company must comply with the general Card acceptance and Transaction processing provisions in this Chapter when accepting Debit Cards. The Debit Card Rules are confidential information of the Payment Networks, and Company will not disclose the Debit Card Rules to any Person except as may be permitted under the Agreement or under requirements of Laws.

Use and Availability of POS Devices and PIN Pads.

- A Cardholder's Debit Card information and PIN are confidential. The Company may not request or require a Cardholder to disclose his or her PIN at any point during a Transaction.
- During the Transaction process, the Company must provide a reasonably secure area for Cardholders to enter their PIN into the PIN Pad. Company is responsible for installing the POS Device and PIN Pad in such a way that Cardholders may enter their PIN into the PIN Pad in a confidential manner.
- Company will cause a POS Device and PIN Pad to be readily available for the use of all Cardholders at all of Company's business locations where PIN-authorized Debit Cards are accepted. Company will take all reasonable steps to ensure that all POS Devices and PIN Pads operated at Company's business locations function with a minimum of error, in a reliable manner, and in accordance with the standards established from time to time by Servicer and the EFT Networks.
- Company will use a POS Device to initiate every PIN-authorized Debit Card Transaction, and Company will require that either the Cardholder or the Company insert and "swipe" the Debit Card through the POS Device to initiate every PIN-authorized Debit Card Transaction, except as set forth herein. No PIN-authorized Debit Card Transaction may be initiated unless the Debit Card is physically present.
- Company will require that each Debit Cardholder enter his or her PIN utilizing a PIN Pad at the POS Device when initiating a PIN-authorized Debit Card Transaction. Company may not require a Debit Cardholder initiating a PIN-authorized Debit Card Transaction to sign a Transaction Receipt or other receipt, or require any other means of identification.

No Minimum or Maximum. Company will not establish minimum or maximum Debit Card Transaction amounts except to establish a maximum cash back dollar amount not to exceed $200.00 or such lower amount as may be required under applicable Payment Network Rules.

Pre-Authorization Requests. Company may initiate pre-authorization requests pursuant to the following procedures:

- The Cardholder must enter the PIN on the PIN Pad.
- The Debit Card must be inserted and "swiped" through the POS Device.
- The pre-authorization request must be for a specific dollar amount and only goods and services, including applicable taxes, may be purchased. The subsequent purchase pre-authorized hereunder must be completed within two (2) hours after the original pre-authorization request.
- Funds will not be transferred with respect to a pre-authorization request.
- In order to complete the subsequent purchase pre-authorization, Company will transmit a completion message indicating the actual dollar amount of the Debit Card Transaction, and will comply with all requirements of a purchase Debit Card Transaction, at that time, except that entry of a PIN and "swiping" of a Debit Card is not required to complete the subsequent purchase if these steps were properly taken in order to pre-authorize such purchase. Such subsequent purchase will not be authorized or completed unless the actual dollar amount of the purchase is less than or equal to the amount specified in the pre-authorization request.

- If Company initiates pre-authorization requests, it will support the processing of partial pre-authorizations.

Debit Card Transactions. Companies that accept PIN-authorized Debit Cards will support the following Debit Card Transactions:

- Purchases, and
- Merchandise credits.

Company may also support the following Debit Card Transactions if supported by the applicable EFT Network:

- Purchase with cashback, and
- Balance inquiries.

Prohibited Transactions. Company will initiate Transactions only for products or services approved by Servicer. In no event will Company initiate, allow, or facilitate a gambling or gaming transaction, or fund a stored value account for such purposes.

Transaction Receipt Requirements. At the time of any Debit Card Transaction (other than a balance inquiry or pre-authorization request), Company will make available to each Cardholder a Transaction Receipt that complies fully with all Laws and containing, at a minimum, the following information:

- Amount of the Debit Card Transaction;
- Date and local time of the Debit Card Transaction;
- Type of Transaction;
- If during the Debit Card Transaction the Cardholder is prompted to select the type of account used, then the type of account accessed must be displayed on the Transaction Receipt;
- Truncated Debit Card number (showing the final four (4) digits);
- Company's name and location at which the Debit Card Transaction was initiated;
- Trace or retrieval reference number;
- Authorization Code;
- Unique number or code assigned to the POS Device at which the Debit Card Transaction was made; and
- Status and disposition of transaction (approved or declined).

Merchandise Returns. Company may electronically perform a merchandise return (if permitted by the applicable EFT Network) for a Debit Card Transaction only at the same Company named on the Transaction Receipt where the original Debit Card Transaction was initiated. If permitted, a merchandise return requires the following procedures:

- The Cardholder must re-enter the PIN on the PIN Pad;
- The Debit Card must be inserted and "swiped" through the POS Device; and
- Company must transmit the reference number or Authorization Code and the exact dollar amount of the Debit Card Transaction to be returned.

For all merchandise returns or any other debit return initiated through Company's POS Device or account, Company bears all responsibility for such Transaction even if fraudulent.

Balance Inquiries. Company may accommodate balance inquiries if the applicable EFT Network and the Issuer support the balance inquiry function, provided that the Company requires that the Cardholder enter their PIN on the PIN Pad and insert and "swipe" the Debit Card through the POS Device.

Purchase with Cash Back. Company may offer purchase with cash back Transactions pursuant to the following procedures:

- For each purchase with cash back, Company will transmit in its Transaction message the amount of cash given to the Cardholder (if permitted by Servicer's Debit System).
- If a request for Authorization of a purchase with cash back is denied solely because the cash requested exceeds the Debit Card Issuer's limit on cash withdrawals, Company will inform the Cardholder of the reason for the denial and that a new purchase Transaction in the amount of the purchase alone might be approved.
- The amount of cash back may be limited by the EFT Networks or Issuer.

Technical Problems. Company will ask a Cardholder to use an alternative means of payment if the Servicer Debit System, the POS Device, or the PIN Pad is inoperative, the electronic interface with any EFT Network is inoperative, or the magnetic stripe on a Debit Card is unreadable, and Company elects not to or is unable to store Debit Card Transactions.

Adjustment. A Debit Card Transaction may be adjusted if an error is discovered during Company's end-of-day balancing only by means of a written request from Company to Servicer. The request for adjustment must reference a settled Debit Card Transaction that is partially or completely erroneous or a denied pre-authorize Transaction for which the pre-authorization request was approved. An adjustment must be completed within forty-five (45) days after the date of the original Debit Card Transaction.

Termination/Suspension. When requested by any EFT Network, in its sole discretion, Company will immediately take action to: (i) eliminate any fraudulent or improper Transactions; (ii) suspend the processing of Debit Card Transactions; or (iii) entirely discontinue acceptance of Debit Card Transactions.

SPECIAL REQUIREMENTS APPLICABLE TO INTERNET PIN-BASED CARD TRANSACTIONS

Acceptance of Internet PIN-Based Card Transactions. This section describes certain special requirements applicable to Internet PIN-Based Card Transactions. Except as specifically provided in this section, Company will comply with the general provisions of this Chapter regarding PIN-authorized Debit Card Transactions with respect to Internet PIN-Based Card Transactions. For the avoidance of doubt, Internet PIN-Based Card Transactions are Card Not Present Transactions. Therefore, notwithstanding anything in this Operating Guide to the contrary, Company is not required to "swipe" a Card in conjunction with any Internet PIN-Based Card Transaction and the Cardholder and the Card are not required to be present at the time of the sale. Fees for Internet PIN-Based Card Transactions will include Authorization, Interchange and access fees, as defined by the respective EFT Network or International Network.

Domestic Internet PIN-Based Debit Card Processing Services. If Company has elected to receive Domestic Internet PIN-Based Debit Card Processing Services, Company may submit for processing Domestic Internet PIN-Based Debit Card Transactions involving Debit Cards issued for acceptance over those EFT Networks identified by Servicer from time to time. Company acknowledges that Servicer may not be able to accept Transactions for Debit Cards on all the EFT Networks.

International Network Requirements.

a. If Company has elected to receive International Internet PIN-Based Card Processing Services, Company may submit for processing International Internet PIN-Based Card Transactions involving Cards issued for acceptance over the International Networks identified on Schedule A (Schedule of Fees) to the Agreement.

b. Company is not permitted to submit International PIN-Based Credit Card Transactions for processing pursuant to this Chapter unless specifically indicated on Schedule A (Schedule of Fees) to the Agreement.

c. Except to the extent superseded by this Chapter, Company's acceptance and processing of International Internet PIN-Based Card Transactions will comply with the provisions of the Operating Guide applicable to acceptance and processing of PIN-based Debit Card Transactions, and references to "Debit Cards" in such provisions will be understood to include International Debit Cards (and, if Company is permitted to accept International PIN-Based Credit Card Transactions pursuant to Schedule A (Schedule of Fees) to the Agreement, International Credit Cards).

d. If Company supports Internet PIN-Based Card Transactions, Company will comply with and be bound by the International Network Requirements and Internet PIN-Based Card Transaction Documentation, which are incorporated by this reference as if fully set forth herein. The International Network Requirements and Internet PIN-Based Card Transaction Documentation are confidential information of the International Networks or of Servicer, as applicable, and Company will not disclose the International Network Requirements or the Internet PIN-Based Card Transaction Documentation to any Person except as may be permitted under the Agreement or under requirements of Laws. If compliance with this Chapter, any other part of the Operating Guide, or the Agreement would cause Company to violate applicable International Network Requirements or Laws, Company will comply with such International Network Requirements or Laws.

Use and Availability of Internet PIN Pads.

- A Cardholder's Card information and PIN are confidential.
- During the Transaction process, an Internet PIN Pad with appropriate technology will be used to maintain the confidentiality of the Cardholder's Card information and PIN.
- Company will use appropriate technology for every Internet PIN-Based Card Transaction so as to prevent the unauthorized recording or disclosure of a Cardholder's PIN.
- Company will take all reasonable steps to ensure that all Internet PIN Pads operated at Company's internet website function with a minimum of error, in a reliable manner, and in accordance with the standards established from time to time by Servicer and the applicable EFT Networks or International Networks.
- Company will require that each Cardholder enter his or her PIN on an Internet PIN Pad when initiating an Internet PIN-Based Card Transaction.

Surcharges. Company may not add any amount to the posted price of goods or services Company offers as a condition of paying with a Card except as permitted by the Operating Guide and the applicable Card Rules or International Network Requirements.

Transaction Receipt Requirements. At the time of any Internet PIN-Based Card Transaction, Company will make available to each Cardholder a Transaction Receipt that complies with all International Network Requirements and Laws and includes:

- Amount of the Internet PIN-Based Card Transaction, or if a Convenience Fee applies, the amount debited from the Cardholder's account (exclusive of the Convenience Fee, shipping, handling and other fees), and the amount debited from the Cardholder's account (inclusive of the fees);
- Description of the goods or services and, for transactions involving the shipment of goods, the promised ship-by date;
- Date and local time (at Company's physical address) of the Internet PIN-Based Card Transaction;
- Type of Transaction;
- Authorization Code, if available;
- Type of account accessed;
- Truncated Card number (showing the final four (4) digits);
- Cardholder's name, email address, and telephone number;
- Company's name, Merchant Identification Number, customer service contact information, and the website address at which the Internet PIN-Based Card Transaction was initiated; and
- Trace or retrieval reference

Refunds / Cashback / Balance Inquiries. If permitted by the applicable International Network or EFT Network, Company may electronically perform a merchandise return or refund for an Internet

PIN-Based Card Transaction. However, credits, balance inquiries and purchases with cash back cannot be performed as Internet PIN-Based Card Transactions.

Merchandise Returns. Company may electronically perform a merchandise return (if permitted by the applicable EFT Network or International Network) for an Internet PIN-Based Card Transaction only if Company initiates the original Internet PIN-Based Card Transaction. If such returns are permitted, Company will transmit the reference number or authorization number and the exact dollar amount of the Internet PIN-Based Card Transaction to be refunded.

Technical Problems. Company will ask a Cardholder to use an alternative means of payment if the Servicer Debit System, the Internet PIN Pad, or the electronic interface with any EFT Network or International Network is inoperative.

Termination / Suspension. When requested by Servicer, Company will immediately (i) eliminate any fraudulent or improper Transactions; (ii) suspend or terminate the acceptance of Internet PIN-Based Card Transactions with respect to a specific EFT Network or International Network; or (iii) suspend or terminate the acceptance of all Internet PIN-Based Card Transactions.

Risk of Internet PIN-Based Card Transactions. Company understands that Internet PIN-Based Card Transactions may be high risk and there is a risk that a Cardholder's PIN may be tracked or improperly disclosed if the Internet PIN Pad and other appropriate security technology is not in place. Company is responsible for implementing and maintaining its own security technology. Accordingly, Company indemnifies Servicer against any claims made by a Cardholder regarding the unauthorized disclosure of such Cardholder's PIN in any Internet PIN-Based Card Transactions submitted to Servicer for processing.

OTHER TRANSACTION TYPES

Company may solicit the following other Transaction types provided that (a) Company discloses such method of processing to Servicer in the Company Application or otherwise in writing, (b) Company has been approved by Servicer to submit such Transactions, and (c) Company meets the additional requirements for the applicable type of Transaction set out below. If Company completes any of these Transaction types without having received Servicer's approval, then Company will be in breach of the Agreement and Servicer may terminate the Agreement in addition to any other remedies available under the Agreement, Laws, or Payment Network Regulations, and Company may pay a surcharge on each such Transaction.

RECURRING PAYMENTS AND PRE-AUTHORIZED ORDERS

Recurring Payments are Transactions for which a Cardholder provides written permission or electronic authorization to a Company to periodically charge his or her Card for recurring goods or services (e.g., monthly membership fees, utility bills, insurance premiums, or subscriptions). When processing Recurring Payments, you must obtain a separate Authorization Code for each Transaction.

Pre-authorized Orders are Transactions in which the Cardholder provides written or electronic authorization to charge his or her Card, one or more times, at a future date. You must be authorized by us to process Pre-authorized Orders.

You must obtain a signed order form or other written agreement from the Cardholder for all Recurring Payments and Pre-authorized Orders. The order form or agreement must contain the following information:

- Card number
- Card expiration date
- Cardholder's name
- Cardholder's signature

- Transaction amount (charged to the Cardholder's Card)
- Charge frequency (weekly, monthly, etc.)
- Length of time over which the recurring charges will occur
- The words "Recurring Payment" or "Pre-authorized Order" written on the signature line of the Transaction Receipt

You must keep a copy of the order form or written agreement for the duration of the recurring service. You must also provide a copy of the order form or agreement for Recurring Payments or Pre-authorized Orders to us upon request. A new order form or written agreement with the Cardholder is needed when a Recurring Payment is renewed.

Recurring Transaction Requirements. Company will not complete any recurring Transaction after receiving: (i) a cancellation notice from the Cardholder; (ii) a notice from Servicer that authority to accept recurring Transactions has been revoked; or (iii) a response that the Payment Device is not to be honored. Company is responsible for ensuring its compliance with Laws with respect to recurring Transactions.

Limitations on the Resubmission of Recurring Transactions. In some limited instances, Company may resubmit a declined preauthorized recurring Transaction up to four (4) times within sixteen (16) calendar days of the original Authorization request, provided that the decline response is one of the following: (i) authorization denied; (ii) insufficient funds; (iii) exceeds approval amount limit; or (iv) exceeds withdrawal frequency.

Recurring Transaction Receipts. Company must print legibly on the Transaction Receipt the words "Recurring Transaction." Company must obtain the Cardholder's signature, which may be an electronic signature or other similar authentication that is effective under applicable Laws, on the Transaction Receipt. Company must also include the frequency and duration of the Recurring Transaction authorization, as agreed to by the Cardholder, on the Transaction Receipt.

Electronic Commerce Recurring Transactions. In addition to the above, for an Electronic Commerce Transaction, Company must also provide a simple and easily accessible online cancellation procedure that complies with Laws, if the Cardholder's request for goods or services was initially accepted online.

Recurring Transactions with Varying Amounts. For Recurring Transactions of varying amounts, all of the following apply: (i) the order form must allow the Cardholder to specify a minimum and maximum Transaction amount to be charged, unless the Cardholder will be notified of the amount and date of each charge, as specified in the remainder of this section; (ii) Company must inform the Cardholder of their right to receive, at least ten (10) calendar days prior to each scheduled Transaction Date, written notification of the amount and date of the next charge; and (iii) the Cardholder may choose to receive the notification in any of the following ways: (a) for every charge; (b) when the Transaction amount does not fall within the range of amounts specified on the order form; or (c) when the Transaction amount will differ from the most recent charge by more than an agreed upon amount. Company is responsible for ensuring that all communications with, and disclosures to, Cardholders comply with Laws.

To perform a Pre-authorized Order, follow these specific guidelines:

- Separately authorize each Transaction for the exact amount of that Transaction, instead of authorizing the entire amount of all the Transactions or no amount at all.
- If applicable to the Transaction, write the words "Delayed Delivery," and "Deposit" or "Balance" on the Transaction Receipt. The Authorization date and Authorization Code must also be printed on the Transaction Receipt.

While you may process the Transaction for the "Deposit" before delivery of the goods and/or services, you may not process the "Balance" of the Transaction until the goods and/or services are delivered.

QUASI-CASH TRANSACTIONS

Quasi-Cash Transactions represent the sale of items that are directly convertible to cash. Examples of Quasi-Cash Transactions include:

- Casino gaming chips
- Money orders
- Deposits
- Wire transfer money orders
- Travelers cheques
- Travel money cards
- Foreign currency

You must be authorized by us to process Quasi-Cash Transactions. No Company may process a Quasi-Cash Transaction as a cash disbursement.

ACCEPTANCE AND ADDITIONAL REQUIREMENTS

In addition to the general requirements described in Chapter 2, *Transaction Receipts*, Companies processing Quasi-Cash Transactions must:

- Review identification (such as a valid passport or driver's license) to validate the Cardholder's identity.
- Record the type of identification presented by the Cardholder on the Transaction Receipt, along with the serial number, expiration date, and Cardholder name (if different than the embossed name on the Card) and address.
- For Visa and MasterCard: Record the printed four digits from the face of the Card (found above or below the embossed account number) on the Transaction Receipt. Refer to Chapter 4, *Unique Card Characteristics* for more information.
- For Discover Network: Record the printed three digits on the signature panel on the back of the Card on the Transaction Receipt. Refer to Chapter 4, *Unique Card Characteristics* for more information.
- Compare the first four digits of the Card account number on the printed Transaction Receipt with the first four digits of the embossed Card account number. If they do not match, decline the Transaction and attempt to recover the Card (reasonably, lawfully, and peacefully), while also noting a description of the Cardholder.

CONTACTLESS TRANSACTIONS

The Contactless Transaction requirements are as follows:

Participation. Company is responsible for:

1. Ensuring that all POS Devices that accept Contactless Cards for Transactions meet the applicable Credit Card Association specifications, are approved by Servicer and/or the applicable Credit Card Associations for use with Contactless Cards, and are configured to transmit the data elements required for Contactless Transactions.
2. Complying with all Payment Network Regulations applicable to Transactions conducted with Contactless Cards, including all operating requirements, technical guides and other requirements specified by the applicable Credit Card Associations in connection with the acceptance of Contactless Cards.

Registration. It is Company's responsibility to ensure that it is eligible and has been approved by Servicer to accept Contactless Cards, and that Company has been registered with the applicable Credit Card Associations to participate in their respective Contactless Card payment program(s).

Processing. Company is responsible for:

1. Providing any data in the Authorization request as required by the applicable Credit Card Associations.
2. Transmitting the full and unaltered contents of Track 1 or Track 2 data of the Card's Magnetic Stripe or Contactless payment chip in the Authorization request.
3. Ensuring that Transactions are not processed as Contactless Transactions if currency conversion is performed.
4. Submitting only a single Authorization per clearing Transaction.

Companies that are eligible for both a Credit Card Association's No Signature Requirement Program and to accept Contactless Cards may combine these programs to further enhance the benefits of accepting Contactless Cards and participating in a No Signature Required Program.

Chapter

3

Settling Daily Transactions

This Chapter describes how to settle your daily Transactions. The guidelines for Settlement within this Chapter can help you:

- Eliminate balancing errors
- Promptly record deposits to your DDA
- Prevent duplicate billing to customers
- Minimize Chargebacks

SETTLING THE DAILY BATCH

To settle the daily Batch, perform the following steps:

1. **Total the day's Transaction Receipts and Credit Transaction Receipts.**
2. **Verify that the Transaction Receipts equal the POS Device totals.** You may print a report from your POS Device to assist you with balancing. For more information about balancing, refer to the instructions that came with your POS Device.

   If the totals do not balance, then do the following:

   - Compare the Transaction Receipts to the individual entries in the POS Device.
   - Make any necessary adjustments before transmitting or closing the Batch. To make adjustments, refer to the instructions for your POS Device.
3. **Close the Batch according to the instructions for your POS Device.**

NOTE: *Submit your Transactions for processing daily to obtain the most favorable pricing.*

PAPER DEPOSITS

If you are not using a POS Device, you must deposit Discover Network, Visa and MasterCard Transaction Receipts or Credit Transaction Receipts within three (3) business days, except:

1. The Transaction Receipts or Credit Transaction Receipts must not be presented until after the products are shipped or the services are performed unless, at the time of the Transaction, the Cardholder agrees to a properly disclosed delayed delivery of the products or services.
2. When the Company receives Cardholder authorization for a delayed presentment (in which case the words "Delayed Delivery" must be noted on the Transaction Receipt or Credit Transaction Receipt).

3. When the Company is obligated by law to retain the Transaction Receipt or Credit Transaction Receipt or return it to a Customer upon timely cancellation, in which case the Company should present the record within ten (10) business days after the Transaction date.
4. When the Company has multiple locations and uses a central facility to accumulate and present records to Servicer, in which event the Company must present the record in accordance with applicable law and, in any event, within thirty (30) calendar days of the Transaction date.

Please include a Batch Header with your Transaction Receipts.

PREPARING PAPER DEPOSITS

To prepare a paper deposit, follow these steps:

1. Place your Company Identification Card and the Batch Header in the Imprinter.
2. Imprint the information onto the Batch Header.
3. Enter the total number and dollar amount of Transaction Receipts. It is not necessary to separate the Discover Network, Visa and MasterCard Transaction Receipts.
4. Enter the total number and dollar amount of Credit Transaction Receipts.
5. Review the Transaction Receipts and Credit Transaction Receipts to make sure they bear legible Discover Network, Visa or MasterCard numbers and amounts. Visa uses 16-digit account numbers beginning with a "4" and MasterCard uses 16-digit account numbers beginning with a "5." Discover Network uses 16-digit account numbers beginning with a "6."
6. Enter the net amount of the Transaction Receipts and the Credit Transaction Receipts.
7. Fill in the date and your DDA (Demand Deposit Account) number.
8. Place the bank copy of all Transaction Receipts and Credit Transaction Receipts behind the Batch Header and insert them into the Company deposit envelope, which is addressed to the paper processing center. If you need additional Company deposit envelopes, please contact merchant services.
9. Retain a copy of the Batch Header, along with your copies of the Transaction Receipts and Credit Transaction Receipts for your records.
10. Make sure the paper processing center address is on the front of the envelope.
11. Mail the Company deposit envelope.
12. Store paper drafts appropriately. For storage requirements for paper drafts in compliance with the PCI Data Security Standard, visit: **http://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.**

ADJUSTMENTS

If we detect an imbalance between your Batch Header and the attached Transaction Receipts, we make an adjustment to your DDA and send you an adjustment notice. Remember, adjustments differ from Chargebacks. If you have any questions concerning an adjustment, contact merchant services.

The most common reasons for adjustments include:

- The Transaction Receipts received do not match the amount shown on the Batch Header.
- A Card number is invalid or illegible. To receive credit, you must correct the number and resubmit the Transaction Receipt with a new Batch Header.
- Your DDA was credited in error or has been debited to reflect a Negative Deposit.

Remember to reconcile your monthly Company Statements with your DDA statement, along with any adjustment notices you may have received.

Chapter

4

Preventing Card Fraud

It is important to take steps to educate yourself and your staff to reduce your risk of accepting a counterfeit or fraudulent Card Transaction. Remember that you are responsible for all Chargebacks, including those for fraudulent Transactions. Fraudulent Card sales involve an invalid Card account number or, more commonly, a valid Card number presented by an unauthorized user. Fraud normally occurs within hours of the loss, theft, or compromise of a Card number or Card, and before most victims report the Card missing or discover the compromise.

If a Transaction is declined, do not request a Code 10 Authorization and do not complete the Transaction. However, if you receive an Approval Code but suspect a Card has been altered or is counterfeit, call the Voice Authorization Center and request a Code 10 Authorization (see Chapter 5, *Code 10 Procedures*).

The following sections provide tips to assist you in protecting yourself against fraud losses.

IDENTIFYING SUSPICIOUS CUSTOMER ACTIONS

Common sense is the best guide for spotting suspicious behavior. Be sure you combine watchfulness with proper Card identification and validation techniques.

Be aware of customers who:

- Make indiscriminate large dollar purchases without regard to size, color, style, or price
- Question the sales clerk about credit limits or the Authorization process
- Attempt to distract the sales clerk (e.g., continually delay selections, talk continuously)
- Hurry a clerk at quitting time
- Purchase a high-ticket item, such as a wide-screen HDTV monitor or other large item, and insist on taking it immediately, rather than having it delivered—even when delivery is included in the price
- Buy a high-ticket item and request that it be sent next day air or request for someone else to pick up the purchase at a later time
- Pull a Card from a pocket rather than a wallet
- Sign the Transaction Receipt in a deliberate or unnatural manner
- Appear too young to make purchases with a Card

- Buy clothing without trying it on for size or decline alterations that are included in the price
- Charge expensive items on a newly valid Card
- Do not have a driver's license, tell you that his or her driver's license is in the car, or provide only a temporary license without a photo
- Do not ask questions on major purchases
- Make purchases, leave the store, and return to make more purchases
- Make purchases just after the store opens or just before it closes
- Use a Card belonging to a friend or relative
- Ship purchases to an address outside of the U.S.
- Recite the Card number from memory rather than presenting the Card itself
- Ask to see the Card again before signing the Transaction Receipt

IDENTIFYING SUSPICIOUS CARD NOT PRESENT TRANSACTIONS

The increased use of Electronic Commerce, mail, and telephone orders has resulted in an increasing amount of fraud. If you accept Card Not Present Transactions, take caution if a customer attempts to:

- Request delivery to a freight forwarder
- Order goods and/or services via a free e-mail service
- Request that an order be rushed and wants a tracking number as soon as possible
- Purchase items that the company does not sell (the most common items are laptop computers and cellular phones)
- Use more than one Card for any given purchase (also known as a "Split Ticket")
- Use Cards that have sequential numbers or patterns
- Place an unusually large or uncommon order compared to your typical Transactions
- Use a Card issued by a foreign bank along with one of the other actions within this list
- Request delivery to a post office box
- Request delivery to a foreign country
- Utilize phone relay service where the Cardholder does not speak directly to the Company
- E-mail purchase orders that involve multiple Card accounts in which each order includes the same product and dollar amount. This is sometimes common for Transactions resulting in foreign Card fraud
- Place an order and then call back to place subsequent orders using the same or different Cards

You should be particularly careful if you sell products that are easily resold. For example, computers and computer equipment, printer cartridges, and jewelry are more susceptible to fraud than perishable items such as food—although criminals can victimize virtually any type of business.

NOTE: *If you receive an order for a large purchase for delivery to a foreign country or to a freight forwarder, we recommend that you contact your Voice Authorization Center to request a Code 10 specifically identifying the Transaction as a large foreign shipment Transaction.*

IDENTIFYING VALID CARDS

Cards share similar qualities to help identify their validity, and there are anti-fraud safeguards unique to each Card brand.

CARDS AND SIGNATURES

You should not accept a Card that is not signed. Many Card users write "Use other ID" (or something similar) in the signature panel because they believe it provides a higher level of security. This is not actually true, it simply allows a thief to sign his or her own name or use a fake ID with any signature.

If an unsigned Card is presented to you:

1. Inform the customer that the Card must be signed.
2. Have the customer sign the Card in your presence and provide a current, valid government ID that has been signed (such as a passport or driver's license). Do not accept a temporary form of ID, such as a temporary driver's license that does not have a photo.
3. Compare the signature on the ID to that on the Card.
4. If the customer refuses to sign the Card, do not complete the Transaction. Remember, you are liable for any Transaction processed with a fraudulent Card.

CARD PROCESSING TIPS

After you swipe a Card, the POS Device prompts you for specific information. The POS Device may also prompt you to enter the last four digits of the account number to verify that the embossed account number matches the number on the Magnetic Stripe (on the back of the Card). If the numbers do not match, the POS Device indicates a mismatch of the digits or an invalid Card. Do not accept the Card. Once you receive an Approval Code, verify that the Card number on the Transaction Receipt matches the number embossed on the Card. If it does not match, do not accept the Card.

CHARACTERISTICS OF MOST CARDS

These characteristics typically apply to most Card brands.

- **Overall Card Quality:** A Card may be any color (but is never faded or washed out) or feature a background pattern or photograph. The Card's edge should be smooth and clean, never rough. The print should be crisp and clear.
- **Matching Account and BIN Numbers:** An identical series of numbers (known as the Bank Identification Number [BIN]) is printed directly above or below the first four embossed numbers on the Card and in the signature panel.
- **Embossing Quality:** A hot iron is sometimes used to smooth embossed numbers and then emboss new numbers. When this is done, the numbers can appear irregular in spacing or in vertical alignment, or there can be a slight "halo" around the numbers. This technique is also used to modify the expiration date, so check both the month and the year for alterations. Refer to Chapter 4, *Examples of Tampering* for details.
- **Hologram Quality:** An authentic Hologram should reflect light and change in appearance as you move the Card. It should barely catch your fingernail, but should not be such that you can peel it off. A fake Hologram is often a sliver of tin foil that lacks the features of an authentic Hologram.
- **Card Account Number and Card Identification Number:** The signature panel on the back of the Card should include either the entire Card account number or its last four digits, followed by the Card Identification Number. These numbers should be printed in reverse italics and should match the embossed numbers.

- **Signature Panel Quality:** The signature panel should not be defaced (e.g., peeled-off white plastic, smudged imprinting, or "void" appearing in the signature panel). Refer to Chapter 4, *Examples of Tampering* for details.
- **Signature Panel Print Design:** With the exception of some ATM Cards and various store-branded Cards, signature panels are rarely plain white. They usually contain an overprint or watermark.

UNIQUE CARD CHARACTERISTICS

For the unique Card design elements specific to the Cards, please visit the following Card websites.

- MasterCard: http://www.mastercard.com/us/personal/en/aboutourcards/credit/index.html
- Visa: http://usa.visa.com/personal/cards/credit/index.html
- American Express: http://www201.americanexpress.com/getthecard/home
- Discover Network: http://www.discovercard.com

EXAMPLES OF TAMPERING

The following section identifies common Card tampering techniques. Although an American Express Card is used in the examples, these tampering methods are widespread among all Card types.

FRAUDULENT EMBOSSING

Characteristics of fraudulent Embossing include:

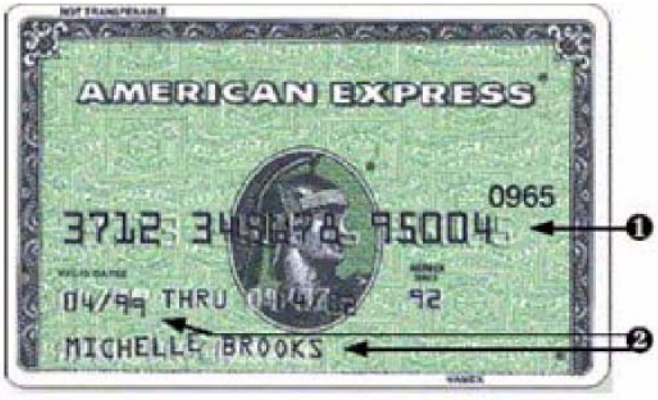

Figure 4-5. Example of Fraudulent Embossing

- The black ink on the Card number (1) or Cardholder name (2) is smudged or messy.
- The Embossed numbers are crooked, out of line, or unevenly spaced (2).
- The typeface of the Card account number does not match the rest of the Card typeface (2).
- The Card number embossed on the front does not match the number printed on the back (1).

ALTERED MAGNETIC STRIPE

Characteristics of altered Magnetic Stripes include:

- The Card number on the printed Transaction Receipt does not match the number embossed on the front of the Card or imprinted on the back.

- The name printed on the Transaction Receipt does not match the name embossed on the Card.
- The Magnetic Stripe is deliberately scratched or altered making it necessary to manually key the Card account number.
- The signature panel has been whited out, taped over or erased.

IDENTIFYING SUSPICIOUS EMPLOYEE ACTIONS

Be aware - not all Card fraud is committed by Customers. Sometimes employees engage in fraud using the following activities:

- **Record Card Numbers:** Employees may pocket receipts left behind by Cardholders or may write Card numbers on another piece of paper.
- **Use Card Skimmers:** Employees may use a Card skimmer (i.e., a battery-operated, hand-held electronic device) that reads a Card's Magnetic Stripe and records it to memory. Card numbers are then downloaded from the skimmer and used to make counterfeit Cards or make unauthorized purchases. Some Card companies offer a reward for information leading to the arrest and conviction of anyone involved in the manufacture or use of counterfeit Cards.
- **Process Credit Transactions to Personal Card Accounts:** Employees may issue credits to their own Card or to an accomplice's Card using the Company's POS Device. Often these credits do not have an offsetting prior sale.

NOTE: *Most POS Device products allow a Company to require a password in order to process a Credit Transaction.*

To help prevent employee-related fraud, do the following:

- Reconcile your work daily rather than monthly.
- Password protect your POS Device, if this feature is available.
- Disable the credit function on your POS Device.
- Secure your POS Device during non-business hours.

FACTORING

Factoring (also known as Laundering) occurs when you process another person's transactions through your Company account. Processing transactions which belong to another person or business is in violation of the Agreement and is prohibited by law in many states. Factoring may result in the termination of your Card acceptance privileges.

Be wary of the "fellow business person" who offers to pay you to process card transactions in return for a fee. These transactions are often questionable or fraudulent. These schemes typically result in a flood of Chargebacks which are debited from your DDA. By the time you realize this has occurred, the other business will most likely have relocated under a different name.

To protect you from these schemes and the devastating losses that ensue, educate yourself and your staff about this serious problem and immediately report Factoring propositions to us or to the U.S. Secret Service. Remember, you are responsible for all transactions processed using your MID, so make sure that all transactions processed through your account represent transactions between you and the Cardholder.

Company will not present for processing or credit, directly or indirectly, any Transaction not originated as a result of a transaction directly between Company and a Cardholder or any Transaction Company knows or should know to be fraudulent or not authorized by the Cardholder. Perpetrators of fraudulent Transactions will be referred to law enforcement officials. Company will not deposit any Transaction Receipt representing the refinancing of an existing obligation of a Cardholder.

Chapter

5

Code 10 Procedures

Code 10 is a term used by the Credit Card Associations to refer to suspicious or questionable Transactions, Cards, or Cardholders.

If you are suspicious of a Card Transaction, contact your Voice Authorization Center and request a Code 10 Authorization. Using the term "Code 10" allows you to call the Voice Authorization Center to question the Transaction without alerting the Cardholder. Follow the instructions given to you on how to proceed to minimize any discomfort between you and the Cardholder.

> **NOTE:** *Be alert to individuals who contact your business via phone or the Internet attempting to make large purchases for overseas shipment, direct or through a freight forwarder. These individuals may utilize one or more Cards in their "urgent" request. If you receive such a request, we encourage you to contact your Voice Authorization Center to request a Code 10, specifically identifying the Transaction as a large foreign shipment Transaction.*
>
> **NOTE:** *Fraudulent transactions, even when authorized, are subject to Chargebacks, and final payment is not guaranteed.*

CODE 10 AUTHORIZATION NUMBERS

To request a Code 10 Authorization for a Discover Network, Visa or MasterCard Transaction, call the telephone number on your Voice Authorization sticker (located on the POS Device). To request a Code 10 Authorization for American Express, call one of the following numbers:

- (800) 528-2121 (provides Approval Codes and verifies names and addresses)
- (800) 876-9786 (validates consumer information)

WHAT TO DO WITH AN UNAUTHORIZED CARD

If you are informed that a Card has been reported lost or stolen, or is otherwise invalid, do not complete the Transaction.

Card Recovery. If Company chooses to recover any Card, Company will use reasonable, peaceful means to recover any Card: (i) on Visa Cards, if the printed four digits below the embossed account number do not match the first four digits of the embossed account number; (ii) if Company is advised by Servicer (or its designee), the Issuer, or the designated voice authorization center to retain it; (iii) if Company has reasonable grounds to believe the Card is lost, stolen, counterfeit, fraudulent, or otherwise invalid, or its use is not authorized by the Cardholder; or (iv) for MasterCard Cards, if the printed four digits below the embossed account number do not match the first four digits of the embossed account number, or the Card does not have the "Twin Globes" hologram on the lower right corner of the Card face.

If you are instructed to retain the Card, follow these procedures:

- Maintain a record of the Card number in your files.
- Cut the Card through the account number lengthwise without damaging the Magnetic Stripe.
- Gather the following information:
  - Company's name, MID, telephone number, and address
  - Employee's name, telephone number, and address
  - Card account number
  - Reason for recovery
- Mail the information to:

  Exception Processing
  ATTN: Card Pick Up
  Elavon, Inc.
  7300 Chapman Highway
  Knoxville, TN 37920

NOTE: *Do not challenge the Card user. Avoid any physical confrontation with anyone who may be using a lost, stolen, or otherwise invalid Card. Do not jeopardize your safety or that of your employees or Customers.*

Once the person leaves your location, note in writing his or her physical characteristics and any other relevant identification information. Keep in mind that a reward may be offered by the Issuer for the recovery and return of a lost, stolen, or otherwise invalid Card.

Chapter

6

Retrieval Requests and Chargebacks

A Cardholder or Issuer may dispute a Transaction for any number of reasons, including a billing error, a quality dispute, or non-receipt of goods and/or services. This Chapter describes the process for handling disputed Transactions by explaining Retrieval Requests and Chargebacks.

Disputes With Cardholders. All disputes by any Cardholder relating to any Transaction will be settled between Company and the Cardholder. Servicer does not bear any responsibility for such Transactions or disputes, other than with respect to processing Chargebacks under the Payment Network Regulations.

Notification Of Retrieval Requests And Chargebacks

Company is fully responsible for all Retrieval Requests and Chargebacks under the Payment Network Regulations. Upon receipt of a Retrieval Request or Chargeback from a Payment Network, Servicer will forward such request or documentation to Company. Company is responsible for responding, as appropriate, to each Retrieval Request or Chargeback, including providing a copy of the relevant Transaction Receipt to Servicer. In addition, Company will cooperate with Servicer in complying with the Credit Card Rules and Debit Card Rules regarding Retrieval Requests and Chargebacks. The following is a non-exhaustive list of reasons for which Company may incur a Chargeback. It is not a complete list of Chargeback reasons and is intended only to provide the most commonly encountered situations where a Chargeback may occur:

- Failure to respond to a Retrieval Request or failure to provide a legible, complete, or proper copy of a Transaction Receipt in response to a Retrieval Request
- Unauthorized use of a Card as alleged by the Cardholder
- Dispute by the Cardholder over the quality of goods or services
- Failure by Company to provide goods or services
- The Transaction Receipt does not bear the Cardholder's signature
- The Transaction Receipt represents a Transaction for which Authorization was initially declined and was subsequently obtained by means of multiple Authorization attempts or other means not permitted hereunder
- The Transaction Receipt fails to comply with the terms and conditions of the Agreement or fails to comply with the Card Rules
- The Transaction evidenced by a Transaction Receipt or any other credit extended in respect thereof includes a cash disbursement made by the Company

- The Transaction evidenced by a Transaction Receipt or any other credit extended in respect thereof is for any reason illegal, null or void
- The Transaction Receipt refers to a Card which has expired or which Servicer has notified Company not to honor
- Copies of the Transaction Receipt have been deposited by Company more than once or Servicer has credited the account more than once with the same Transaction Receipt
- The Company has processed a Transaction for goods sold or services performed (or alleged to have been sold or performed) by parties other than Company
- An Electronic Commerce Transaction is or is claimed by the Cardholder to be unauthorized except where the Company provides Servicer with the appropriate Cardholder authentication verification value which matches that passed to Company by the Issuer for such Electronic Commerce Transaction
- You may elect to receive Retrieval Requests and Chargeback notices by U.S. mail, Autofax or online. To update or change the way you receive a Retrieval Request or Chargeback notification, contact merchant services or the Chargeback department at the toll-free telephone number listed on your notice

RETRIEVAL REQUESTS

A Retrieval Request is made by the Issuer on behalf of the Cardholder for a copy of the Transaction Receipt. A Retrieval Request (also known as a Copy Request) most often occurs when a Cardholder:

- Loses his or her copy of the Transaction Receipt;
- Does not remember the Transaction; or
- Questions the Transaction for any reason.

The Retrieval Request notice you receive will include the following information to help you identify the Transaction:

- **Card number.** Retrieval Request notices do NOT include the Cardholder's name, because this information is not provided by the Issuer.
- **Dollar amount.** For Transactions charged on foreign Cards, the dollar amount may vary because of currency exchange rates.
- **Transaction Date.** The Transaction Date listed on the Retrieval Request may differ a few days from the date of the actual Transaction. If you cannot locate a specific Transaction Receipt in your records for the date specified on the Retrieval Request notice, search your records for three days before and three days after the Transaction Date listed.

When you receive a Retrieval Request notice, you are required to provide us with a copy of the applicable Transaction Receipt so we can send it to the Issuer on your behalf. The Transaction Receipt copy must be clear and legible, signed by the Cardholder, and provided within the time frame specified in the notice.

We suggest you maintain Transaction Receipts in chronological order so that you can retrieve them quickly and easily when needed. Records may be stored off site, provided they are secure and readily accessible to the appropriate personnel. Remember, all records must be retained for a minimum of two (2) years.

Your response to a Retrieval Request may be sent by U.S. mail, Autofax or online, as outlined in the Retrieval Request notice. Due to possible delays using U.S. mail, we recommend that you submit your response via Autofax, online or send it via overnight mail. If you elect to send your response via U.S. mail, make sure you allow sufficient time to meet the deadline.

If we do not receive your response to the Retrieval Request by the deadline given, a Chargeback will be issued and your DDA will be debited for the amount of the Transaction. This type of Chargeback cannot be reversed. To avoid such Chargebacks, you should make it a priority to respond to Retrieval Request notices as soon as you receive them.

CHARGEBACKS

A Chargeback is a Transaction disputed by the Cardholder or an Issuer. If you receive a Chargeback, we debit your DDA for the amount of the Transaction, including any applicable currency fluctuations, and send you a Chargeback notice. This notice includes the details of the Transaction as well as specific instructions on how to respond.

There are several situations in which Chargebacks may occur. The most common Cardholder-initiated disputes include:

- Dissatisfaction with the quality of merchandise or services received
- Failure to receive merchandise or services
- A questionable Transaction
- A processing error by Company staff
- Unauthorized use of a Card

While it may not be possible to eliminate Chargebacks entirely, you can reduce their occurrence by resolving issues and disputes directly with the Cardholder and by following the proper Authorization and processing procedures. Because Chargebacks can be costly to the Company, you should make every effort to prevent them. Generally, you should remember to:

- Avoid duplicate processing of a Transaction.
- Work with the Cardholder to resolve disputes regarding the quality of merchandise or services rendered.
- Refuse to process a Transaction when you receive a Declined Code during Authorization.
- Call for Voice Authorization, if needed.
- Call for a Code 10 Authorization if you are still suspicious of the Cardholder, Card, or Transaction after receiving an Approval Code.
- Follow the procedures for processing Transactions as outlined in Chapter 3, *Settling Daily Transactions.*
- Include a description of the goods or services on the Transaction Receipt.
- Deliver merchandise or services before charging the Card.
- Obtain an Authorization Code.
- Include the CVV2/CVC2/CID and AVS codes for Card Not Present Transactions, if applicable.
- Submit Transaction Receipts on the same day Transactions are authorized.
- Make sure an Imprint appears on a manual Transaction Receipt or that the relevant Transaction information appears on the POS Device-generated Transaction Receipt (see Chapter 2, *Transaction Receipts* for more details).
- Never accept expired Cards or Cards having effective dates prior to the date of the Transaction.
- Make sure the signature on the Transaction Receipt matches the signature on the back of the Card.
- Obtain a signature from the Cardholder when merchandise is delivered.
- Be cautious of shipments to an address other than the Cardholder’s billing address.

HOW TO RESPOND TO A CHARGEBACK

A Company's written reply to a Chargeback is known as a Chargeback rebuttal.

You must submit your rebuttal to us in a timely manner so we can present it to the Issuer. If you submit a valid rebuttal, we issue a provisional credit in the amount of the Transaction to your DDA. The Issuer will then review your rebuttal to determine if the Chargeback is remedied. If the Issuer determines that the Chargeback is not remedied, they will initiate a second Chargeback and we debit your DDA a second time.

You must submit a legible and valid rebuttal within the time frame specified in the Chargeback notice. Failure to do so will delay credit to your DDA and may result in a waiver of your right to rebut the Chargeback.

For more information on rebuttal procedures, contact the Chargeback department using the toll free number provided in the Chargeback Notice.

CHARGEBACKS THAT CANNOT BE REVERSED

There are specific instances when a Chargeback cannot be reversed. In these cases, you are responsible to us for the Transaction amount regardless of the Authorization Code you received. These situations include:

- When the Card is present but it is not swiped or manually Imprinted;
- When the Card is present but you did not have the Cardholder sign the Transaction Receipt; and/or
- When the signature on the Transaction Receipt does not match the signature of the Cardholder on the back of the Card.

EXCESSIVE ACTIVITY

Company's presentation to Servicer of Excessive Activity will be a breach of the Agreement and cause for termination of the Agreement if the Excessive Activity thresholds outlined in this section are met for Company's accounts as a whole. Alternatively, in Servicer's sole reasonable discretion, if Excessive Activity occurs for any one or more POS Device identification number(s) or MID(s), only the account(s) that meet the Excessive Activity threshold may be terminated. "Excessive Activity" means, during any monthly period, Chargebacks and/or Retrieval Requests in excess of one percent (1%) of the gross dollar amount of Company's Transactions or returns in excess of two and one-half percent (2.5%) of the gross dollar amount of Transactions. Company authorizes, upon the occurrence of Excessive Activity, Servicer to take additional actions as either of them may deem necessary including, without limitation, suspension of processing privileges or creation or maintenance of a Reserve Account in accordance with the Agreement.

Chapter

7

International Transactions

DYNAMIC CURRENCY CONVERSION TRANSACTIONS

Dynamic Currency Conversion (DCC) is a service that allows a Company to offer international Cardholders the option to pay in their home currency rather than U.S. Dollars at the point-of-sale. The following describes how to process Dynamic Currency Conversion Transactions for the designated Cards. These guidelines can help you:

- Understand your responsibilities for DCC Transactions
- Handle mail order and telephone order DCC Transactions
- Process Electronic Commerce DCC Transactions
- Accept Priority Check-Out and Express Return Transactions (in limited Travel and Entertainment (T&E) situations) as DCC Transactions

YOUR RESPONSIBILITIES AND RESTRICTIONS

You must register with the Payment Networks through us prior to offering DCC service to Cardholders. You have sole responsibility to comply with Laws and Payment Network Regulations governing DCC Transactions, including all of the following:

- You must inform the Cardholder that the DCC Transaction is optional and that the Cardholder must actively choose to have the Transaction processed in his or her home currency. The Cardholder must expressly agree to the DCC Transaction and check the "accept" box on the Transaction Receipt.
- If the Cardholder does not actively choose to have the Transaction processed in his or her home currency, you must not complete the DCC Transaction, but may complete the Transaction in your local currency. Depending on your POS Device, you may be required to reverse or void the DCC Transaction when the Cardholder does not actively choose to have the Transaction processed in his or her home currency. Please refer to your Quick Guide Reference or Point-of-Sale Operating Guide for complete instructions. If a void or reversal is necessary, you can complete the Transaction in Company's local currency.
- You are prohibited from converting a Transaction in your local currency into an amount in a Cardholder's home currency after the Transaction has been completed with the Cardholder but not yet entered into Interchange.
- Failure to follow the Payment Network Regulations may result in a Chargeback of the Transaction. If the Transaction is processed in a currency different from the currency listed on the Transaction Receipt, a Chargeback may be issued for the full amount of the Transaction. There is no right of re-presentment or rebuttal of the Chargeback.

- If a Cardholder states in writing that he or she was not offered a choice during the DCC Transaction process or did not know that a DCC Transaction would occur, a Chargeback may be issued for the full amount of the Transaction. Re-presentments may be requested using your local currency but may not include DCC Transaction commissions, fees, or mark-ups.
- Credit Card Associations have the right to terminate their provision of the DCC services to Company. Failure to comply with the DCC requirements may result in fines, penalties, and/or termination of the DCC services.
- The Agreement may be terminated for your failure to comply with the DCC requirements.

DCC Written Disclosure Requirements

You must comply with the following DCC Cardholder written disclosure requirements in all acceptance environments, with the exception of telephone order (TO) Transactions.

- Currency symbol of the Company's local currency.
- Transaction amount of the goods or services purchased in the Company's local currency.
- Exchange rate used to determine the Transaction amount in the Cardholder's home currency.
- Any currency conversion commission, fees, or mark-up on the exchange rate over a wholesale rate or government mandated rate.
- Currency symbol of the proposed Transaction currency.
- Total Transaction amount charged by the Company in the proposed Transaction currency.

For TO Transactions, you must verbally notify the Cardholder of all the disclosure requirements listed above before initiating a DCC Transaction.

DCC Transaction Receipt Requirements

In addition to the appropriate electronic or manual Transaction Receipt requirements, DCC Transaction Receipts must also include:

- The price of the goods or services in the Company's local currency, accompanied by the Company's local currency symbol next to the amount.
- The total price in the Transaction currency, the Transaction currency symbol, and the words "Transaction Currency."
- The exchange rate used to convert the total price from the Company's local currency to the Transaction currency.
- The currency conversion commission, fees, or mark-up on the exchange rate over a wholesale rate or government mandated rate.
- A statement in an area easily seen by the Cardholder stating that the Cardholder was offered the option to pay in the Company's local currency.
- Cardholder expressly agrees to the Transaction Receipt information by marking an "accept" box on the Transaction Receipt.
- An indication that DCC is conducted by the Company.

MAIL ORDER (MO) TRANSACTIONS

Prior to initiating an MO DCC Transaction, you must ensure that the following information is included on the MO form:

- Specific Transaction currency agreed to by the Cardholder and Company.
- A statement that the exchange rate that will be used to convert the Transaction amount from the Company's local currency to the Cardholder's home currency will be determined at a later time without additional consultation with the Cardholder.
- Currency conversion commission, fees, or mark-up on the exchange rate over a wholesale rate or government mandated rate.
- That the Cardholder has a choice of payment currencies, including the Company's local currency.
- An "accept" box that Cardholder may mark to indicate acceptance of the DCC Transaction.

ELECTRONIC COMMERCE TRANSACTIONS

Prior to initiating an Electronic-Commerce (EC) DCC Transaction, you must inform the Cardholder of all of the DCC Written Disclosure Requirements listed above. You must provide this information with an "accept" or other affirmative button that requires Cardholder agreement to proceed.

PRIORITY CHECK-OUT AND EXPRESS RETURN TRANSACTIONS (LIMITED T&E SITUATIONS)

Prior to initiating a T&E DCC Transaction, you must inform the Cardholder of all of the following information:

- The specific currency in which the DCC Transaction will take place.
- That the Cardholder has a choice of payment currencies, including the Company's local currency.
- The Cardholder understands that a DCC Transaction will take place.
- That the exchange rate is determined at a later time without further Cardholder consultation.
- Currency conversion commissions, fees, or mark-up on the exchange rate over a wholesale rate or government mandated rate.

This information must be documented in a written agreement that is signed by the Cardholder before checkout or rental return that authorizes Company to deposit a Transaction Receipt without the Cardholder's signature for the total amount of their obligation. Further, the Cardholder must expressly agree to DCC by marking the "accept" box on the written agreement.

The Company must send the Cardholder a copy of the Transaction Receipt through the postal service (or by email if selected by the Cardholder) within three (3) business days of completing the Transaction.

MULTI-CURRENCY PRICING

Multi-Currency Pricing (MCP) is a service that allows a Company to display the price of goods or services in a currency other than, or in addition to, your local currency. You have sole responsibility to comply with Laws and Payment Network Regulations governing MCP, including all of the following:

- The displayed price and currency selected by the Cardholder must be the same price and currency charged to the Cardholder, printed on the Transaction Receipt and entered into Interchange by Servicer.
- At least one of the currencies of the prices displayed cannot be Company's local currency.
- The Cardholder makes a purchase decision based on the price and currency displayed by Company.
- The Transaction must be completed with the price and currency selected by the Cardholder, with no currency conversion performed by Company.

In addition to the appropriate electronic or manual Transaction Receipt requirements, it is important that the Transaction Receipt clearly shows the Transaction currency and the corresponding currency symbol or code. The currency code is the three digit ISO alpha country code. For Transaction Receipts without a currency symbol or code, the receipt will be assumed to be in Company's local currency, which may give rise to rights of Chargeback.

Chapter

8

Vehicle Rental or Leasing Authorization Procedures

In addition to the Authorization procedures set out in this document, Companies that provide vehicle rental will follow the procedures set out in this Chapter.

PREPARATION OF TRANSACTION RECEIPTS

EXECUTION

You must prepare Transaction Receipts for all Transactions as described in Chapter 2, *Transaction Receipts*. The Cardholder must sign the Transaction Receipt. However, the Cardholder must not be required to sign until the total Transaction amount is known and indicated on the Transaction Receipt.

MULTIPLE CARD TRANSACTION SALES

The Company will include all items of goods and services purchased or leased in a single Transaction in the total amount of a single Transaction Receipt except:

- When the balance of the amount due is paid by the Cardholder at the time of sale in cash or by check or both
- When the Company is providing vehicle rental or leasing and the Transaction involves an additional ancillary charge or a calculation error for which a separate Transaction Receipt is completed and deposited

If Company is engaged in vehicle rental or leasing, Company may obtain Authorization for such Transactions based upon estimates of the Transactions according to the following procedures:

1. The Company estimates the amount of the Transaction based on the Cardholder's intended rental period at the time of rental, the rental rate, tax and mileage rates and ancillary charges. The estimate may not include an extra amount for possible car damage, or for the insurance deductible amount if the Cardholder has waived insurance coverage at the time of rental.

2. If the Company later estimates that the Transaction amount will exceed the initial estimated Transaction amount, the Company may obtain additional authorizations for additional amounts (not cumulative of previous amounts) at any time before the rental return date. The Company must disclose to the Cardholder the authorized amount for the estimated car rental or leasing Transaction on the rental date. A final or additional authorization is not necessary if the actual Transaction amount does not exceed 115% of the sum of the authorized amounts.

3. If the Company alters a Transaction Receipt or prepares an additional Transaction Receipt to add delayed or add-on charges previously specifically consented to by the Cardholder, the Company must deliver an explanation of the change to the Cardholder (i.e., mail a copy of the amended or additional Transaction Receipt to the Cardholder), and the Company must fully comply with the requirements in Chapter 8, *Vehicle Rental Or Leasing Ancillary Charges*.

4. Regardless of the terms and conditions of any written pre-Authorization form, the Transaction Receipt amount for a vehicle rental or lease Transaction cannot include any consequential charges. The Company may pursue consequential charges set forth in its terms and conditions by means other than Card Transaction.

VEHICLE RENTAL OR LEASING ANCILLARY CHARGES

If the Company discovers additional ancillary charges or an error in calculation after the rental car is returned, the Company may bill the Cardholder provided that the signed rental contract allows for additional charges and final audit.

The Company may not recover charges related to car damage, theft or loss. Valid charges may include:

- Taxes
- Mileage charges
- Fuel
- Insurance
- Rental fees
- Parking tickets and other traffic violations

For parking tickets and traffic violations:

- The incident must have occurred while the Cardholder was in possession of the vehicle,
- The Company must support the charge with documentation from the appropriate civil authority, including the license number of the rental vehicle, date, time and location of the violation, statute violated, and amount of the penalty.

These charges must be processed on a delayed or amended Transaction Receipt within 90 calendar days of the rental return or base end date. A copy of this Transaction Receipt must be mailed to the Cardholder's address as indicated in the rental contract or folio. This Transaction Receipt does not require the Cardholder's signature if the Company:

- Has the signature on file, and
- Includes "Signature on File" on the signature line.

Chapter

9

Lodging Accommodations Authorization Procedures

In addition to the Authorization procedures set out in this document, Companies that provide lodging accommodations in the hotel and hospitality industry will follow the procedures set out in this Chapter.

PREPARATION OF TRANSACTION RECEIPTS

EXECUTION

You must prepare Transaction Receipts for all transactions as described in Chapter 2, *Transaction Receipts*. The Cardholder must sign the Transaction Receipt. However, the Cardholder must not be required to sign until the total Transaction amount is known and indicated on the Transaction Receipt.

MULTIPLE CARD TRANSACTION SALES

The Company must include all goods and services purchased or leased in a single Transaction in the total amount of a single Card Transaction except:

- When the balance of the amount due is paid by the Cardholder at the time of sale in cash, check or both,
- When the Company is providing lodging accommodations and the Transaction involves (1) Advance Deposit Services or (2) an additional ancillary charge for which a separate Transaction Receipt is completed and deposited.

The Company may obtain authorizations for Card Transactions involving the provision of lodging accommodations based upon estimates of the transactions according to the following procedures:

1. The Company must estimate the amount of the Transaction based on the Cardholder's intended length of stay at check-in time, the room rate, applicable tax and/or service charge and any Company-specific methods for estimating additional ancillary charges. Company must request Authorization for the estimated amount of the Transaction.

Companies approved for participation in the Visa/MasterCard Prestigious Hotel Authorization Service are exempt from this requirement if estimates to do not exceed the service's established floor limits. In this event, the Company must obtain a Status Check Authorization of $1.00 (one dollar).

2. If the Company later estimates that the Transaction amount will exceed the floor limit (in cases where no Authorization was required) or will exceed the amount previously authorized (in all other cases), based on the Cardholder's actual charges, the Company must request Authorization for the increase in the estimated Transaction amount. If necessary, the Company may obtain and record additional Authorizations for additional amounts (not cumulative of previous amounts) at any time before the check-out date.

   A final or additional Authorization is not necessary if the actual Transaction amount does not exceed:

   - The applicable floor limit or
   - 115% of the sum of the authorized amounts.

3. The Company must record on the Transaction Receipt the Authorization amount(s), Authorization date(s), and Authorization code(s) for all authorizations obtained. If Authorization is declined, the Company must follow its normal procedures for a declined Authorization.
4. If the Company alters a Transaction Receipt or prepares an additional Transaction Receipt to add delayed or add-on charges previously specifically consented to by the Cardholder, the Company must deliver an explanation of the change to the Cardholder (i.e., mail a copy of the amended or additional Transaction Receipt to the Cardholder), and the Company must fully comply with the requirements in Chapter 9, *Lodging Accommodations Ancillary Charges*.
5. The Company understands that its right to use special Authorization procedures under this section may be terminated at any time if Servicer, Discover Network, Visa, or MasterCard determines in its sole discretion that Company has been abusing its privileges under or not complying with prescribed procedures.

LODGING ACCOMMODATIONS ANCILLARY CHARGES

If the Company discovers additional ancillary charges after the Cardholder has checked out, the Company may bill the Cardholder provided that the Cardholder agreed to be liable for such charges.

Valid charges may include room, food, beverage and tax charges. The Company may not recover charges related to theft, damage, or loss except as set out below for MasterCard Transactions.

All delayed or amended charges must be processed on a separate or amended Transaction Receipt within 90 calendar days of the check-out date. A copy of this Transaction Receipt must be mailed to the Cardholder's address as indicated on the itemized hotel bill. This Transaction Receipt does not require the Cardholder's signature if the Company:

- Has the signature on file,
- Includes "Signature on File" on the signature line.

MASTERCARD TRANSACTIONS FOR ANCILLARY CHARGES

For MasterCard Transactions, charges for loss, theft, or damages must be processed as a separate transaction from the underlying rental, lodging, or similar transaction. The Cardholder must authorize the charge after being informed of the loss, theft, or damage. To obtain the Cardholder Authorization for damages, the Company must prepare a Transaction Receipt with proof of Card presence, provide the estimated amount for repairs (indicating that the amount will be adjusted accordingly pursuant to completion of the repairs and submission of the invoice for said repairs), and obtain the Cardholder's signature. The final transaction amount may not exceed the Company's estimated amount by more than one hundred fifteen percent (115%) (or less, as directed by local ordinances). The Company must submit a credit if the final cost of repairs is less than the estimated amount on the Transaction Receipt. The Company has thirty (30) days from the date of the subsequent transaction related to damages to submit the item into clearing.

LODGING RESERVATION SERVICE

In order to be eligible to accept Discover Network, Visa and/or MasterCard Cards to guarantee reservations for lodging accommodations, the Company will satisfy the following requirements and procedures:

1. Reservation Procedures

a. The Company will accept all Discover Network, MasterCard or Visa Cards without discrimination for all Cardholders requesting reservations under the applicable Card Rules.

b. The Company must obtain the Cardholder's name, account number, and expiration date embossed or printed on the Card, and will also inform the Cardholder that a Card Authorization check is made at the time of the Cardholder's arrival.

c. The Company will inform the Cardholder that the accommodations are held until check-out time on the day following the scheduled arrival date unless canceled by 6:00 p.m. establishment time (defined as the time zone in which the physical premises of the Company are located) on the scheduled arrival date. The Company must not require more than 72 hours cancellation notification prior to the scheduled arrival date or as otherwise permitted under the applicable Card Rules.

d. The Company will advise the Cardholder that if he or she has not checked in (registered) by check-out time the following day after his or her scheduled arrival date and the reservation was not properly canceled, the Cardholder is billed for one night's lodging plus applicable tax.

e. The Company will quote the rate of the reserved accommodations, the exact physical address of the reserved accommodations, including name, address, city, state and country and provide the Cardholder a reservation confirmation code, advising that it be retained.

f. The Company will verbally confirm and, if requested, provide a written confirmation to the Cardholder of the reservation including the Cardholder name provided by the Cardholder, account number and Card expiration date embossed or printed on the Card, the reservation confirmation code, name and exact physical address of the reserved accommodations, the provisions of the applicable Card Rules relating to the Cardholder's obligation, including cancellation procedures and any other details related to the accommodations reserved, and the rate of the accommodations.

2. Cancellation Procedures

a. The Company will accept all cancellation requests from Cardholders, provided the cancellation request is made prior to the specified cancellation time.

b. The Company will provide the Cardholder with a cancellation code and advise the Cardholder that it must be retained to preserve his or her rights in case of dispute. If requested, the Company will provide (by mail) the Cardholder written confirmation of the cancellation including the Cardholder account number, expiration date and name embossed on the Card, the cancellation code, and the details related to the accommodations canceled, including the name of the Company's employee that processed the cancellation.

3. Scheduled Arrival Date Procedures (Unclaimed Accommodations)

a. If accommodations reserved under the applicable Card Rules, have not been claimed or canceled prior to the specified cancellation time (a "**No Show**"), the Company must hold the room(s) available according to the reservation until check-out time the following day.

b. If the Cardholder does not cancel the reservation or does not check-in within the prescribed time, the Company will deposit a Transaction Receipt for one (1) night's lodging plus applicable tax indicating the amount of one (1) night's lodging plus applicable tax, the Cardholder account

number, expiration date and name embossed or printed on the Card, and the words "No Show" on the Cardholder signature line.

c. The Company will obtain an Authorization Code for the No Show Transaction.

4. Alternate Accommodations

If accommodations which were guaranteed pursuant to the Card Rules, are unavailable, the Company will provide the Cardholder with the following services at no charge:

a. The Company will provide the Cardholder with comparable accommodations for one (1) night at another establishment.

b. The Company will provide transportation for the Cardholder to the location of the alternative establishment.

c. If requested, the Company will provide the Cardholder with a three (3) minute telephone call.

d. If requested, the Company will forward all messages and calls for the Cardholder to the location of the alternative establishment.

ADVANCE LODGING DEPOSIT SERVICE

In order to participate in the Advance Lodging Deposit service under which a Cardholder uses his or her Card for payment of an advance deposit required by the Company to reserve lodging accommodations ("**Advance Lodging Deposit**"), the Company will adhere to the following procedures and requirements set forth below:

1. Reservation Procedures

a. The Company will accept all Cards for an advance deposit when the Advance Lodging Deposit service is agreed to by the Cardholder.

b. The Company must hold a valid Advance Lodging Deposit service contract with us, either as part of the Agreement or as a separate contract.

c. The Company will determine the amount of an Advance Lodging Deposit Transaction by the intended length of stay, which amount must not exceed the cost of seven (7) nights of lodging. The amount of the Advance Lodging Deposit Transaction must be applied to the total obligation.

d. The Company will inform the Cardholder in writing (i) of the Company's advance deposit requirements, (ii) of the reserved accommodation and the Transaction amount, (iii) of the exact Company name and location, (iv) of the Company's cancellation policy requirements, and (v) that the accommodations are held for the number of nights used to determine the amount of the Advance Lodging Deposit Transaction.

e. The Company will obtain the Card account number, Card expiration date, the name embossed or printed on the Card, telephone number, mailing address, scheduled date of arrival, and intended length of stay.

f. The Company will inform the Cardholder (i) that the Company will hold the accommodations according to the reservation, and (ii) that if changes in reservation are requested, written confirmation of such changes is provided at the Cardholder's request.

g. The Company will advise the Cardholder that if (i) he or she has not checked in by check-out time the day following the last night of lodging used to determine the amount of the Advance Lodging Deposit Transaction, or (ii) the reservation was not canceled by the time and date specified by the Company, the Cardholder will forfeit the entire amount of the Advance Lodging Deposit Transaction or a portion of that amount. The Company will not, under any circumstances, present any additional No Show Transaction in connection with a Transaction made under the Advance Lodging Deposit service.

h. The Company will quote the rate of the reserved accommodation, the amount of the Advance Lodging Deposit Transaction and the exact location of the reserved accommodations. The Company will provide the Cardholder with a confirmation code (advising that it must be retained) and with the actual date and time the cancellation privileges expire.

i. The Company will complete a Transaction Receipt for the amount of the advance deposit, indicating the Cardholder account number, Card expiration date, the name embossed on the Card, telephone number, mailing address, and the words "Advance Deposit" on the signature line. The Cardholder's confirmation code, scheduled arrival date, and the last day and time the cancellation privileges expire without forfeiture of the deposit if the accommodations are not used must also be indicated on the Transaction Receipt.

j. The Company will follow normal Authorization procedures for lodging Transactions. If the Authorization request results in a decline, the Company will so advise the Cardholder and will not deposit the Transaction Receipt.

k. The Company will mail the Cardholder's copy of the Transaction Receipt and the Company's written cancellation policy to the address indicated by the Cardholder within three (3) business days from the date of the Transaction Receipt.

l. The Company will deposit the Transaction Receipt in accordance with usual procedures as specified in this guide and the requirements for normal deposit for lodging Companies as specified in the Card Rules.

2. Cancellation Procedures

The Company will adhere to the following procedures when the Cardholder cancels the reservation on a timely basis:

a. The Company will accept all cancellation requests from Cardholders, provided the cancellation request is made prior to the specified cancellation date and time.

b. The Company will provide a cancellation code and advise the Cardholder that it must be retained to preserve his or her rights in the case of dispute.

c. The Company will complete a Credit Transaction Receipt including the entire amount of the Advance Lodging Deposit Transaction, the Cardholder account number, Card expiration date, the name embossed or printed on the Card, mailing address, the cancellation code, and the words "Advance Deposit Cancellation" on the signature line.

d. The Company will (1) deposit the Credit Transaction Receipt within three (3) calendar days of the Transaction Date, and (2) mail the Cardholder's copy of the credit voucher to the address indicated by the Cardholder within three (3) business days from the date of the issuance of the Transaction Receipt.

3. Alternate Accommodations

a. If accommodations which were reserved under the Advance Lodging Deposit Service are unavailable, the Company will complete and deliver to the Cardholder a Credit Transaction Receipt to refund the entire amount of the Advance Lodging Deposit Transaction.

b. The Company will provide the following services at no charge to the Cardholder:

i At least comparable accommodations at an alternative establishment (a) for the number of nights used to determine the amount of the Advance Lodging Deposit Transaction, not to exceed seven (7) nights, or (b) until the reserved accommodations are made available at the original establishment, whichever occurs first.

ii Transportation to the location of the alternative establishment and return transportation to the original establishment. If requested, transportation to and from the alternate establishment must be provided on a daily basis.

iii If requested, provide the Cardholder two three (3) minute telephone calls.

iv If requested, forward all messages and calls for the Cardholder to the location of the alternate establishment.

4. Central Reservation Services

In the event that Company is a "Central Reservation Service" (defined as an entity holding operating agreements with various geographically contiguous lodging establishments to act as a reservations resource for such establishments), Company further agrees and warrants as follows:

a. Company will have a written contract with each such lodging establishment, which will be duly executed by an officer or manager of the lodging establishment, setting out the respective rights and duties of Company and such lodging establishment; and

b. Company will be registered with the Credit Card Associations as a Central Reservation Service; will not use an agent to perform such services; will follow the procedures for reservations, cancellations, alternate accommodations and Chargebacks herein set out; and will accept full responsibility for resolving any Cardholder problems related to the Advance Lodging Deposit Service.

PRIORITY/EXPRESS CHECK-OUT SERVICES

In order to participate in a service under which a Cardholder authorizes the use of his or her Card for payment of his or her total obligation to the Company, with or without prior knowledge of the total amount ("**Priority/Express Check-out**"), the Company will follow the following procedures and requirements (also see Chapter 7, *Priority Check-Out and Express Return Transactions (Limited T&E Situations)*):

CHECK OUT PROCEDURES

1. Company will accept all Discover Network, Visa and MasterCard Cards when a Cardholder requests Priority Check-out service.

2. Company must hold a valid Priority/Express Check-out service contract with Servicer.

3. Company must provide the Cardholder with a Priority/Express Check-out agreement which must contain, at a minimum, the following information:

a. Cardholder account number

b. Cardholder's name and address

c. Expiration date of the Card

d. Company's name, address and telephone number

e. Check-in date and departure date of the Cardholder

f. Roommate and room number of the Cardholder

g. A statement authorizing the Company to charge the designated Cardholder Account number for the amount of the bill and to present the Transaction Receipt without the Cardholder's signature

h. Space for Cardholder's signature

i. Transaction date

j. Identification of the Transaction currency

k. Transaction amount indicated in the Transaction currency

l. A legend identifying the Cardholder's request for specific billing receipts, including the name and address to whom the receipts are to be mailed

4. The Company will inform the Cardholder that the Priority/Express Check-out agreement must be completed, signed and returned, and that the Cardholder's mailing address must be included to receive a copy of the hotel bill supporting the final Transaction amount.

5. The Company will obtain the completed Priority/Express Check-out agreement and ensure that the Cardholder account number identified in such agreement is identical to the account number imprinted on the Transaction Receipt.
6. The Company will follow the Authorization procedures for lodging transactions as set forth in this guide.
7. When the Cardholder has checked out, Company will complete the Transaction Receipt, indicating the total amount of the Cardholder's obligation and the words "Signature on File - Priority/Express Check-out" on the signature line.
8. Upon the Cardholder's departure, the Company will mail the Cardholder's copy of the Transaction Receipt, the itemized hotel bill, and, if requested, the signed Priority/Express Check-out agreement to the address provided by the Cardholder on the Priority/Express Check-out Agreement within three (3) business days of the Cardholder's departure.
9. Company must retain the itemized bill and signed Priority/Express Check-out agreement for a minimum of six (6) months after the Transaction Date.

Chapter

10

Convenience Fee and Government/ Public Institution Service Fee Requirements

This Chapter describes the requirements applicable to the assessment of Convenience Fees by registered Companies and Government/Public Institution Service Fees available to government and public institution Companies operating in certain designated Merchant Category Codes in compliance with the Payment Network Regulations. In addition to the requirements in the Agreement and other applicable procedures included elsewhere in the Operating Guide, Companies that elect to assess Convenience Fees or Government/Public Institution Service Fees will adhere to the requirements in this Chapter.

CONVENIENCE FEES

1. **Company-Managed.** If Company is eligible to charge Convenience Fees and has elected to manage Convenience Fees (with or without use of a Service Provider), then Company will comply with the following provisions:

   ASSESSMENT OF CONVENIENCE FEES

   Company must not assess Convenience Fees unless Company has disclosed such fees to Servicer previously in writing and Company has been approved by Servicer to assess such fees. If Company completes a Transaction and assesses a Convenience Fee without having disclosed such fee previously in writing and obtained Servicer's consent, Company will be in breach of the Agreement and Servicer may terminate the Agreement in addition to any other remedies available under the Agreement, Laws, and Payment Network Regulations. If an applicable government authority has passed legislation or regulation that requires assessment of Convenience Fees or other fees or charges by government agencies as a component of Payment Device acceptance, such laws will control if they conflict with Payment Network Regulations. If assessment of any Convenience Fees or other fees or charges by government agencies as a component of Payment Device acceptance is not required by Law, Company bears all responsibility and liability associated with the assessment of such fees, including all assessments, fees, fines and penalties levied by the Payment Networks. Convenience Fees may be prohibited by Laws in some States. Company may not charge Convenience Fees where prohibited by Laws.

   CONVENIENCE FEE REQUIREMENTS

   Companies who accept both Visa and MasterCard Credit Cards and/or Debit Cards that desire to assess a Convenience Fee must comply with each of the following requirements:

- A Convenience Fee cannot be assessed for recurring payments. The Convenience Fee is designed for one-time payments and not for payments in which a Customer authorizes recurring charges or debits for recurring goods or services. Examples of recurring charges include, but are not limited to, insurance premiums, subscriptions, internet service provider monthly fees, membership fees, or utility charges.
- Company must provide a true "convenience" in the form of an alternative payment channel outside Company's customary face-to-face payment channels, and the Convenience Fee must be disclosed to the Customer as a charge for the alternative payment channel convenience that is provided. (Companies that do not accept face-to-face payments are not eligible to assess Convenience Fees.)
- The Convenience Fee must be disclosed prior to the completion of the Transaction, and the Customer must be given the option to cancel the Transaction if they do not want to pay the fee.
- The Convenience Fee must be (i) included in the total amount of the Transaction (it cannot be "split" out from the Transaction amount), and (ii) assessed by the same Company actually providing the goods and services and not by a different merchant or any third party; provided, that Companies operating in MCCs 8220 (Colleges/Universities), 9211 (Courts), 9222 (Fines) or 9399 (Miscellaneous Government Services) who utilize a third party agent to collect a Convenience Fee must process the Convenience Fee as a separate Transaction and such third party agent's name must appear in the clearing record for the separate Convenience Fee Transaction.
- If a Convenience Fee is assessed, it must be for all payment types (Visa, MasterCard, Discover, American Express and ACH) within a particular payment channel (mail order, telephone order, and internet).
- The Convenience Fee must be flat regardless of the value of the payment due (not tiered or percentage based), except that an ad valorem amount is allowed where the Company's pricing is subject to regulatory controls that make a flat fee infeasible.
- A customer service number must be transmitted to Servicer for both the payment and the Convenience Fee collected.

If Visa is not among the types of Credit Cards and/or Debit Cards accepted by Company, then the Convenience Fee may be:

- Charged in face-to-face Transactions;
- Tiered, percentage based, or flat;
- Authorized and settled separately from the primary transaction; and
- Assessed by Company's third-party agents.

As between Company and Servicer, should the Payment Networks impose fees or fines as a result of Company's non-compliance with Laws relating to Convenience Fees, all such fees, fines, penalties or damages will be Company's responsibility.

2. **Elavon-Managed.** If Company is eligible to charge Convenience Fees and has elected to have Servicer manage Convenience Fees, then in addition to complying with the foregoing provisions, Company agrees to the following provisions, as applicable.

   a. **General.** So long as Company is in compliance with Payment Network Regulations and Laws, Servicer will inform Company of the amount of the Convenience Fee Company is required to charge for each eligible Transaction, and Company will assess the Convenience Fee. Any Convenience Fee Company charges will be retained by Servicer and constitutes Servicer's property, and Company will have no right, title or interest in such amounts, including if the underlying Transaction is charged back to Company. Servicer may adjust the Convenience Fee from time to time as necessary to accommodate changes in Payment Network fees (including Interchange fees), material changes in average ticket size or monthly Transaction volume, Interchange classification or downgrades, changes in Chargeback rates, or changes in Payment Devices accepted or payment channels offered by Company. Servicer also may immediately

terminate the Convenience Fee Services if Company's Chargeback rates materially exceed industry averages.

b. **POS Devices and Convenience Fee Changes.** Company will ensure that its software, POS Devices and Payment Device acceptance procedures fully comply with Servicer's instructions and Payment Network Regulations, including with respect to programming of software and POS Devices handling of eligible Transactions, for the proper assessment of Convenience Fees and modification of the amount of Convenience Fees charged upon request from Servicer. Company is further responsible for complying with all requirements as provided by Servicer from time to time to appropriately process the eligible Transactions to qualify for optimal Interchange rates within five (5) days of Servicer's communication to Company of the same. If Company fails to make changes to its POS Devices or Payment Device acceptance procedures, or fails to adjust the amount of the Convenience Fee charged per Transaction, within five (5) days of Servicer's request, Servicer may discontinue the program or suspend a certain payment type, or bill Company for charges in excess of the Convenience Fee to recover losses related to Transactions that did not qualify for optimal Interchange rates or did not include the Convenience Fee amount requested by Servicer.

3. **Fees.**

a. If Company has elected that Convenience Fees will be "Company-managed" then Company will pay standard per-transaction fees for Convenience Fee Transactions.

b. If Company has elected that Convenience Fees will be "Elavon-managed," then Servicer will net from the Transaction settlement paid to Company the full amount of the Convenience Fee established by Servicer, and the Convenience Fee retained by Servicer will constitute full payment to Servicer for Servicer's processing of such Transactions. Servicer's retention of the Convenience Fee amount will not relieve Company of any obligation to compensate Servicer for any fines, penalties or other extraordinary fees assessed by Servicer or a Payment Network. Servicer will not refund to Company the amount of the Convenience Fee in the event of a Chargeback.

GOVERNMENT/PUBLIC INSTITUTION SERVICE FEES

1. **Applicability of Chapter.** If Company has requested authority to charge or to have Servicer charge a GPISF to its Customers for Eligible Transactions (defined below) the following provisions apply to such Eligible Transactions and the related GPISF charged.

2. **Definition of Government/Public Institution Service Fee.** A Government/Public Institution Service Fee, or "GPISF," is the fee charged by Servicer or Company, at Company's election, to Customers conducting Eligible Transactions where Company is operating in an eligible Merchant Category Code. GPSIFs include fees referred to as a "service fee" or "convenience fee" (in the context of the eligible MCCs described herein) as used in the applicable rules of the Payment Networks, where the fee is processed as a separate Transaction from the underlying purchase or payment Transaction.

3. **GPISF Services.**

a. **Elavon-Managed and Company-Managed GPISFs.**

i. If Company elects an Elavon-managed GPISF, any GPISF collected in connection with an Eligible Transaction will be retained by Servicer, such amount will be Servicer's property, and Company has no right, title or interest in such amounts. Further, if Company elects an Elavon-managed GPISF, Company agrees that Servicer may adjust the GPISF amount from time to time as necessary or appropriate to accommodate changes in Payment Network fees (including Interchange fees), material changes in average ticket size or monthly Transaction volume, Interchange classification or downgrades, changes in Chargeback rates, or changes in Payment

Devices accepted or payment channels offered by Company. Additionally, Servicer may immediately terminate the Processing Services for GPISFs if Company's Chargeback rates materially exceed industry averages.

ii. If Company elects a Company-managed GPISF, Company will receive and retain the GPISF collected in connection with Eligible Transactions and will pay regular per-transaction fees to Servicer for the Services provided by Servicer with respect to such Transactions. Company agrees that the minimum annual Transaction fees (which include any Servicer-retained GPISF) paid to Servicer for Transactions processed under this Chapter will be at least equal to the "Minimum Annual Fees" amount identified in Schedule A (Schedule of Fees) to the Agreement. For any partial period of less than a full year, the actual amount of fees Company paid to Servicer for Transactions processed under this Chapter will be annualized to determine if Company has satisfied this obligation. At the end of each year (the first year beginning on the effectiveness of this Chapter as to Company), Servicer may notify Company if the actual Transaction fees Company paid in respect of this Chapter are less than the Minimum Annual Fees amount. If Company's actual Transaction processing fees under this Chapter for any such period are less than the Minimum Annual Fees, Company will promptly pay Servicer the difference.

b. **Conflict of Laws.** If an applicable government authority has passed legislation or regulation that requires assessment of GPISFs or other fees or charges by government agencies as a component of Payment Device acceptance, such laws will control if they conflict with Payment Network Regulations. If assessment of any GPISFs or other fees or charges by government agencies as a component of Payment Device acceptance is not required by Law, Company bears all responsibility and liability associated with the assessment of such fees, including all assessments, fees, fines and penalties levied by the Payment Networks.

4. **Requirements for GPISFs.** If Company accepts both Visa and MasterCard-branded Credit Cards or signature Debit Cards for Eligible Transactions, Company will comply with the most restrictive of these Credit Card Association requirements for all Transactions so as not to discriminate among different Payment Devices or Payment Networks. Company may assess or have Servicer assess a GPISF to Transactions involving Discover Network Payment Devices on the same terms as GPISFs are assessed to the other Payment Devices Company accepts.

a. **Eligible Transactions.** Eligible Companies (as defined in (b) and (c) below) may charge or have Servicer charge a GPISF only in connection with the following transactions ("**Eligible Transactions**"):

1. Payments to elementary and secondary schools for tuition and related fees, and school-maintained room and board;

2. Payments to colleges, universities, professional schools, junior colleges, business schools and trade schools for tuition and related fees, and school-maintained room and board;

3. Payments to federal courts of law that administer and process court fees, alimony and child support payments;

4. Payments to government entities that administer and process local, state and federal fines;

5. Payments to local, state and federal entities that engage in financial administration and taxation; or

6. Payments to Companies that provide general support services for the government.

b. **Companies Accepting Visa Cards for Eligible Transactions.** The following requirements apply

if Company accepts Visa Credit Cards or Visa signature Debit Cards and wants to charge or to have Servicer charge a GPISF.

i. **Eligible Companies.** Companies operating in MCCs 8211 (Elementary and Secondary Schools), 8220 (College Tuition), 8244 (Business and Secretarial Schools), 8249 (Trade Schools), 9211 (Court Costs), 9222 (Fines), 9311 (Tax) and 9399 (Miscellaneous Government Services) are eligible to charge or to have Servicer charge a GPISF to Customers in connection with Eligible Transactions listed in Section (4)(b)(ii) below.

ii. **Transaction Requirements.** The following requirements apply to Eligible Transactions under this Section (4)(b):

1. Company must provide Servicer with the necessary documentation to facilitate Servicer's registration of Company in the "Visa Government and Higher Education Payment Program" and the convenience fee program of Discover Network, in each case to the extent applicable and required.

2. The GPISF must be disclosed to the Cardholder prior to the completion of the Transaction, and the Cardholder must be given the option to cancel the Transaction if the Cardholder does not wish to pay the GPISF.

3. Company may not also assess a separate Convenience Fee or U.S. Credit Card Surcharge (as such terms are defined in Visa's Payment Network Regulations).

4. The GPISF must be disclosed as a fee assessed by Company or Servicer.

5. Company must accept Visa as a means of payment in all channels (i.e., face-to-face, mail/telephone, and Internet environments, as applicable).

6. Companies accepting Visa cards for Eligible Transactions must include the words "Service Fee" in the "Company name" field of the Visa Transaction clearing record for the collection of the GPISF.

c. **Companies Accepting MasterCard Cards for Eligible Transactions.** The following requirements apply if Company accepts MasterCard Credit Cards or signature Debit Cards and wants to charge or to have Servicer charge a GPISF.

i. **Eligible Companies**. Companies operating in MCCs 8211 (Elementary Schools), 8220 (Colleges/Universities), 8299 (Miscellaneous School and Education Services), 9211 (Courts), 9222 (Fines), 9223 (Bail and Bonds), 9311 (Taxes), 9399 (Miscellaneous Government Services) and 9402 (Government Postal Services) are eligible to charge or to have Servicer charge a GPISF to Customers in connection with Eligible Transactions listed in Section (4)(c)(ii) below.

ii. **Transaction Requirements.** The following requirements apply to Eligible Transactions under this Section (4)(c).

1. Company must provide Servicer with the necessary documentation to facilitate Servicer's registration of Company in the "MasterCard Convenience Fee Program for Government and Education" or the convenience fee program of Discover Network, in each case to the extent applicable and required.

2. The GPISF must be disclosed to the Cardholder prior to the completion of the Transaction, and the Cardholder must be given the option to cancel the Transaction if the Cardholder does not wish to pay the GPISF.

3. The GPISF collected for other commercial Credit Cards or other consumer signature Debit Cards may be different than the GPISF assessed for MasterCard consumer Credit Cards and MasterCard commercial Credit Cards. This requirement does not apply to payments made by ACH, cash, check or PIN-based Debit Card.

4. The GPISF for MasterCard consumer Credit Cards can be different than the GPISF for MasterCard commercial Credit Cards.

5. The GPISF must not be advertised or otherwise communicated as an offset to the Company discount rate.

d. **Additional Requirements for Companies Utilizing Proprietary Solutions or Service Providers.**

i. **POS Devices.** Company will ensure that its software, POS Devices and Payment Device acceptance procedures comply with Servicer's instructions, including with respect to programming of software and POS Devices for handling Eligible Transactions, for the proper assessment of GPISFs. If the GPISF is Elavon-managed, Company also will comply with all Servicers requirements for appropriately processing the Eligible Transactions to qualify for optimal Interchange rates within five days of receiving the requirements. If Company does not change its POS Devices or card acceptance procedures within five days of Servicer's request, Servicer may discontinue the program or suspend a certain payment type. Further, if Company fails to make such changes and the GPISF is Elavon-managed, Servicer may adjust the GPISF amount and bill Company for charges in excess of the GPISF to recover losses related to Transactions that did not qualify for optimal Interchange rates or for applicable Credit Card Associations' reimbursement programs.

ii. **Approval Required to Charge or Adjust GPISF.** Company may not charge or adjust a GPISF for any Transaction without Servicer's approval. If Company breaches this section, Servicer may immediately terminate the Agreement in addition to pursuing any other remedies available under the Agreement, Laws and Payment Network Regulations.

iii. **Service Provider.** If Company uses a Service Provider to manage and assess Company's GPISF, the "Company name" field of the Transaction clearing record must include the Service Provider's name rather than Company's name. The Service Provider must be clearly identified to the Cardholder as the entity that is assessing the GPISF.

5. **Additional Processing Requirements.** If Company voids an underlying Eligible Transaction, the associated GPISF must be voided as well. If Company processes a refund for an underlying Eligible Transaction, Company will disclose to Customers that the associated GPISF is non-refundable. Company will be assigned separate MIDs for use in connection with Eligible Transactions and related GPISFs. Company will use MIDs assigned for use with Eligible Transactions or GPISFs only to process Eligible Transactions.

6. **Payment and Transaction Types Supported.** GPISF capability for Credit Cards and signature Debit Cards depends on Company's MCC and the Payment Network Regulations of the applicable Payment Network. Not all payment and transaction types are supported for all products. Company's proprietary software, POS Devices, or Service Providers must be certified to process Elavon-managed GPISF Transactions. Closed network prepaid cards, electronic benefits transfer, and dynamic currency conversion are not supported for GPISF processing.

Chapter

11

Electronic Benefits Transfer (EBT) Transactions

If Company accepts EBT Transactions, Company agrees to the following provisions:

Company agrees to issue benefits to recipients in accordance with the procedures specified in Servicer's applicable EBT Quick Reference Guide (QRG) provided to Company by Servicer, as amended from time to time and in accordance with all Laws and Payment Network Regulations pertaining to EBT Transactions, including without limitation, laws pertaining to delivery of services to recipients and recipient confidentiality, including, without limitation, the Federal Civil Rights Act of 1964, Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, Clean Air Act, Clean Water Act, Energy Policy and Conservation Act, Immigration Reform and Control Act of 1986, and regulations issued by the Department of Agriculture pertaining to the Food Stamp Program. The QRG, as amended from time to time, will be deemed to be incorporated by reference into the Operating Guide and constitutes a part of the Agreement.

Chapter

12

PIN-less Bill Payment Transactions

This Chapter describes how to process PIN-less Bill Payment Transactions utilizing PIN-authorized Debit Cards. A PIN-less Bill Payment Transaction is a PIN-less Debit Card payment Transaction resulting in funds transfer from Cardholders to Companies in connection with payments for recurring services (excluding casual or occasional purchases) for which a corresponding invoice is periodically presented to the Cardholder by the Company, and which Transaction is initiated via a telephone (Voice Recognition Unit, Interactive Voice Recognition) or Internet device.

ACCEPTANCE OF PIN-LESS BILL PAYMENT DEBIT CARDS

Authentication. Prior to entering into a PIN-less Bill Payment Transaction, Company must authenticate the Cardholder using information that is not commonly known, but is only known by the Cardholder and Company, such as the Cardholder's account number with Company or information present on the Cardholder's hard copy bill from Company. Company must submit its authentication procedures to Servicer for approval by the appropriate EFT Networks, and Company warrants that it will follow such authentication procedures for each PIN-less Bill Payment Transaction. The use of an authentication procedure, or the approval of such procedure by an EFT Network, is not a guarantee of payment, and Company remains liable for any Chargebacks resulting from any PIN-less Bill Payment Transactions.

No Minimum or Maximum. Company will not establish minimum or maximum PIN-less Bill Payment Transaction amounts. Company must accept PIN-less Bill Payment Transactions on terms no less favorable than the terms under which Company accepts other Payment Devices.

Convenience Fees. Company may not add any amount to the posted price of goods or services Company offers as a condition of paying with a Debit Card unless permitted by the applicable Debit Card Rules.

Purchases Only. Company will support PIN-less Bill Payment Transactions involving purchases only. Company may not initiate a Debit Card Transaction or a Credit Card Transaction for returns or refunds, and must utilize other payment avenues (such as cash, check, or invoice adjustment) to return funds to a Cardholder.

Prohibited Transactions. Company will initiate Transactions only for services approved by Servicer. In no event will Company initiate, allow, or facilitate a gambling or gaming transaction, or fund a stored value account for such purposes.

INTERNET TRANSACTION RECEIPT REQUIREMENTS

At the time of any Internet PIN-less Bill Payment Transaction, Company will make available to each Cardholder a Transaction Receipt (printable from a screen or via e-mail) that complies fully with all Laws and containing, at a minimum, the following information:

- Amount of the PIN-less Bill Payment Transaction, or if a Convenience Fee applies, the amount debited from the Cardholder's account (exclusive of the Convenience Fee, shipping, handling and other fees), and the amount debited from the Cardholder's account (inclusive of the fees);
- Date and local time of the PIN-less Bill Payment Transaction;
- Type of Transaction;
- Type of account accessed;
- Truncated Debit Card number (showing the final four (4) digits);
- Trace or retrieval number;
- Company name;
- MID;
- Company's web site home page URL;
- Promised shipment time period (for Internet Transactions which involve shipment of goods);
- Cardholder's name;
- Authorization Code;
- Description of the bill payment;
- Customer service contact information; and
- Fees imposed by the Company on the Cardholder, including shipping and handling fees, taxes, and Convenience Fees, as applicable.

ADDITIONAL INTERNET REQUIREMENTS

- **Internet Payment Screen and Sales Policy**. Company must prominently display on the Internet Payment Screen the Company's name, telephone number, city and state. Company must also obtain explicit confirmation that the Cardholder understands and agrees that the funds will be immediately debited from their account upon approval of the Transaction, before submission of the PIN-less Bill Payment Transaction. Company must display a clearly visible and conspicuous notice on the Internet Payment Screen of the imposition of any Convenience Fee or the payment of a rebate for a PIN-less Bill Payment Transaction prior to submitting the payment request from the Cardholder. Such notice must include: (i) a heading of "Fee Notice" in at least 14-point type; (ii) text in at least 10-point type; and (iii) the amount of the Convenience Fee or rebate and the name of the party imposing the Convenience Fee or the Company that receives the Convenience Fee.

- **Communication and Encryption**. Company must participate in an approved authentication program as designated by the EFT Networks. All authentication information must be encrypted upon entry into the Internet device and must never leave the Internet device in cleartext form. The Internet device used by Company must meet or exceed the minimum communication and encryption protocol set forth by the EFT Networks.

TELEPHONE TRANSACTION REQUIREMENTS

At the time of a telephone PIN-less Bill Payment Transaction, Company will provide each Cardholder with Transaction information that complies fully with all Laws and containing, at a minimum, the following information:

- Approval or denial of the PIN-less Bill Payment Transaction,

- Amount of the PIN-less Bill Payment Transaction, or if a Convenience Fee applies, the amount debited from the Cardholder's account (exclusive of the Convenience Fee, shipping, handling and other fees), and the amount debited from the Cardholder's account (inclusive of the fees);
- Trace number;
- Authorization Code or confirmation number;
- Customer service contact information; and
- Fees imposed by the Company on the Cardholder, including shipping and handling fees, taxes, and Convenience Fees, as applicable.

Technical Problems. Company will ask a Cardholder to use an alternative means of payment if the Servicer Debit System or the electronic interface with any EFT Network is inoperative.

Adjustment. A PIN-less Bill Payment Transaction may be adjusted if an error is discovered during Company's end-of-day balancing only by means of a written request from Company to Servicer. The request for adjustment must reference a settled PIN-less Bill Payment Transaction that is partially or completely erroneous or a denied pre-authorized Transaction for which the pre-authorization request was approved. An adjustment must be completed within forty-five (45) days after the date of the original PIN-less Bill Payment Transaction.

Company Warranty. In order to accept PIN-less Bill Payment Transactions, Company warrants that it is: (i) a municipal, state or other public utility system operated for the manufacture, production, or sale of electricity, natural or artificial gas, water or waste collection; (ii) an insurance service provider that is licensed by a state to sell property, casualty, life and health insurance policies and that the Transaction involves the payment of premiums on such policies; (iii) a public or private provider of telecommunications services, including telephone, cellular, digital and cable services, which is licensed and governed by any federal, state or municipal authority; (iv) a public or private provider of cable or satellite media services, which is regulated by the Federal Communications Commission or any other federal, state or municipal authority, or (v) any other acceptable Company type, or covered under a pilot program approved by, the EFT Networks.

Termination/Suspension of Bill Payment. When requested by any EFT Network in its sole discretion, Company will immediately take action to: (i) eliminate any fraudulent or improper Transactions; (ii) suspend the processing of PIN-less Bill Payment Transactions; or (iii) entirely discontinue acceptance of PIN-less Bill Payment Transactions.

Chapter

13

No Signature Required Transactions

This Chapter describes how to process No Signature Required Transactions. The No Signature Required Program is limited to qualified Companies and offers only limited protection from Chargebacks.

General Requirements

The No Signature Required Program offerings are as follows:

Participation. Company is responsible for validating that its Merchant Category Code (MCC) is eligible for participation in a No Signature Required Program and that it has been approved by Servicer to participate in the program.

No Signature Required Program. Certain Credit Card Associations have waived signature requirements that allow qualifying Companies to process under-floor-limit transactions without having to obtain a Cardholder signature or provide a Transaction Receipt unless a Cardholder requests a Transaction Receipt. This No Signature Required Program is available to those Companies in a qualifying MCC segment if the following Transaction criteria are met:

1. Transaction amount is less than $25.00.
2. Transaction occurs in a qualifying MCC. Please contact Servicer to determine if your MCC is eligible.
3. The Cardholder is present and the Transaction occurs in a face-to-face environment.
4. The full and unaltered content of Track 1 or Track 2 data of the Card's Magnetic Stripe is read and transmitted as part of the Authorization, or the Transaction is processed via Contactless processing or unaltered chip data is sent for Authorization.
5. Specific MCC's may require at least one (1) Contactless installation within the Company location.
6. One Authorization is transmitted per clearing Transaction.
7. Applies to domestic (U.S.) Transactions only.
8. Currency conversion is not performed.

Eligible Companies that submit Transactions meeting these requirements will receive Chargeback protection against the signature requirement for Transactions that qualify under the specific Credit Card Associations' No Signature Required Program.

Limitations. You understand that participation in a No Signature Required Program provides only limited protection against specific Chargebacks as designated by the sponsoring Credit Card Association.

POS Device. It is your responsibility to determine if your POS Device is configured to prompt for and transmit the data elements required for No Signature Required Transactions.

Chapter

14

Wireless Service Transactions

This Chapter describes how to process wireless Transactions. In addition to the requirements set forth in the Agreement and the procedures set forth elsewhere in the Operating Guide, Companies that process wireless Transactions will adhere to the requirements set forth in this Chapter.

Use of Wireless Services. Company may use the Wireless Services solely as a means of establishing wireless (cellular) connectivity between a Wireless POS Device and Servicer's systems. Company agrees not to use the Wireless Services for remote medical monitoring or any unlawful, fraudulent, abusive or any other unauthorized purposes. Company will promptly notify Servicer in writing in the event that Company becomes aware of any actual or suspected use of the Wireless Services in violation of the Agreement or the Operating Guide, and any applicable schedules, attachments, exhibits, applications and enrollments. Company agrees that it will locate all Wireless POS Devices accessing the Wireless Services within the areas served by the wireless network of the Servicer subcontractor that facilitates the Wireless Services and that all equipment with roaming capabilities will not be permanently located in a roaming area. Company agrees not to use the Wireless Services in connection with any server devices, host computer applications or other systems that drive continuous heavy traffic or data sessions, or as substitutes for private lines or frame relay connections. Further, Company agrees not to use the Wireless Services in a manner that results in highly concentrated usage in limited areas of the wireless network through which the Wireless Services are provided. Company acknowledges and agrees that any violation of the terms and conditions in this Chapter 14 may result in the immediate suspension or termination of Wireless Services.

Limitations of Wireless Technology. Company acknowledges and agrees that because of the emerging nature of wireless technology, certain limitations exist that may affect the performance, Coverage Area, and reliability of wireless technology and wireless processing. Without limiting the generality of the foregoing, wireless processing and the use of a Wireless POS Device are limited to the Coverage Area and may further be limited by a variety of other factors, circumstances, and considerations including, but not limited to, the following: (i) use of a Wireless POS Device outside the Coverage Area will not be possible; (ii) within the Coverage Area, there may exist certain weak coverage areas or other fringe areas where wireless Transaction processing may be intermittent or otherwise interrupted; (iii) within the Coverage Area, certain geographic areas may exist in which wireless Transaction processing may be intermittent or not possible; and (iv) at any time and without notice, any wireless network may become inoperative due to technical difficulties or for maintenance purposes thereby affecting the Company's use of the Wireless Services. In the event Company's ability to use the Wireless Services is limited or prevented for any reason, Company agrees that it will not process any Transaction through the use of Wireless Services, and will in all events obtain an Authorization Code for any such Transaction through means other than wireless processing, as described in the Agreement.

Hardware Devices and Applications. Company acknowledges and agrees that only hardware devices and applications approved by Servicer may be used in conjunction with the Wireless Services. Company further acknowledges and agrees that hardware devices and applications that have not be approved by Servicer may not function or may function improperly when used in conjunction with the Wireless Services.

Completing Unauthorized Transactions. If you choose to complete a Transaction without an Authorization Code because wireless coverage is not available (i.e., you store Transaction data in a Wireless POS Device, provide the Cardholder goods or services and subsequently request Authorization of the Transaction), you do so at your own risk. You understand the risk associated with not obtaining an Authorization Code prior to completing the Transaction (i.e., you subsequently may receive a "decline" or "error" message in response to the later Authorization request). You are fully liable for all Transactions whether or not an Authorization Code is received.

Prohibition on Use of Regeneration Equipment. Company must obtain written approval from Servicer prior to installing, deploying or using any regeneration equipment or similar mechanism (for example, a repeater) to originate, amplify, enhance, retransmit or regenerate the Wireless Services provided hereunder.

Relationship Between Company and Underlying Wireless Services Provider. Company expressly understands and agrees that it has no contractual relationship whatsoever with the operator of the wireless network (or any of its affiliates or contractors) through which the Wireless Services are provided and that Company is not a third party beneficiary of any agreement between Servicer and any such network operator. In addition, Company acknowledges and agrees that the operator of the wireless network through which the Wireless Services are provided and its affiliates and contractors will have no legal, equitable, or other liability of any kind to Company and Company hereby waives any and all claims or demands thereof. Company further acknowledges that representatives of the operator of the wireless network through which the Wireless Services are provided may have met with Company individually or together with Servicer to discuss and review printed materials that explain such network operator's understanding of the services provided by Servicer and such network operator hereunder. Company acknowledges that it has had the opportunity to fully investigate the capabilities, quality and reliability of the Wireless Services and has satisfied itself that such Wireless Services satisfactorily meet its business needs. Company agrees that the operator of the wireless network through which the Wireless Services are provided and its affiliates and contractors will have no legal, equitable, or other liability of any kind to Company arising from or related to any meeting, discussions or explanations regarding the Wireless Services and Company hereby waives any and all claims or demands it may have against the operator of the wireless network through which the Wireless Services are provided and its affiliates and contractors therefor.

Chapter

15

Store and Forward Application Transactions

This Chapter describes how to process Store and Forward Transactions using specific product applications. Specifically, Servicer has developed certain product applications which allow Companies to store transaction data in a POS Device at the time of the sale if a communication channel for transmittal of authorization is not available, and forward such transaction data to Servicer at a later time when a communication channel is available ("**Store and Forward Application**").

GENERAL REQUIREMENTS

The Store and Forward Application Transactions general requirements are as follows:

Participation. Once Company has been approved by Servicer to accept Transactions using the Store and Forward Application and its POS Device has been programmed with the Store and Forward Application, Company may utilize the Store and Forward Application only when a communication channel for transmittal of Authorization information cannot be obtained.

Limitations. Company will not utilize the Store and Forward Application to process any type of PIN-based Debit Card Transactions, Electronic Gift Card Transactions or ECS Transactions.

Forwarding Transaction Data. Company will forward Transaction Data to Servicer via a POS Device within twenty-four (24) hours of the Transaction.

Risk. Company understands that there is significant risk associated with utilizing the Store and Forward Application and not obtaining an Authorization at the time of the sale (i.e., Company may receive a "decline" or "error" message in response to the subsequent Authorization request). Company acknowledges and agrees it is fully liable for all Transactions whether or not an Authorization Approval Code is received.

Changes to Store and Forward Application; Termination. Company acknowledges and agrees that Servicer, in its sole discretion, may make changes to or terminate the Store and Forward Application at any time. Company will indemnify and hold Servicer harmless for any action it may take pursuant to this Chapter.

Warranties and Limitation of Liability.

a. Servicer is not responsible for Store and Forward Transactions.

b. Servicer makes no warranty, express or implied, with respect to the services provided hereunder including, without limitation, any express or implied warranty regarding the services' compliance with any Laws or Payment Network Regulations governing the acceptance of Store and Forward Transactions.

c. Company understands that Transactions processed via the Store and Forward Application are high risk and may be subject to, without limitation, a higher incidence of declined Authorization requests and Chargebacks. Company is liable for all Chargebacks, losses, fees, fines, and penalties related to Transactions processed via the Store and Forward Application including, but not limited to, those resulting from or related to declined Authorization requests and fraudulent Transactions. Further, Servicer is not liable to Company in the event the Transaction Data is not stored within the POS Device for any reason. Notwithstanding the provisions of the Agreement or this Chapter, the liability, if any, of Servicer under this Chapter for any claims, costs, damages, losses and expenses for which they are or may be legally liable, whether arising in negligence or other tort, contract, or otherwise, will not exceed in the aggregate One Thousand Dollars and No Cents ($1,000.00).

Chapter

16

Electronic Gift Card (EGC) Services

This Chapter describes certain services that are available to Companies that have been approved by Servicer for Electronic Gift Card Services. In addition to the requirements set forth in the Agreement and the other applicable procedures set forth in the Operating Guide, Companies that process Electronic Gift Card Transactions will adhere to the requirements set forth in this Chapter.

ECG Processing Services

1. **General Obligations.**

    a. Company will comply with all Laws applicable to the issuance, sale, distribution, use, or acceptance of Electronic Gift Cards (including all Laws relating to purchase, service and dormancy fees, Laws relating to expiration dates, Laws governing the treatment of unused or unclaimed funds or other property, Laws relating to money transmission, and Laws relating to consumer protection), specifically including the Prepaid Access Rule (31 CFR Parts 1010 and 1022) and all other rules promulgated and guidelines published by the Financial Crimes Enforcement Network division of the United States Department of the Treasury.

    b. Until EGC Cardholder Data and Transaction Information have been received and validated by Servicer, Company will maintain enough "backup" information and data (e.g. Transaction Receipts or detailed reporting) with respect to Electronic Gift Cards sold to reconstruct any information or data loss due to a system malfunction or transmission error.

    c. Servicer must participate in all Electronic Gift Card Transactions. If a third party must also participate in such a Transaction, Company will use a Servicer-approved third party.

    d. All Electronic Gift Cards must be printed by Servicer or a Servicer-approved third party.

    e. Company is responsible for all card production and delivery costs.

2. **Direct Settlement.** Company authorizes Servicer to initiate credit and debit entries among Company's individual chain locations for any transactions that change the balance of an Electronic Gift Card. If Servicer cannot accomplish a credit or debit entry to reflect the effect of a Transaction, Company authorizes Servicer to credit or debit (as applicable) the designated Master Account or Primary Company. Servicer may offset any debits against the related credit Transactions of the applicable chain or Company location. Company will notify Servicer in writing of any asserted errors within 45 days of the statement date on which the asserted error first appeared and understands that any failure to do so will preclude further claims or assertion of the error. Company will pay (or will cause its individual chain locations to pay) related direct settlement fees.

3. **Loss, Theft, and Fraud.** Servicer is not responsible for lost, stolen or fraudulent Electronic Gift Cards.

4. **Additional Locations.** Locations added to this processing relationship will be boarded on Servicer's system according to the paperwork submitted by Company to Servicer. If Company submits paperwork reflecting an error or omission of fees payable by Company, the Services fees and other monthly fees applied to the locations during the initial set up or subsequent negotiations will be applied to such locations.

5. **Closing Locations.** If a location closes or changes its Merchant Identification Number (MID), Servicer may bill the Primary Company for any fees associated with subsequent Transactions processed on Electronic Gift Cards activated by the closed MID, including system generated transactions, such as deduction and points conversion transactions. Servicer may also bill to the Primary Company any monthly fees billed for Loyalty Cards or members activated at the closed location.

6. **Post Termination.** Following termination of the Electronic Gift Card Services, Company will pay Servicer a transfer fee based on, among other things, the number of issued Electronic Gift Cards that must be converted to another processor and the data specifications required by Company or such other processor.

7. **Additional Fees.** Company agrees to pay Servicer for EGC production once Company has approved the EGC design proof. Company accepts full responsibility for all EGC production costs. One proof per EGC order is included in the cost of EGC production, and Company agrees to pay thirty-five dollars ($35) for additional proofs. If any order is cancelled prior to EGC production, Company agrees to pay to Servicer a one hundred dollar ($100) cancellation fee.

WEBSUITE SERVICES

"**WebSuite Services**" means an electronic commerce solution provided by Servicer's third party service providers that permits Customers to purchase or add value to Electronic Gift Cards through Company's "WebSuite" site. Customers submit payment for the Electronic Gift Card via a Payment Device through the Processing Services.

If Company has elected to receive WebSuite Services, the following terms will apply:

Company acknowledges that Servicer may engage third party service providers to assist with the performance of the WebSuite Services.

1. **General Obligations.**

   a. Company will timely provide to Servicer specifications for the customization of Company's WebSuite site, including Customer options, web and e-mail content. Company modifications subsequent to the initial submission are subject to change fees.

   b. Servicer is not responsible for any Electronic Gift Card information Company posts to the Company's WebSuite site.

   c. Servicer is not responsible for incomplete or inaccurate payment information provided by any Customer in connection with the WebSuite Services. Company acknowledges that additional Transaction verification and fraud prevention data elements and processes may be available through a particular Payment Network (including address verification) to reduce Transaction risk, and Company agrees that Servicer will only be responsible for implementing the Transaction risk controls that are specifically requested in writing by Company. The use of such Transaction risk controls does not constitute a guarantee of payment or prevent a Transaction from being disputed or subject to Chargeback.

   d. Company acknowledges that Servicer may provide sample terms of use, privacy policy, and other content and disclosure for use on Company's WebSuite site. Company's use of the WebSuite site confirms that Company has had an opportunity to review the sample disclosures and agrees to be solely responsible for all content and disclosures on the WebSuite site.

e. Company is responsible for all Retrieval Requests and Chargebacks under the Payment Network Regulations in connection with Transactions processed using the WebSuite Services. Upon receipt of a Retrieval Request or documentation related to a Chargeback from a Payment Network, Servicer will forward such request or documentation to Company. Company is responsible for responding, as appropriate, to each Retrieval Request or Chargeback.

2. **Electronic Gift Card Order Fulfillment.** Servicer will fulfill all WebSuite Electronic Gift Card orders and include with each order a Company-approved standardized letter customized with the order detail. All orders will be shipped pursuant to the method directed by the Customer.

3. **Electronic Gift Card Loss Protection Program.** Company will determine which data elements it will require its Customers to provide to establish an account or register an Electronic Gift Card on Company's WebSuite site. Company is responsible for notifying its Customers that to take advantage of the Electronic Gift Card loss protection program, the Electronic Gift Card must be registered prior to the loss. Once a registered Electronic Gift Card is reported lost or stolen via the WebSuite site, Servicer will notify Company and freeze the unused balance of the Electronic Gift Card. Company is responsible for transferring the unused balance to a new Electronic Gift Card, sending a replacement Electronic Gift Card to the Customer, and notifying Servicer of the replacement Electronic Gift Card via the WebSuite site.

4. **Reloading of Electronic Gift Cards.** Company will determine the Electronic Gift Card reloading options available to its Customers. While the WebSuite Services permit the anonymous reloading of Electronic Gift Cards, Servicer recommends that Company require its Customers to register the Electronic Gift Card in order to reload value onto the Electronic Gift Card.

5. **Customer Information.** The WebSuite Services will permit Company to have access to Customer information and other data that Company requires to establish an account or register an Electronic Gift Card. Company is responsible for maintaining the appropriate safeguards to protect such Customer information, and to properly disclose the use of such information and its privacy policies on Company's WebSuite site or website. Company must maintain the confidentiality of all Transaction Information and EGC Cardholder Data as provided in the Agreement.

6. **E-Certificates.** Company may choose to use the E-Certificate module, which delivers a "virtual gift card" electronically. The terms applicable to Electronic Gift Cards in this Chapter apply equally to E-Certificates.

PROCESSING ELECTRONIC GIFT CARD TRANSACTIONS

In connection with processing Electronic Gift Card Transactions, Company must comply with the following requirements:

- Supply Servicer with all information and data required by Servicer to perform services related to Company's acceptance of Electronic Gift Cards, including the location of POS Devices and EGC Cardholder Data.
- Maintain all Transaction Receipts and any other receipts as required by Laws.
- When Company sells an Electronic Gift Card from its physical location or locations, including sales completed via electronic commerce, Company is responsible for the collection and settlement of all funds relating to the sale of the Electronic Gift Card, including processing costs associated with such purchase (such as any Credit Card transaction fees or bank service fees, where applicable).

ELECTRONIC GIFT CARD PROCESSING SERVICES

Electronic processing of Transactions and purchases made by Customers using Electronic Gift Cards. Servicer will confirm electronically that the Cardholder presenting the Electronic Gift Card for the purchase of goods or services through Company has an active account on Servicer's Electronic Gift Card processing system and that there is sufficient value associated with the Electronic Gift Card to

allow the Customer to complete the purchase. Servicer will adjust the Cardholder's account through either a debit or credit, as applicable, in the amount of any approved Transaction.

Transaction Record Maintenance. Servicer will maintain an accessible electronic record of the Transactions conducted using an Electronic Gift Card for the lifetime of the card balance and after the balance on the card has been depleted for a period not less than sixty (60) days.

DOWNTIME

Company will not process Electronic Gift Card Transactions if the Electronic Gift Card processing system is down and not able to verify the validity and available balance on an Electronic Gift Card. Company will be solely liable for any losses or damages incurred if Company processes an Electronic Gift Card Transaction without receipt of such verification.

ELECTRONIC GIFT CARD ARTWORK

Electronic Artwork. If applicable, Company is responsible for submitting electronic artwork to Servicer for approval, as described in the Graphic Specifications and Procedures manual provided separately by Servicer (the "**Graphic Specifications and Procedures**"). Company will comply with the Graphic Specifications and Procedures. Company understands that the card proof cannot be created without the submission of artwork, if requested or required. Failure to submit artwork or comply with the Graphic Specifications and Procedures may result in additional fees charged to Company for design work performed to correct the artwork and will result in the delay of the card production process. Servicer and card manufacturer cannot be held responsible for the quality of cards produced using artwork that does not meet the Graphic Specifications and Procedures. Digital artwork should be submitted to:

Artwork@elavon.com

OR

Elavon, Inc.
Attn: Boarding - EGC
7300 Chapman Highway
Knoxville, TN 37920

When sending in artwork, please include:

1. Company name and MID
2. Indicate standard or custom card order
3. Name and telephone number of graphic contact should there be any questions or issues with the artwork submitted

For complete detailed specifications, please send a request for Graphic Specifications and Procedures to Artwork@elavon.com. In your request please indicate that you want standard card or custom card specifications.

Proofing and Production Procedure. Proofs for custom card orders are provided electronically and sent to the email provided. Please print the proof, sign and fax back pursuant to the instructions on the proof. One proof is included in the card production costs. Each additional proof will be billed at thirty-five dollars ($35) each. All proofs for standard card orders are provided electronically as an Adobe pdf document. The proof will be sent to the email address then currently on file with Servicer. If the proof is acceptable, simply reply to the email and indicate approval. Provide detailed information if changes are required. In some instances you may also receive a printer's proof and you will be required to follow the instructions included with the proof. **IMPORTANT: Incorrect graphics WILL delay your order. After you approve the proof, normal production timeframe for card delivery is 2-3 weeks for standard cards and 6-8 weeks for custom cards.**

Chapter

17

Petroleum Services

This Chapter describes certain services that are available to Companies operating in the petroleum industry that have been approved by Servicer to receive Petroleum Services. In addition to the requirements set forth in the Agreement and the procedures set forth elsewhere in the Operating Guide, Companies that use the Petroleum Services will adhere to the requirements set forth in this Chapter.

Provisions Applicable To All Petroleum Services

1. **Access.**

   a. Servicer and Servicer's authorized representatives may access, during normal business hours and occasionally after normal business hours, the Equipment and Software and Company's premises, including offices, facilities, equipment, personnel and other Company resources as required for Servicer to perform the site survey, Equipment and Software installation, inspection, maintenance, and other Petroleum Services. Company will arrange permitted access to areas of third-party facilities as necessary. Servicer will comply with reasonable rules, regulations, and security restrictions regarding access that Company provides in advance and in writing. Company will allow Servicer electronic access to the Equipment and Software at all times. Company will make sure that Servicer's representatives have access to electrical power at Company's location as required for Servicer to efficiently perform the Petroleum Services.

   b. Servicer reserves the right not to provide Petroleum Services with respect to any Equipment at a Company location where Servicer reasonably determines that physical access to such Equipment or other conditions at the locations are unsafe. Servicer will notify Company of the unsafe condition so that Company can correct the safety issue.

2. **Unpermitted Access.** Company will not attempt to obtain Petroleum Services by rearranging, tampering or making unpermitted connection with Servicer's (or its vendors' or subcontractors') system. Company will not, and will not assist anyone else to, (i) copy or duplicate the Software, or (ii) decompile, disassemble, modify, create derivative works of, tamper, reverse engineer or emulate the Equipment or Software. Company will not sell, rent, lend or allow physical or electronic access to any Equipment, Software or Petroleum Services without Servicer's written consent.

3. **Cooperation.** Company will make sure that its personnel assist Servicer as necessary to install and integrate the Equipment and Software, to troubleshoot and isolate faults in the Equipment or Software, and to otherwise perform Petroleum Services. Company will also make sure that its locations are adequately staffed during installation and maintenance to assist Servicer to commission, troubleshoot, and isolate faults in any locations. Servicer will not be liable for any delay in performing, or inability to perform, its duties under this Chapter to the extent caused by any failure by Company to perform the

duties assigned to it or to provide such resources. Company will reimburse Servicer for the reasonable expenses Servicer incurs as a direct result of Company failing to meet such obligations.

4. **Fraud Prevention**. Company will take reasonable steps to reduce, detect and manage fraud. Company will appoint a representative available to Servicer or its vendors or subcontractors to promptly respond to any fraud-related matters.

5. **Title to Software**.

   a. Company acknowledges that any Software and related updates Servicer supplies in connection with the Petroleum Services are subject to the proprietary rights of Servicer or its vendors (the "**Licensors**"). The Licensors will retain all right, title and interest in the Software, all copies, partial copies, compilations and translations of the Software, and underlying intellectual property.

   b. Company will have no ownership interest or proprietary right in the Software, or any enhancements or derivative works, regardless of whether Company requests the development of or pays for such Software, enhancement, or derivative work. If Company pays for such Software, enhancement or derivative work, Company will have the right to use such Software, enhancement or derivative work to receive the Petroleum Services.

   c. Company acknowledges that the Software constitutes trade secrets of the Licensors and that the Software is protected by copyright law. Company will use the Software and its related documentation for its internal use only and will not distribute, sell, assign, transfer, offer, disclose, reproduce, modify, lease or license the Software. Company will not use the Software to process the data of third parties or in a service bureau operation. Company will notify Servicer immediately of the unauthorized possession, use or knowledge of the Software.

   d. Company agrees that its breach of this Section 5 will cause the Licensors irreparable harm.

COMPANY'S OBLIGATIONS FOR SATELLITE SERVICES

1. **Approvals.** Company will obtain all approvals required for the Satellite Services, including landlord approvals, construction permits, and zoning variances if required. If additional or special documentation (such as stamped engineering drawings, location specific drawings or soil test reports) are required, or if Servicer or its representatives are required to attend meetings before local planning or zoning boards or other governmental bodies, additional fees will apply and Company agrees to pay those fees.

2. **Site Survey.** All Company locations require a site survey to identify technically suitable locations for installing the indoor and outdoor Equipment and cables. Company will pay Servicer a site survey fee for each such visit to a Company location.

3. **Non-Standard Installation.** Company will pay for (a) any non-standard installation procedures at any installation location, such as requiring union subcontracting or the use of local facilities personnel, the need to structurally reinforce walls or roofs, landscaping, tree removal, excavation into pavement, blacktop or concrete for cable conduit, roof penetrations, restricted roof access requiring cranes or helicopters, ground mount poles exceeding 6 feet, trenching more than 20 feet of soil, alternate mounting techniques for wall, roof or complex ground mounts, ground cable longer than 15 feet or interconnecting cables longer than 25 feet, and (b) delays due to Company's failure to respond or to provide access.

4. **Cancellation or Expedited Installation**. If Company decides not to proceed with or cancels the installation at a location, Company will pay the cancellation fees set forth in Schedule A (Schedule of Fees) ot the Agreement. Further, if Company requests installation in less than 45 days, Company will

pay the expedited installation fee set forth Schedule A (Schedule of Fees) to the Agreement. Payment of the expedited installation fee does not guarantee a specific installation date.

5. **Specifications.** Company will conform all POS Devices to Servicer's POS Device specifications. Any Company POS Devices that are not Triple DES Derived Unique Key Per Transaction (DUKPT) compliant may be restricted from processing on-line (PIN) debit transactions through some or all of the EFT Networks unless a waiver is obtained by Company from the EFT Networks. Company is responsible for any fines or penalties assessed to Servicer by the Payment Networks due to Company's non-compliance. Company will make sure that the indoor environment conditions comply with the following requirements: operating temperature 10°C to 40°C (50°F to 104°F) and humidity 10% to 90%.

6. **Telecommunications.** Company is responsible for arranging the installation of business telephone lines in its locations. Company is responsible for managing and repairing problems associated with its own telecommunications and processing systems (both hardware and Software).

7. **Included Maintenance.** In consideration for Company's payment of the monthly access and maintenance fees set forth in the Agreement, Servicer will provide the following corrective maintenance for Satellite Services: diagnostic testing; removal and replacement of any malfunctioning field replaceable unit; reorientation of the antenna subsystem in the event of a misalignment; repair or replacement of VSAT interconnecting cables; reloading initial instructions and recommissioning; and verification of proper operation.

8. **Excluded Maintenance.** Maintenance does not include the following services, unless specifically requested by and paid for by Company at Servicer's then-current rates: maintenance, repair, or replacement of parts damaged or lost through catastrophe, accident, lightning, theft, misuse, fault or negligence of Company, or causes external to the Equipment, including failure of, or faulty, electrical power or air conditioning, operator error, failure or malfunction of data communication Equipment not provided to Company by Servicer, or from any cause other than intended and ordinary use; modifications or alterations to the Equipment other than Servicer-approved upgrades and configuration; modifications or alterations to the Equipment by anyone other than Servicer; and deinstallation, relocation or removal of the Equipment or any accessories, attachments, or other devices.

9. **Modifications.** Company is responsible for any alterations or modifications to the Equipment required to comply with any applicable Law.

10. **Equipment.** Company's obligation to pay for Satellite Services, including monthly access and maintenance charges and, if applicable, lease payments, continues with respect to any Equipment provided in connection with Satellite Services regardless of: (a) any loss or destruction of any Equipment, including any VSAT, from any cause whatsoever, other than loss or destruction caused by Servicer; (b) any interference with the use of any Equipment by any private person, corporation or governmental authority other than Servicer; or (c) any force majeure, except in all cases when caused by Servicer.

    a. **Equipment Lease Term.** The initial lease term ("**Initial Lease Term**") for each VSAT will be a period of thirty-six (36) or sixty (60) months, at the option of Company as reflected on Schedule A (Schedule of Fees) to the Agreement, and the term may be different for each VSAT leased. The Initial Lease Term for each VSAT will commence on the first day of the month after the installation date. The lease term will automatically renew for successive periods that are the same length as the Initial Lease Term (each, a "**Renewal Lease Term**"), unless the lease is otherwise terminated by either party providing written notice of an intent not to renew to the other at least one hundred twenty (120) days prior to the expiration of the then current term. Servicer may terminate the lease without prior notice if Company fails to pay Servicer any amounts owed when due.

b. **Possession.** Company will ensure that any Equipment provided hereunder remains in its possession and control, and will not alter the Equipment or have the Equipment moved from the location at which it was originally installed, unless otherwise agreed to in writing by Servicer.

c. **Surrender.** On or before the expiration date of any applicable lease term, Company will, at its cost and expense, surrender possession of the Equipment at such location(s) as Servicer may direct or order deinstallation of the equipment at the price provided in Schedule A (Schedule of Fees) to the Agreement. The Equipment will be returned in the same condition as it was installed (ordinary wear and tear resulting from proper use excepted) and in the condition otherwise required by this Chapter. Company will remain liable for all fees incurred and to be incurred during the remainder of any applicable lease term, as well as any additional continuing fees after such time until the Equipment is returned to Servicer.

d. **Lease Termination.** If Company terminates the lease for any piece of Equipment before the end of the Initial Lease Term or Renewal Lease Term, as applicable, Company will immediately pay Servicer, as liquidated damages, a lease buyout fee equal to the monthly lease payment multiplied by the number of remaining months on the current Initial or Renewal Lease Term. Company agrees that the lease buyout fee is not a penalty, but is reasonable in light of the financial harm caused by early termination of the lease.

e. **Personal Property.** It is expressly understood and agreed that the Equipment will remain personal property notwithstanding the manner in which it may be attached or affixed to realty. Company will, indemnify, defend and hold Servicer harmless from and against any and all loss, liability, cost, damage and expense (including reasonable attorney's fees and court costs) arising out of or related to any claim that the Equipment constitutes a fixture or is a part of the realty in or upon which it is located.

f. **Leased Equipment.** Notwithstanding Company's possession and use of the Equipment, Servicer will retain full legal title to all Equipment that has not been purchased by Company. Company will, at its expense, protect and defend Servicer's title as well as the interest of any assignees, against all persons claiming against or through Company and will at all times keep the Equipment free and clear from any legal process, liens or encumbrances whatsoever (except any placed thereon by Servicer). COMPANY will NOT ASSIGN, SUBLET, MORTGAGE OR HYPOTHECATE ANY EQUIPMENT OR THE INTEREST OF COMPANY HEREUNDER, NOR will COMPANY REMOVE ANY EQUIPMENT FROM ITS ORIGINAL LOCATION OR OUTSIDE THE CONTINENTAL UNITED STATES WITHOUT THE PRIOR WRITTEN CONSENT OF SERVICER.

g. **Damage, Destruction or Loss.** On the installation date of the Equipment, such Equipment will be deemed delivered and accepted by Company. From and after the installation of the Equipment, Company will be responsible for and hereby assumes the entire risk of loss, damage or destruction with respect to any installed Equipment resulting from any cause whatsoever.

- In the event any Equipment is materially damaged, Company will promptly notify Servicer. If such damaged Equipment can be repaired by Servicer or its representatives, Company will pay Servicer for such repairs in accordance with Servicer's then-current rates.

- If any Equipment is damaged beyond repair or is lost, stolen, destroyed, or in the opinion of Servicer rendered permanently unusable or not economically repairable, then Company will immediately notify Servicer in such event and, at Company's expense, will promptly purchase from Servicer or otherwise replace the affected Equipment with a like unit, in good condition and otherwise acceptable to Servicer, free and clear of any liens and encumbrances, and having a fair market value equal to or greater than that of the replaced Equipment prior to it being so affected. Any such replacement of leased Equipment will be the property of Servicer and will be deemed to be the Equipment that it replaced and will be subject to the terms of this Chapter.

h. **Labeling.** Company agrees that, if requested by Servicer, Company will mark or will permit Servicer to mark each piece of Equipment in a reasonably prominent location to provide notice regarding Servicer's ownership interest in such Equipment, and Company will not remove or deface any such marking or labels affixed to any Equipment by Servicer which indicates Servicer's interest therein. Company will replace or permit Servicer to replace any stenciling, tag or plate which has been removed or destroyed or has become illegible. Company will keep all Equipment free from any marking or labeling which might be interpreted as a claim of ownership thereof by Company or any party other than Servicer or anyone so claiming through Servicer.

11. **INSURANCE.** During the term of this Agreement, Company must, at its sole cost and expense, maintain in full force and effect "all risk" extended coverage fire and casualty insurance on the Equipment with an insurance carrier reasonably acceptable to Servicer. Such insurance will: (a) provide for coverage in an amount equal to the greater of the aggregate replacement cost of the Equipment or the aggregate fair market value of the Equipment; (b) be in the form and substance and with insurers reasonably satisfactory to Servicer; (c) designate Servicer as an additional insured and as the loss payee for distribution of the insurance proceeds in accordance with its interest; (d) provide that the policy may not be canceled or materially altered without thirty (30) days prior written notice to Servicer; and (e) provide Servicer with thirty (30) days written notice in which Servicer will be permitted to cure any default by Company under such insurance policy. Upon request from Servicer, Company will furnish to Servicer insurance certificates evidencing the above coverage.

COMPANY'S OBLIGATIONS FOR SMARTLINK SERVICES

1. **Internet Access.** Prior to using SmartLink Services, Company must supply at its expense a high speed Internet connection (e.g., business class DSL or cable Internet or the equivalent). Company will make such high speed Internet connections available for SmartLink Services at all times. Servicer not be liable for such Internet services, and Company will be responsible for managing and repairing problems associated with Company's own telecommunications and processing systems (both hardware and Software).

2. **Integration.** Company will cooperate with Servicer to integrate SmartLink Services at Company's locations, including by reasonably assisting Servicer with interfacing the SmartLink Services with Servicer's vendors and subcontractors. Company is responsible for properly installing the Equipment and Software and is responsible for providing suitable secure space, power, network connectivity and other services for the proper operation of the Equipment and Software, in each case at its expense.

3. **Included Maintenance.** In consideration for Company's payment of the monthly access and maintenance fees set forth in the Agreement, Servicer will provide corrective maintenance for SmartLink Services.

4. **Excluded Maintenance.** Maintenance does not include the following services, unless specifically requested by and paid for by Company at Servicer's then-current rates: maintenance, repair, or replacement of parts damaged or lost through catastrophe, accident, lightning, theft, misuse, fault or negligence of Company, or causes external to the Equipment or Software, including failure of, or faulty, electrical power or air conditioning, operator error, failure or malfunction of data communication Equipment or Software not provided to Company by Servicer, or from any cause other than intended and ordinary use; modifications or alterations to the Equipment or Software other than Servicer-approved upgrades and configuration; modifications or alterations to the Equipment or Software by anyone other than Servicer; and deinstallation, relocation or removal of the Equipment or Software or any accessories, attachments, or other devices.

5. **Modifications.** Company is responsible for any alterations or modifications to the Equipment required to comply with any applicable Law.

COMPANY'S OBLIGATIONS FOR VOYAGER CARD ACCEPTANCE

Conditions of Voyager Card Acceptance. Company agrees to abide by all terms and conditions that apply to accepting Voyager Cards and receiving payment, including the following:

1. Company will honor all valid Voyager® Cards for purchases under the terms and conditions of the Operating Guide and the Agreement.

2. Company is responsible for checking the expiration date and any printed restrictions for both electronic and manual Transactions. Company will electronically authorize all Transactions. If the POS Device authorization system malfunctions, Company will obtain an Authorization by calling the designated Voyager® phone number. If a sale is declined, the Voyager® Card will not be used to complete the sale.

3. At Customer-activated POS Devices, the sales draft will include truncated account number, sub number, truncated expiration date of the Voyager® Card, the Transaction date and time, type of fuel sold, the total sale price, Authorization number, as required, and odometer reading.

4. All cashier-assisted electronic sales drafts and credit vouchers will be completed to include POS Device print showing the Card account name encoded in the Magnetic Stripe (if point-of-sale function is applicable), truncated account number, sub number, truncated expiration date of the Card, the signature of the authorized user, the Transaction date and time, type of fuel sold, a description of the service rendered (if requested), odometer reading (as permitted by the electronic POS Device), total sale price, and the Authorization number.

5. Company will provide a copy of the sales draft or receipt and credit vouchers to the Voyager® Card Cardholder at the time of sale or return. Company will retain a copy of the sales draft for a period of six months from the date of purchase.

6. A Chargeback will be made for sales that are disputed for any reason, including (a) required Authorization was not obtained, (b) were for unauthorized merchandise, (c) were fraudulently made by an employee of Company, (d) the procedures for completing and handling sales drafts or receipts or credit vouchers were not followed, or (e) were in violation of printed instructions. Servicer will promptly notify Company of any Chargeback.

7. Company will maintain a fair policy for the exchange and return of merchandise. Company will promptly submit credits for any returns that are to be credited to the Voyager® Card Cardholder's account.

8. Fees for processing Voyager® Card will accrue daily and be collected by electronically debiting Company's DDA at the same time that processing fees for other Payment Devices are debited. If Company's bank rejects or returns Servicer's debit, Company remains liable for payment of Voyager® processing fees, Equipment and Software, along with any collection fees as specified in the Agreement.

COMPANY'S OBLIGATIONS FOR WRIGHT EXPRESS CARD ACCEPTANCE

If Company has been approved to accept commercial fleet Payment Devices associated with Wright Express, Company agrees to enter into and accept such Payment Devices pursuant to a Wright Express Charge Card Acceptance Agreement. Company acknowledges that Servicer will only provide authorization or data capture services, or both, for Wright Express, and Company will rely upon Wright Express for all other services, including settlement.

COMPANY'S OBLIGATIONS FOR PRIVATE LABEL CARD ACCEPTANCE

If Company notifies Servicer and obtains Servicer's approval, and enters into and abides by an agreement

with the issuer of a Payment Device designed for commercial fleet Transactions issued by a third party, exclusive of Voyager® or Wright Express (a "**Private Label Card**") for the acceptance of such Private Label Cards, then Company may accept such Private Label Card Transactions. Company agrees that Servicer will only provide authorization or data capture services, or both, for such Private Label Cards, and Company will rely upon the issuer of the Private Label Card for all other services, including settlement.

Chapter

18

Converge Services

This Chapter describes certain services that are available to Companies that have been approved by Servicer for Converge Services, including Converge Tokenization Services if selected by Company. In addition to the requirements set forth in the Agreement and the other applicable procedures set forth in the Operating Guide, Companies that use Converge Services will adhere to the requirements set forth in this Chapter.

USE OF CONVERGE SERVICES

The Converge online terminal and payment system (the "**Converge Payment System**") owned and operated by Servicer is provided to Company under the terms and conditions of the Converge Terms of Use, which may be updated from time to time and which are incorporated by reference into the Operating Guide.

BY LOGGING ON TO THE CONVERGE PAYMENT SYSTEM, COMPANY AGREES TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THE CONVERGE TERMS OF USE. IF COMPANY DOES NOT ACCEPT THE TERMS OF USE, COMPANY MAY NOT USE THE CONVERGE PAYMENT SYSTEM.

In addition, Companies who use the Converge Payment System may use the Converge payment system mobile application (the "**Converge Application**") to access the Converge Payment System. Company's use of the Converge Application is subject to the Converge Terms of Use and the End User License Agreement for the Converge Application, which is available on the Converge Application.

In connection with the Converge Services, Company is responsible for:

- Compliance with the Developer Guide to the Converge Services, which is available at http://www.convergepay.com, as the same may be updated by Servicer from time to time.
- All content, design and development of any Customer-facing payments website or interface, except to the extent such content, design and development is exclusively controlled by Servicer as set forth in the Developer Guide to the Converge Services.
- Configuring the Converge interface in accordance with the Developer Guide to the Converge Services.

For more information about Converge Services, please visit http://www.convergepay.com.

ADDITIONAL TERMS APPLICABLE TO CONVERGE SERVICES

1. **License Grant**. Servicer grants to Company a nonexclusive, nontransferable license (without a right of sublicense) to access and use, as applicable, the Converge Payment System, including the Converge Application and documentation, exclusively for Company's internal business use to receive the Converge Services.

2. **Converge Services Restrictions**. Company will not, and will ensure that its employees, agents, contractors, and vendors do not:

   a. copy (other than maintaining one backup or archival copy for Company's internal business use only), re-sell, republish, download, frame or transmit in any form or by any means the Converge Payment System, or any part thereof;

   b. rent, lease, subcontract, operate or otherwise grant access to, or use for the benefit of, any third party, the Converge Payment System;

   c. decompile, disassemble, reverse engineer or translate the Converge Payment System;

   d. change, modify, alter or make derivative works of the Converge Payment System;

   e. without Servicer's prior written consent, grant any third party access to the computers, hardware, system or equipment on which the Converge Payment System or the Converge Services are accessible;

   f. attempt to interfere with or disrupt the Converge Payment System or attempt to gain access to any other services, hardware or networks owned, maintained or operated by Servicer or its suppliers;

   g. disclose any passwords or other security or authentication device with respect to the Converge Payment System to any person other than the person to whom it was issued;

   h. remove, conceal or alter any identification, copyright or other proprietary rights notices or labels on the Converge Payment System;

   i. directly or indirectly, ship, export or re-export the Converge Payment System;

   j. directly or indirectly resell or re-offer the Converge Services; or

   k. act as a gateway through which a third party may gain access to the Converge Payment System or the Converge Services.

3. **Implementation**. Company will pay for any preparation of its facilities necessary for it to access the Converge Payment System and use the Converge Services in connection with this Chapter.

4. **Ownership**. The Converge Payment System, Servicer's Internet websites, and any related intellectual property will remain the exclusive property of Servicer or its licensors, as applicable. Company has no right in or license grant to any source code contained in or related to the Converge Payment System. As between Servicer and Company, Servicer or its licensors, as applicable, will retain all rights, title and interest in the Converge Payment System and the intellectual property. Any information obtained or works created in violation of this Chapter will be both the intellectual property and the Confidential Information of Servicer or its licensors, as applicable, and will automatically and irrevocably be deemed to be assigned to and owned by Servicer or its licensors, as applicable.

5. **Use by Third Parties**. Company may allow one or more third parties to access the Converge Payment System and use the Converge Services, but only for Company's benefit and in connection with Company's internal business operations and activities, including access to the Converge Payment System and use of the Converge Services from backup equipment at a secure off-site backup location and for testing purposes, subject to the restrictions of this Chapter and provided such third parties have agreed to be bound by the licensing terms and restrictions of this Chapter.

6. **Upgrades**. Servicer will make available to Company any updates, upgrades or modifications to the Converge Payment System that Servicer generally makes available to its other customers, and each

such update, upgrade or modification will be deemed to be part of the Converge Services and will be governed by the terms of this Chapter.

TERMS APPLICABLE TO CONVERGE TOKENIZATION SERVICES

1. **Converge tokenization services.** The Converge Tokenization Services consist of a tokenization feature pursuant to which Servicer will provide Company with randomized numerical tokens (each, a "**Token**") in substitution for the account numbers associated with certain types of cards and other payment devices as further specified in the Converge Developers Guide, as the same may be updated by Servicer from time to time (each such number, a "**Card Account Number**"; such services, the "**Converge Tokenization Services**"). More specifically, when a Card Account Number associated with a Transaction is transmitted from Company to Servicer through the Converge Services, Servicer will:

   a. generate a Converge Token;

   b. associate the Converge Token with the Card Account Number; and

   c. send the Converge Token, instead of the Card Account Number, back to Company in the Transaction authorization response message.

   As long as Company elects to purchase the Converge Tokenization Services, the Converge Token, rather than the associated Card Account Number, may be submitted by Company to Servicer through the Converge Services to process additional Transactions to the Credit Card or Signature Debit Card associated with such Converge Token across all Company locations. The Card Account Number associated with each Converge Token generated by Servicer can be retrieved by Servicer, on Company's written request, until the date that is three years after the expiration or termination of the Converge Tokenization Services (the "**Converge Token Validity Period**"), provided that the retrieval of Card Account Numbers after the expiration or termination of this Chapter will be subject to additional terms and conditions and at an additional cost to Company. Company acknowledges that the Converge Tokens will be formatted in Servicer's reasonable discretion and may not be compatible with other Company systems, equipment, communications devices, databases and/or services.

2. **Company's responsibilities regarding the Converge Tokenization Services:**

   a. Company will cause the appropriate hardware, including POS Devices, to be readily available for use at all Company locations that are the recipients or users of the Converge Tokenization Services.

   b. Company acknowledges that Servicer does not store Credit Card or Debit Card expiration dates. In order to use a Converge Token to process a Transaction through the Converge Services, Company must provide the Converge Token (in lieu of a Card Account Number) together with the expiration date for the original Credit Card or Debit Card.

3. **De-tokenization**. Company may request a reversal of the Converge Tokenization process as follows:

   a. To reverse the Converge Tokenization process on an individual Converge Token basis, Company may access a Servicer web portal and, with appropriate authentication credentials, retrieve the Card Account Number associated with any Converge Token.

   b. To reverse the Converge Tokenization process on a bulk basis (i.e., in excess of 100 Converge Tokens at a time), an officer of Company must make a request in writing to Servicer and provide Servicer with the Converge Tokens for which Company wishes to reverse the Converge Tokenization process. Servicer will provide Company's requesting officer with an encrypted file containing the Card Account Numbers associated with such Converge Tokens within 30 days of

receiving the request. Company acknowledges and agrees that additional terms and conditions may apply to reversal of Converge Tokenization on a bulk basis.

4. **Relationship to other Services.** The terms specific to the SAFE-T Services are inapplicable to the Converge Services and the Converge Tokenization Services and the terms of this Chapter are inapplicable to the SAFE-T Services.

Chapter

19

Payment Service Providers

This Chapter describes certain services that are available to Companies that have been approved by Servicer to receive Processing Services as a Payment Service Provider on behalf of Sponsored Companies. In addition to the other requirements set forth in the Agreement and the procedures set forth elsewhere in the Operating Guide, Companies that receive Processing Services as a Payment Service Provider on behalf of Sponsored Companies will adhere to the requirements set forth in this Chapter. Payment Service Providers must comply with the Payment Network Regulations, as modified from time to time, and in the event of any conflict between the Payment Network Regulations and this Chapter or any other provisions of the Operating Guide, the Payment Network Regulations will control.

DUE DILIGENCE OF SPONSORED COMPANIES

The Payment Service Provider will perform due diligence on each of its Sponsored Companies in accordance with this Chapter, the Agreement and the Payment Network Regulations.

INITIAL DUE DILIGENCE

Prior to receiving Processing Services on behalf of a Sponsored Company, the Payment Service Provider will, in relation to each proposed Sponsored Company:

- Verify that each Sponsored Company is a bona fide business operation, including:
  - undertaking credit checks, background investigations and reference checks of the Sponsored Company. In the event that such diligence raises questions or fails to provide sufficient information, the Payment Service Provider will also conduct a credit check of:
    - The owner of the Sponsored Company, if the entity is a sole proprietorship;
    - The partners of the Sponsored Company, if the entity is a partnership; or
    - The principal shareholders of the Sponsored Company, if the entity is a corporation.
  - inspecting the Sponsored Company's premises and/or website(s) and records to ensure that the Sponsored Company has the proper facilities, equipment, inventory, agreements and personnel needed, and if necessary, any license or permit and other capabilities required to conduct its business. If the Sponsored Company has more than one set of premises or more than one website, the Payment Service Provider must inspect at least one of them.

ONGOING DUE DILIGENCE

In addition to its initial diligence obligations, the Payment Service provider must conduct ongoing due diligence of its Sponsored Companies, including:

- retaining records covering the investigation of any of its Sponsored Companies and providing such records to Servicer immediately upon Servicer's request. The Payment Service Provider must retain all records concerning the investigation of any Sponsored Company for a minimum of two (2) years after the date the Sponsored Company Agreement is terminated or expires;

- monitoring each Sponsored Company's activity on an ongoing basis to detect and deter fraud or other wrongful activity; and

- maintaining, on an ongoing basis, the names, addresses and URLs, if applicable, of each of its Sponsored Companies. The Payment Service Provider must promptly supply Servicer and/or the Payment Networks with any such information at Servicer's request.

VERIFYING TERMINATED COMPANY FILES

The Payment Service Provider must verify that the Sponsored Company is not and does not become listed on any Payment Network's terminated merchant file.

- Before entering into, extending or renewing a Sponsored Company Agreement, the Payment Service Provider must request that Servicer make an inquiry to confirm that the Sponsored Company does not appear on any Payment Network's terminated merchant file. Servicer may choose not to accept a Sponsored Company that is listed in a terminated merchant file for any reason, and Servicer will not accept a Sponsored Company that is listed on a Payment Network's terminated merchant file as having been terminated for the following reasons:

    - as a result of an account data compromise;

    - the Sponsored Company unknowingly or unintentionally facilitated by any means, the unauthorized disclosure or use of account information (common point of purchase);

    - money laundering occurs;

    - as a result of excessive Chargebacks;

    - as a result of excessive fraud;

    - there has been a fraud conviction;

    - where a Sponsored Company is bankrupt or in the process of liquidation or a Bankruptcy Proceeding occurs or has occurred in relation to the Sponsored Company;

    - due to a violation of the Payment Network Regulations;

    - where the Sponsored Company has participated in fraudulent collusive activity;

    - as a result of non-compliance with the Payment Card Industry (PCI) Data Security Standards;

    - illegal transactions;

- where there has been identity theft;
- as a result of breach of a Sponsored Company Agreement or any agreement that the Sponsored Company has entered into for the purposes of receiving processing services from Servicer; and
- where the Sponsored Company has exceeded the Payment Networks' thresholds for counterfeit or other fraud or Chargeback activity or the like established periodically by the Payment Networks.

- The Payment Service Provider must inform Servicer, in relation to each Sponsored Company, if a Sponsored Company is terminated for any of the reasons listed in the preceding paragraph, and Servicer will add each Sponsored Company terminated for any such reason to the Payment Networks' terminated merchant files in accordance with the Payment Network Regulations.

PERIODIC REPORTING OBLIGATIONS

The Payment Service Provider will prepare and submit to Servicer as required by the Payment Networks, but not less than quarterly, an activity report for each Sponsored Company containing the following information.

- Each Sponsored Company's name and location as it appears in the card acceptor name/location field of clearing records;
- Each Sponsored Company's "doing business as" name or URL;
- Each Sponsored Company's MCC(s);
- Transaction sales count and amount for each Sponsored Company's MCC(s) by calendar month;
- Transaction Chargeback count and amount for each Sponsored Company's MCC(s) by calendar month; and
- Transaction credit count and amount for each Sponsored Company's MCC(s) by calendar month.

More frequent reporting obligations apply with respect to High-Risk Payment Service Providers, as set forth below.

SPONSORED COMPANY AGREEMENT; SPONSORED COMPANY OVERSIGHT

The Payment Service Provider must enter into a Sponsored Company Agreement with each Sponsored Company. The Sponsored Company Agreement must, in substance, include all of the following provisions, that:

- on an ongoing basis, the Sponsored Company must promptly provide the Payment Service Provider with the current address of each of its offices, all 'doing business as' (DBA) names used by the Sponsored Company, and a complete description of goods sold and services provided;
- in the event of any inconsistency between any provision of the Sponsored Company Agreement and the Payment Network Regulations, the Payment Network Regulations will prevail;
- the Payment Service Provider acknowledges and agrees that the Payment Service Provider is responsible for the Payment Device acceptance policies and procedures of all Sponsored

Companies and the Payment Service Provider has the right to and will require that Sponsored Companies make changes to their websites or otherwise that the Payment Service Provider deems necessary or appropriate to ensure that the Sponsored Company remains in compliance with the Payment Network Regulations;

- the Payment Service Provider will automatically and immediately terminate the Sponsored Company Agreement if the Payment Networks de-register the Payment Service Provider, if Servicer ceases to be a member of the Payment Networks for any reason, if Servicer no longer has a license to use the Payment Network marks, or if Servicer otherwise requires Payment Service Provider to terminate the Sponsored Company Agreement;

- the Payment Service Provider reserves the right to immediately terminate the Sponsored Company Agreement for activity which the Payment Service Provider, Servicer or the Payment Networks deem to be fraudulent or otherwise wrongful;

- the Payment Service Provider will ensure that all Sponsored Companies acknowledge and agree:

    - to comply with applicable Payment Network Regulations, as amended from time to time;

    - that the Payment Networks are the sole and exclusive owners of the Payment Network marks;

    - that the Sponsored Company will not contest the ownership of the Payment Network marks for any reason; and

    - that the Payment Networks may at any time, immediately and without advance notice, prohibit the Sponsored Company from using any of the Payment Network marks for any reason.

PROHIBITED SPONSORED COMPANIES

The Payment Service Provider may not sponsor as a Sponsored Company any entity conducting business that may be described under the following merchant types, which may be classified with MCCs 4814, 5912, 5962, 5966, 5968 and 5969, and which are ineligible to be Sponsored Companies:

- Buyers clubs/membership clubs

- Credit counseling or credit repair services

- Credit protection/identity theft protection

- Direct marketing – subscription merchants

- Infomercial merchants

- Internet pharmacies

- Internet pharmacy referral sites

- Multi-level marketing businesses

- Outbound telemarketers

- Rebate-based businesses

- Up-Selling merchants

HIGH-RISK PAYMENT SERVICE PROVIDERS

- A Payment Service Provider that proposes to sponsor as a Sponsored Company any entity conducting business that may be described under any one of the following MCCs or any entity that as a merchant was reported under the Payment Networks' excessive Chargeback programs is deemed a High-Risk Payment Service Provider:

    - Telecom merchants – MCCs 4813, 4816 and 5967 (other than those telecom merchants classified under MCC 4814, which are prohibited);

    - Electronic commerce (e-commerce) adult content (videotext) merchants – MCCs 5967, 7273, 7841;

    - Non-face-to-face gambling Companies – MCC 7995;

    - Non-face-to-face prescription drug merchants – MCC 5122 (other than those merchants classified under MCC 5912, which are prohibited); and

    - Non-face-to-face tobacco product merchants – MCC 5993.

    The Payment Service Provider must notify Servicer prior to signing a Sponsored Company Agreement with any such Sponsored Company (or prior to accepting any Transactions from such a Sponsored Company if an existing Sponsored Company) to enable Servicer to register each such entity in the Payment Networks' registration systems before accepting Transactions from any such Sponsored Company. Servicer reserves the right to decline to register and to require Payment Service Provider not to enter into a Sponsored Company Agreement, or to terminate an existing Sponsored Company Agreement, with any Sponsored Company that causes or would cause Payment Service Provider to be a High-Risk Payment Service Provider.

- If the Payment Service Provider is a High-Risk Payment Service Provider, the Payment Service Provider will ensure that each Sponsored Company implements real-time and batch procedures to monitor continually the following:

    - simultaneous multiple Transactions using the same Payment Device; and

    - consecutive or excessive attempts using same Payment Device.

- When attempted fraud is evident, the Payment Service Provider will ensure that the Sponsored Company implements temporary bank identification number locking as a fraud deterrent.

- The Payment Service Provider will ensure that each Sponsored Company complies with the fraud control standards prescribed by the Payment Networks and maintains a Chargeback to Interchange sales volume ratio below the Payment Networks' requirements regarding excessive Chargebacks.

- On a monthly basis, the High-Risk Payment Service Provider will provide to Servicer an activity report for each Sponsored Company the sponsorship of which causes Payment Service Provider to be a High-Risk Payment Service Provider. Monthly reports will include the following:

    - Each Sponsored Company's name and location as it appears in the card acceptor name/location field of clearing records;

    - Each Sponsored Company's "doing business as" name or URL;

- Each Sponsored Company's MCC(s);
- Transaction sales count and amount for each Sponsored Company's MCC(s) by calendar month;
- Transaction Chargeback count and amount for each Sponsored Company's MCC(s) by calendar month; and
- Transaction credit count and amount for each Sponsored Company's MCC(s) by calendar month.

Chapter

20

Services in Canada

This Chapter describes certain requirements with which Companies operating in Canada ("**Canadian Companies**") must comply. Canadian Companies must execute a separate agreement or otherwise be approved to receive Services from Servicer for Transactions accepted at Company locations in Canada. Canadian Companies must comply with the requirements set forth in the Agreement and in the Operating Guide, as such requirements are supplemented and/or modified by the following requirements contained in this Chapter.

For purposes of Transactions in Canada, please note the following:

- All references to "U.S. Mail" also include the Canadian Postal Service.
- All U.S. dollar amounts contained within the Operating Guide should be deemed to be Canadian dollars by Canadian Companies.
- All references to U.S. law enforcement agencies in the Operating Guide are replaced with references to the Royal Canadian Mounted Police or the local police of the jurisdiction, as applicable.

CHAPTER 1

The following provisions are hereby added to or amended in Chapter 1 of the Operating Guide, *About Your Card Program*:

- In the "Types of Cards" section of Chapter 1 of the Operating Guide, *About Your Card Program*, the following provision is hereby added:

    - "Automated Teller Machine (ATM) Card" includes an Automated Banking Machine (ABM) Card. An ABM Card is issued by a financial institution and allows a Customer to withdraw funds, make deposits or perform other banking functions though an ABM.

- In the "General Operating Guidelines" section of Chapter 1 of the Operating Guide, *About Your Card Program*, in the "Do Not Set Restrictions on Card Transactions" section, the following is hereby added after the second sentence: "Further, Company may provide differential discounts among different Payment Networks. All discounts must be clearly marked at the point-of-sale."

- In the "General Operating Guidelines" section of Chapter 1 of the Operating Guide, *About Your Card Program*, the "Do Not Discriminate" section is deleted and replaced with the following: "**No Obligation to Accept All Cards of a Payment Network:** If you accept Credit Card payments from a particular Payment Network you are not obligated to accept Debit Card payments from that same Payment Network, and vice versa. You can choose to accept only Credit Card or Debit Card payments from a Payment Network without having to accept both."

- In the "General Operating Guidelines" section of Chapter 1 of the Operating Guide, *About Your Card Program*, in the "Security Program Compliance" section, the reference to "Visa's Cardholder Information Security Program (CISP)" is hereby replaced with "Visa's Account Information Security (AIS) program," with which Canadian Companies and any third party vendors utilized by Canadian Companies must comply.

CHAPTER 2

The following provisions are hereby added to or amended in Chapter 2 of the Operating Guide, *Processing Transactions*:

- In "The Electronic Authorization Process" section of Chapter 2 of the Operating Guide, *Processing Transactions*, Canadian Companies must send "Declined Pick-Up" Cards to the following Canadian address:

  Exception Processing
  ATTN: Card Pick Up
  Elavon Canada Company
  P.O. Box 4373 STN A
  Toronto, Ontario M5W3P6

- The "Transaction Processing Restrictions" section, "Surcharges" paragraph, of Chapter 2 of the Operating Guide, *Processing Transactions*, is inapplicable, as surcharging of Credit Card Transactions is not permitted in Canada.

- In the "Processing Card Not Present Transactions – Card Identification Number and Address Verification Service" section of Chapter 2 of the Operating Guide, *Processing Transactions*, Canadian Companies needing more information about processing Card Not Present Transactions should call the following numbers for assistance from American Express and Discover Network:

  - American Express: (800) 268-9824
  - Discover Network: (800) 263-0104

- In the "Additional Requirements Applicable to PIN-Authorized Debit Card Transactions" section of Chapter 2 of the Operating Guide, *Processing Transactions*, the following provisions are hereby added with respect to PIN-authorized Debit Card Transactions in Canada:

  Surcharges. Company may add an amount to the price of goods or services Company offers as a condition of paying with a Interac Debit Card provided that the Cardholder is notified through the POS Device of such amount and the Cardholder has the option to cancel the Debit Card Transaction, without cost, prior to the Debit Card Transaction being sent to the Issuer for Authorization and provided that the addition of a surcharge or user fee is permitted by the Debit Card Rules. Visa, MasterCard and Discover Network do not permit surcharging of Debit Card Transactions in Canada.

  Non-Disclosure of Debit Card Rules. Company will not disclose the Debit Card Rules to any Person except as may be permitted under the Agreement or required by applicable Law. For purposes of Transactions in Canada, the Debit Card Rules include all applicable rules and operating regulations of the EFT Networks, and all rules, directions, operating regulations, and guidelines for Debit Card Transactions issued by Servicer from time to time, including, without limitation, all amendments, changes, and revisions made thereto from time to time. Company agrees to take care to protect the Debit Card Rules using a degree of care at least equal to that used protect Company's own confidential information, and Company will not use the Debit Card Rules for its own benefit or the benefit of any third person without the consent of the EFT Networks.

Employee Logs; Due Diligence. Company will maintain accurate logs of employee shifts, and will provide these logs to Servicer within 24 hours of a request to do so as part of an investigation of a Debit Card fraud or other incident. Company acknowledges and agrees that the EFT Network requires Servicer or its designated agents to perform a due diligence review to determine that Company is able to comply with all applicable requirements for the Debit Card Transaction services, including but not limited to security and technical standards specified by Servicer and the EFT Networks. Company acknowledges that additional due diligence may be conducted by Servicer or its designated agents in the event of a change in control of Company's business. Servicer will not be required to provide the Debit Card Transaction services to Company if Servicer determines that to do so would pose a material risk to the security or integrity of the Debit Card Transaction services.

- In the "Additional Requirements Applicable to PIN-Authorized Debit Card Transactions" section of Chapter 2 of the Operating Guide, *Processing Transactions*, the following provisions are added to the "Use and Availability of POS Devices and PIN Pads" heading with respect to PIN-authorized Debit Card Transactions in Canada:

  - Company is responsible for installing the POS Device and PIN Pad in such a way that Cardholders may enter their PIN into the PIN Pad in a confidential manner. Company must not install the PIN Pad in a location that will allow easy visibility by third parties when the PIN Pad is in use by a Cardholder. For attended operations, Company must equip the PIN Pad with a privacy shield or design it to be hand-held so that the Cardholder can shield it with his or her body.

  - Company must take all reasonable precautions to ensure that all POS Devices are closed and unavailable for use after business hours. Company also must advise Servicer immediately if Company suspects that any POS Device has been tampered with or if any PIN Pad has been lost or stolen.

  - Company must not manually key direct Debit Card information into a POS Device in order to complete a Transaction. Company must give the Cardholder a Transaction Receipt regardless of whether a Debit Card Transaction is approved, declined or not completed.

  - If Company's printer is not operational and Company's POS Device has processed the Debit Card Transaction, Company will (i) provide an alternate Transaction Receipt, such as a completed and dated sales slip or manually created facsimile showing the account number on the Debit Card to indicate that payment was made with that Debit Card, or (ii) reverse the Debit Card Transaction on the day of the request or the next business day if the Cardholder requests that Company do so.

  - If a Debit Card is left at Company's premises, Company agrees to promptly return it to the Cardholder, subject to satisfactory identification of the Cardholder, or if Company is unable to return the Debit Card or if the Debit Card is not claimed within twenty four (24) hours, Company must deliver such card to us at Company's first available opportunity.

- In the "Additional Requirements Applicable to PIN-Authorized Debit Card Transactions" section of Chapter 2 of the Operating Guide, *Processing Transactions*, in addition to the listed requirements under the "Transaction Receipt Requirements" heading, the following requirements apply with respect to PIN-authorized Debit Card Transactions in Canada:

  Transaction Receipt Requirements. Company will retain a copy of each Debit Card Transaction Receipt for a period of three (3) years from the date of the applicable Transaction.

  The following requirements are hereby added to the information which must be contained on a Debit Card Transaction Receipt:

  - Unique number or code assigned to the POS Device at which the Debit Card Transaction was made;
  - Issuer Authorization Number;

- Indicate the status and disposition of the Transaction, approved or declined; and
- Amount of any user fee or surcharge amount, if imposed.

o In the "Additional Requirements Applicable to PIN-Authorized Debit Card Transactions" section of Chapter 2 of the Operating Guide, *Processing Transactions*, in addition to the listed procedures under the "Merchandise Returns" heading, the following procedures apply with respect to PIN-authorized Debit Card Transactions in Canada:

Merchandise Returns.

- For all Merchandise returns, or any other debit return initiated through Company's POS Device or account, Company bears all responsibility for such transactions even if fraudulent.

o In the "Other Transaction Types" section of Chapter 2 of the Operating Guide, *Processing Transactions*, under the "Quasi Cash Transactions" heading, the following additional language is added to "Casino gaming chips":

- Casino gaming chips—must be authorized using a POS Device that is capable of reading the Card Verification Value from the Magnetic Stripe. A key-entered Transaction is not permitted for the purpose of obtaining Casino gaming chips.

CHAPTER 5

The following provision is applicable to Canadian Companies and is hereby added to Chapter 5 of the Operating Guide, *Code 10 Procedures*:

o Canadian Companies that encounter unauthorized Cards should send the information set forth in Chapter 5 of the Operating Guide to the following Canadian address:

Exception Processing
ATTN: Card Pick Up
Elavon Canada Company
P.O. Box 4373 STN A
Toronto, Ontario M5W3P6

CHAPTER 7

The provisions set forth in Chapter 7, *International Transactions*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 8

The provisions set forth in Chapter 8, *Vehicle Rental or Leasing Authorization Procedures*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 9

The provisions set forth in Chapter 9, *Lodging Accommodations Authorization Procedures*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 10

The following provision is hereby added to Chapter 10 of the Operating Guide, *Convenience and Government/Public Institution Service Fee Requirements* in the Convenience Fee subsection:

- Company may charge a convenience fee only if Company does not accept Visa in the channel of commerce to which the convenience fee is applied.

The provisions set forth in Chapter 10 in the Government/Public Institution Service Fee Requirements subsection are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 11

The provisions set forth in Chapter 11, *Electronic Benefits Transfer (EBT) Transactions*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 12

The provisions set forth in Chapter 12, *PIN-less Bill Payment Transactions*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 13

The provisions set forth in Chapter 13, *No Signature Required Transactions*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 14

The provisions set forth in Chapter 14, *Wireless Service Transactions*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 15

The provisions set forth in Chapter 15, *Store and Forward Application Transactions*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 19

The provisions set forth in Chapter 19, *Payment Service Providers*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 21

The provisions set forth in Chapter 21, *Services in Puerto Rico*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 22

The provisions set forth in Chapter 22, *Fanfare Loyalty and Gift Card Services*, are inapplicable, as these services are not available to Canadian Companies.

CHAPTER 32

The following provision is applicable to Canadian Companies and is hereby added to Chapter 32 of the Operating Guide, *Additional Resources*:

- To obtain Payment Network-specific information, Canadian Companies can access the following web sites:

  American Express: http://www.americanexpress.ca

  Discover Network: http://www.novusnet.com

  MasterCard: http://www.mastercard.com/canada/business/merchant

  Visa: http://www.visa.ca

INTERAC ONLINE SERVICES

Interac Online is a service whereby an Interac Online Cardholder may choose to pay Company for goods and services purchased over the Internet from a Customer account at a financial institution. The following provisions are applicable to Canadian Companies utilizing the Interac Online services.

Interac Online Rules. Company will comply with and be bound by the Interac Online Rules, which are incorporated by this reference as if fully set forth herein. Servicer and/or the Acxsys Corporation may amend the Interac Online Rules and any of their requirements and/or regulations at any time and continued use of the Interac Online services will evidence Company's agreement to be immediately bound by any new requirements and/or regulations. Company hereby grants to Servicer the right to verify that Company is in compliance with the Interac Online Rules. Company will not disclose the Interac Online Rules to any Person except as may be permitted under the Agreement or as required by applicable Law.

Due Diligence. Company acknowledges and agrees that Servicer or its designated agent may perform a due diligence review to determine Company's ability to comply with all applicable requirements of the Interac Online Rules. Company acknowledges and agrees that additional due diligence may be conducted by Servicer or its designated agent in the event of a change in control of Company's business. Servicer will not be required to provide the Interac Online services to Company if Servicer determines that to do so would pose a material risk to the security or integrity of the Interac Online system. Company provides informed consent that Servicer may use any information collected from its Companies.

Security. Company agrees to provide to Servicer the information required to complete Servicer's security compliance certification program, as required by the Interac Online Rules.

Minimum Transaction. Company agrees to comply with any minimum transaction values which may be set by Servicer or the bank or other financial institution issuing the Interac Online Card.

Types of Transactions. Company may process purchases and refunds (credits) for Interact Online Cardholders. Company may not process Transactions for cash back or balance inquiries.

Interac Online Transaction Fees. Company may not add any amount to the posted price of goods or services as a condition of paying with an Interac Online Card, unless permitted by the applicable Interac Online Rules.

Display of Interac Online Logo and/or Wordmark. Unless otherwise informed by Servicer, Company will prominently display the most current version of the Interac Online logo and/or wordmark on the checkout page of Company's website in accordance with the specifications and requirements set forth in the Interac Online Rules. Company's right to use or display such marks will continue only as long as the Agreement remains in effect and such right will automatically terminate upon termination of the Agreement.

Website Requirements. Company's website must comply with the Agreement and the Interac Online Rules, including, but not limited to, the following:

- *Confirmation Page*: Company must display both the bank or other financial institution's name and confirmation number as received in the form post message. The Customer must be given the opportunity to print the confirmation page as a record of the Transaction, which may be accomplished using the web browser's print function. Further, the confirmation page should state that the Transaction was successful.
- *Timeout message*: If Company allows less than 30 minutes for a Customer to complete a Transaction through an issuer's website, Company will post notice on the Company website to inform the Customer the amount of time allotted to complete the Transaction and that the Transaction will "timeout" if the Customer does not complete the Transaction within the allotted time.
- *Currency*: Company website must disclose the amount that will be debited from the Customer's account in Canadian funds, and indicate that the currency is Canadian dollars (e.g., by using the prefix "C$" or "CAD").
- *Learn More*: Company must provide a link to the "Learn More" site before the Customer initiates the Transaction and leaves Company's website.

CHIP AND PIN TRANSACTIONS

Credit Cards and Debit Cards are changing from signature-based and PIN-based Magnetic Stripes to PIN-based Chip Cards. This initiative, which is known as "Chip and PIN," is in response to escalating levels of fraud, most notably, counterfeiting and the use of lost or stolen Cards. A Chip Card contains a microchip, which is embedded into the Card. It contains extremely secure memory and processing capabilities. The information it contains helps ensure that the Chip Card is authentic and makes it difficult and expensive for a criminal to counterfeit the Chip Card. A PIN is entered by the Cardholder to confirm that they are the actual owner of that Chip Card.

Chip Card Acceptance.

- The Chip Card and Cardholder must be present for all Chip and PIN Transactions.
- To initiate a Chip and PIN Transaction, insert the Chip Card into the Chip-Reading Device.
- Company will require that each Cardholder enter his or her PIN at the Chip-Reading Device. No data referencing the Cardholder's PIN will be printed on any Transaction Receipt.
- Company must submit Authorization and clearing messages for Chip and PIN Transactions using full data.
- Company must provide the Authorization Code in the clearing record for all Chip and PIN Transactions that are approved offline.
- If a Canada Issuer (or its agent) issues a Declined Code or a Declined Pick-Up Code, or a Compliant Chip Card declines a Chip and PIN Transaction, the Transaction must not be processed by any other means.
- If the Chip or Chip-Reading Device is inoperable, Company must obtain a Magnetic Swipe Authorization. If the Magnetic Stripe cannot be read, or if Magnetic Swipe Authorization is not available, existing Card acceptance and Transaction processing procedures apply. Note that where an Authorization request is made when the Chip or Chip-Reading Device is inoperable, Company must include the appropriate values in the Authorization request identifying the Transaction as a fallback Transaction to the Chip and PIN Transaction.

- Company must comply with all, and ensure that its Chip-Reading Devices comply with all, Payment Network Regulations applicable to Chip and PIN Transactions, including all operating requirements, technical guides and other requirements specified by the applicable Payment Networks in connection with the acceptance of Chip Cards.

Note that Company will have sole and exclusive liability for counterfeit and fraudulent Transactions that occur, but which could have been prevented had Company installed and properly used Chip and PIN Technology in accordance with all Payment Network Regulations.

Chapter

21

Services in Puerto Rico

This Chapter describes certain requirements with which Companies operating in Puerto Rico ("**Puerto Rican Companies**") must comply. Puerto Rican Companies must execute a separate agreement or otherwise be approved to receive Services from Servicer for Transactions accepted at Company locations in Puerto Rico. Puerto Rican Companies must comply with all requirements set forth in the Agreement and in this Operating Guide, as such requirements are supplemented and/or modified by the provisions contained in this Chapter.

CHAPTER 1

The following provisions are hereby added to or amended in Chapter 1 of the Operating Guide, *About Your Card Program*:

- In the "General Operating Guidelines" section of Chapter 1 of the Operating Guide, About Your Card Program, in the "Security Program Compliance" section, the reference to "Visa's Cardholder Information Security Program (CISP)" is hereby replaced with "Visa's Account Information Security (AIS) program," with which Puerto Rican Companies and any third party vendors utilized by Puerto Rican Companies must comply.

CHAPTER 2

The following provisions are hereby added to or amended in Chapter 2 of the Operating Guide, *Processing Transactions*:

- In the "Additional Requirements Applicable to PIN-Authorized Debit Card Transactions" section of Chapter 2 of the Operating Guide, Processing Transactions, the following provisions are hereby added with respect to PIN-authorized Debit Card Transactions in Puerto Rico:

  Surcharges. The ATH Network does not permit surcharging of Debit Card Transactions at POS Devices.

  Non-Disclosure of Debit Card Rules. Company will not disclose the Debit Card Rules to any Person except as may be permitted under the Agreement or required by applicable Law. For purposes of Transactions in Puerto Rico, the Debit Card Rules include all applicable rules and operating regulations of the EFT Networks, and all rules, directions, operating regulations, and guidelines for Debit Card Transactions issued by Servicer from time to time, including, without limitation, all amendments, changes, and revisions made thereto from time to time. Company agrees to take care to protect the Debit Card Rules using a degree of care at least equal to that used protect Company's own confidential information, and Company will not use the Debit Card Rules for its own benefit or the benefit of any third person without the consent of the EFT Networks.
  Employee Logs; Due Diligence. Company will maintain accurate logs of employee shifts, and will

provide these logs to Servicer within 24 hours of a request to do so as part of an investigation of a Debit Card fraud or other incident. Company acknowledges and agrees that the EFT Networks require Servicer or its designated agents to perform a due diligence review to determine that Company is able to comply with all applicable requirements for the Debit Card Transaction services, including but not limited to security and technical standards specified by Servicer and the EFT Networks. Company acknowledges that additional due diligence may be conducted by Servicer or its designated agents in the event of a change in control of Company's business. Servicer will not be required to provide the Debit Card Transaction services to Company if Servicer determines that to do so would pose a material risk to the security or integrity of the Debit Card Transaction services.

- In the "Additional Requirements Applicable to PIN-Authorized Debit Card Transactions" section of Chapter 2 of the Operating Guide, Processing Transactions, the following provisions are added to the "Use and Availability of POS Devices and PIN Pads" heading with respect to PIN-authorized Debit Card Transactions in Puerto Rico:

  - Company is responsible for installing the POS Device and PIN Pad in such a way that Cardholders may enter their PIN into the PIN Pad in a confidential manner. Company must not install the PIN Pad in a location that will allow easy visibility by third parties when the PIN Pad is in use by a Cardholder. For attended operations, Company must equip the PIN Pad with a privacy shield or design it to be hand-held so that the Cardholder can shield it with his or her body.

  - Company must take all reasonable precautions to ensure that all POS Devices are closed and unavailable for use after business hours. Company also must advise Servicer immediately if Company suspects that any POS Device has been tampered with or if any PIN Pad has been lost or stolen.

  - Company must not manually key direct Debit Card information into a POS Device in order to complete a Transaction.

  - Company must give the Cardholder a Transaction Receipt regardless of whether a Debit Card Transaction is approved, declined or not completed. If Company's printer is not operational and Company's POS Device has processed the Debit Card transaction, Company will (i) provide an alternate Transaction Receipt, such as a completed and dated sales slip or manually created facsimile showing the account number on the Debit Card to indicate that payment was made with that Debit Card, or (ii) reverse the Debit Card Transaction on the day of the request or the next business day if the Cardholder requests that Company do so.

  - If a Debit Card is left at Company's premises, Company agrees to promptly return it to the Cardholder, subject to satisfactory identification of the Cardholder, or if Company is unable to return the Debit Card or if the Debit Card is not claimed within twenty four (24) hours, Company must deliver such card to us at Company's first available opportunity.

- In the "Additional Requirements Applicable to PIN-Authorized Debit Card Transactions" section of Chapter 2 of the Operating Guide, Processing Transactions, in addition to the listed requirements under the "Transaction Receipt Requirements" heading, the following requirements apply with respect to PIN authorized Debit Card Transactions in Puerto Rico:

  Transaction Receipt Requirements. Company will retain a copy of each Debit Card Transaction Receipt for a period of three (3) years from the date of the applicable Transaction. The following requirements are hereby added to the information which must be contained on a DebitCard Transaction Receipt:

  - Unique number or code assigned to the POS Device at which the Debit Card Transaction was made;

- Issuer Authorization Number;
- Indicate the status and disposition of the Transaction, Approved or Declined; and
- Amount of any user fee or surcharge amount, if imposed.

o In the "Additional Requirements Applicable to PIN-Authorized Debit Card Transactions" section of Chapter 2 of the Operating Guide, Processing Transactions, in addition to the listed procedures under the "Merchandise Returns" heading, the following procedures apply with respect to PIN-authorized Debit Card Transactions in Puerto Rico:

Merchandise Returns.

- For all Merchandise returns, or any other debit return initiated through Company's POS Device or account, Company bears all responsibility for such transactions even if fraudulent.

CHAPTER 10

The following provision is hereby added to Chapter 10 of the Operating Guide, *Convenience Fee Requirements*:

o Company may charge a convenience fee only if Company does not accept Visa in the channel of commerce to which the convenience fee is applied.

CHAPTER 12

The provisions set forth in Chapter 12, *PIN-less Bill Payment Transactions*, are inapplicable, as these services are not available to Puerto Rican Companies.

CHAPTER 22

The provisions set forth in Chapter 22, *Fanfare Loyalty and Gift Card Services*, are inapplicable, as these services are not available to Puerto Rican Companies.

IVU Loto Program

Companies operating in Puerto Rico must comply with the requirements of this Chapter. All Companies that operate locations in Puerto Rico are obligated to register with the Department of Treasury and may be required to participate in the IVU Loto program. Companies operating in Puerto Rico must complete the IVU Loto registration process to determine if your business qualifies.

Company Obligations in the IVU Loto Program

All Companies are obligated to register for the IVU Loto program. If you have not registered, please follow the registration steps below:

- Visit the Department of Treasury's internet website at www.ivuloto.pr.gov and click on the *Portal de Registro*.
- During the registration process, please select **Elavon** as your processor.
- You will be notified whether your business qualifies for IVU Loto and you will receive a Company Registration Number.

- If you complete the registration process, but are advised that you are not eligible for the IVU Loto program, you have complied with the requirements of the IVU Loto program.
- Please note that any company that does not register could be subject to a penalty imposed by the Department of Treasury.

All eligible Companies must:

- Process or register through your POS Device all transactions for goods or services for which the purchaser is present at the point of sale.
- Provide the purchaser the official purchase receipt, with the IVU Loto code, printed by the POS Device.
- Transmit, on a daily basis, all IVU Loto codes to Elavon via your POS Device and Elavon will relay that information to the Department of Treasury.
- Exercise due care in using the POS Device.

Guidelines for Companies

Elavon offers several POS Devices that support the IVU Loto program as an integrated feature of our transaction-processing services.

BOARDING

- Contact Elavon Customer Service to request support for the IVU Loto program on your POS Device.
- Complete and sign an Add Equipment form. Be sure to include your Company Registration Number received from the Department of Treasury.
- Submit the Add Equipment form to Elavon.
- The POS Device will be updated with the appropriate IVU Loto-supported application.

TRANSACTION PROCESSING

For all on-line transactions, such as Credit Card or Debit Card transactions, you must enter the amount of the sale plus the State Sales Tax and the Municipal Sales Tax into the POS Device during the course of entering the transaction information.

For cash and cash equivalent transactions, such as cash, check or money order transactions, you must enter these transactions into the POS Device, including the State Sales Tax and Municipal Sales Tax.

During periods of time when the system and/or POS Device are not functioning properly, IVU Loto codes will not be generated for transactions until such time as the system is restored and/or the POS Device is repaired.

Please note that Elavon is not responsible for the validity of the information entered into the POS Device for each transaction.

SAMPLE RECEIPT

Below is an example of the manner in which the sales tax information will appear on the purchaser receipt:

Below is an example of the manner in which the IVU Loto-related information will appear on the purchaser receipt:

```
IVULOTO: NNNNN-NNNNN
PP DRAW### MM/DD/YY
```

More Information

You can find more information regarding the IVU Loto program, including contact information and technical support information, at www.ivuloto.pr.gov.

FanFare Loyalty Services and Fanfare Gift Card Services

The provisions set forth in Chapter 22, *Fanfare Loyalty and Gift Card Services*, are inapplicable, as these services are not available in Puerto Rico.

Chapter

22

Fanfare Loyalty and Gift Card Services

This Chapter describes certain services that are available to Companies that have been approved by Servicer to receive Fanfare Services. In addition to the requirements set forth in the Agreement and other applicable procedures set forth in the Operating Guide, Companies that use Fanfare Services will adhere to the requirements set forth in this Chapter.

GENERAL FEATURES AND REQUIREMENTS

Overview of Fanfare Services. Company has elected to receive from Servicer one or both of the Fanfare Loyalty Services and/or the Fanfare Gift Card Services. Servicer delivers the Fanfare Services through the Fanfare Platform. Company's access to and use of the Fanfare Services and the Fanfare Platform are subject to the Agreement, the provisions of the Operating Guide, and the materials made available to Company by Servicer that relate to the Fanfare Services, including any quick reference guides and best practices guides.

Fanfare Web Portal. Servicer will provide Company with access to the Fanfare Web Portal. Company agrees to review and to comply with any materials made available by Servicer through the Fanfare Web Portal from time to time in connection with Company's use of the Fanfare Services and its operation of its Fanfare Loyalty Program and/or Fanfare Gift Card Program.

FANFARE LOYALTY SERVICES

Companies that elect to use the Fanfare Loyalty Services will have access to the Fanfare Services and Fanfare Platform made available by Servicer for Company's development, implementation and maintenance of its Fanfare Loyalty Program.

- **Company Enrollment and Set Up.** Company must enroll and be approved by Servicer to participate in and use the Fanfare Loyalty Services. Once approved, Servicer will provide Company with a welcome kit that may include Model Documents, generic branded marketing materials to help Company promote its Fanfare Loyalty Program to Customers, marketing tips, staff training tips, and a terminal quick reference guide. Only Fanfare Enrolled Customers may participate in Company's Fanfare Loyalty Program.
- **Customer Enrollment.** Company's Customers must affirmatively enroll in Company's Fanfare Loyalty Program in order to participate. Company may not use an opt-out or other negative consent campaign to enroll Customers in its Fanfare Loyalty Program. A Customer is considered a Fanfare Enrolled Customer when the Customer explicitly opts into participation in Company's Fanfare Loyalty Program and agrees to be subject to Company's Fanfare Loyalty Program terms and conditions and related privacy policy. A Fanfare Enrolled Customer's election to participate in Company's Fanfare Loyalty Program will be

communicated to Servicer through Company's properly-enabled Supported Hardware (for point-of-sale enrollments) or when the Customer registers for Company's Fanfare Loyalty Program at Company's Fanfare Loyalty Website (for Customers that do not enroll at the point of sale).

Company Fanfare Loyalty Website. As part of the Fanfare Loyalty Services, Servicer will provide a Fanfare Loyalty Website for Customer registration and Fanfare Loyalty Program Account management. Company must ensure that the internet address of its Fanfare Loyalty Website is included on every Transaction Receipt the Company prints for Customers that enroll in the Company's Fanfare Loyalty Program at the Company's point of sale (as described below). The Fanfare Loyalty Website will:

- Make available to Customers all Company Fanfare Loyalty Program disclosures;
- Enable Customers to enroll and un-enroll in the Company Fanfare Loyalty Program;
- Collect Customer Data; and
- Provide Customers with access to information about available rewards and programs, rewards eligibility, and progress toward achieving rewards.

METHODS OF CUSTOMER ENROLLMENT IN COMPANY'S FANFARE LOYALTY PROGRAM

Enrollment at Point of Sale. Customers may initially enroll in Company's Fanfare Loyalty Program at the time of a point-of-sale purchase Transaction at a Company location. Company offers Customers the opportunity to enroll at the point-of-sale through prompting via Company's Supported Hardware. Company may not offer point-of-sale Fanfare Loyalty Program enrollment other than through Supported Hardware. **Company is responsible for ensuring that any Customer offered enrollment in Company's Fanfare Loyalty Program is notified that such enrollment is optional and is not a condition to completing the purchase Transaction.** When Company is collecting information in connection with enrolling a Customer in Company's Fanfare Loyalty Program at the point of sale, Company should clearly communicate to the Customer that the purpose for collecting such information is loyalty program enrollment and not a part of the Transaction.

- Company must obtain a phone number from the Customer at the time of the Customer's enrollment at the point-of-sale, and must input the phone number into the POS Device so that Servicer may reflect the Customer as a Fanfare Enrolled Customer in Company's Fanfare Loyalty Program.
- Company may present a Customer electing to enroll at the point-of-sale with the option to (i) link the Customer's Credit Card or Debit Card with the Fanfare Enrolled Customer's Fanfare Loyalty Program Account, or (ii) receive a Fanfare Loyalty Card linked to the Fanfare Enrolled Customer's Fanfare Loyalty Program Account. Each of these options is described further below.
- When a Customer enrolls at the point-of-sale, the Transaction Receipt provided to the Customer at the conclusion of the Transaction must confirm enrollment and direct the Fanfare Enrolled Customer to follow the internet link disclosed on the Transaction Receipt to the Company's Fanfare Loyalty Website where the Fanfare Enrolled Customer may view the full terms and conditions and privacy policy governing the Fanfare Enrolled Customer's participation in Company's Fanfare Loyalty Program.

Enrollment through Fanfare Loyalty Website. Customers that do not enroll at the point of sale may enroll by visiting the Company's Fanfare Loyalty Website and completing the online registration process described under "Fanfare Loyalty Program Registration" below.

FANFARE LOYALTY PROGRAM REGISTRATION AND ADDITIONAL FEATURES

Fanfare Loyalty Program Registration. Customers that wish to enroll in Company's Fanfare Loyalty Program online, and Customers that have enrolled at the Company's point-of-sale but wish to enhance their Fanfare Loyalty Program experience, may register at Company's Fanfare Loyalty Website. Each registering

Customer will be required to provide a phone number and other identifying information to register through Company's Fanfare Loyalty Website. Fanfare Registered Customers may also elect to link a Credit Card or Debit Card, and/or a Fanfare Loyalty Card, with their Fanfare Loyalty Program Account, each as further described below.

Linking a Credit Card or Debit Card to a Fanfare Enrolled Customer's Fanfare Loyalty Program Account. A Fanfare Enrolled Customer may link a Credit Card or Debit Card to the Fanfare Enrolled Customer's Fanfare Loyalty Account. Linking a Credit Card or Debit Card may be completed at the Company's point-of-sale using Supported Hardware (including at the time of initial enrollment) or at the Company's Fanfare Loyalty Website.

Linking a Fanfare Loyalty Card to a Fanfare Enrolled Customer's Fanfare Loyalty Program Account. If Company's selected Fanfare Loyalty Program supports this feature, Company may choose to offer a Fanfare Enrolled Customer the option to receive and use a Fanfare Loyalty Card as a means of accessing the Fanfare Enrolled Customer's Fanfare Loyalty Account. Linking a Fanfare Loyalty Card may be completed at the Company's point-of-sale using Supported Hardware or at the Company's Fanfare Loyalty Website. Fanfare Loyalty Cards must be ordered through Servicer and must comply with Servicer's requirements related to Fanfare Loyalty Cards.

Rewards. Company may use the Fanfare Web Portal to create offers and establish rewards and qualifications. All offers and rewards established under Company's Fanfare Loyalty Program are available to all Fanfare Enrolled Customers, except where Servicer supports and Company elects to make certain offers or rewards available only to a select segment of Fanfare Enrolled Customers. Company is solely responsible for ensuring that all offers and rewards established by Company (including any offers or rewards suggested by Servicer for Company's use) are suitable for Company's situation and business, and that all such offers and rewards (including how such offers and rewards are promoted or marketed) comply with all Laws. Company will not make or promote offers or rewards that are unrelated to Company's business or that include infringing, obscene, threatening, defamatory, fraudulent, abusive or otherwise unlawful or tortious material, including material that is harmful to children or violates third party privacy rights. Company is solely responsible for the costs and any other expenses or liabilities arising from or in connection with any offers or rewards made or promoted by Company.

COMPANY FANFARE LOYALTY PROGRAM MARKETING AND COMMUNICATION

Companies using the Fanfare Loyalty Services will have access to e-mail marketing services supported by the Fanfare Platform for communicating with and marketing to Fanfare Registered Customers regarding Company's Fanfare Loyalty Program. Fanfare Registered Customers will be able to manage their marketing preferences through their Fanfare Loyalty Program Account accessible at the Fanfare Loyalty Website. Company will control, and is solely responsible for, the marketing or communication characteristics (such as frequency, timing, recipients, and opt-out lists associated with such marketing or communications) and the content of any such marketing or communication efforts through the Fanfare Platform. Further, Company assumes full responsibility and liability for ensuring that any such marketing efforts or communications comply with (i) Laws, including where Company's marketing materials are based on templates or make use of services provided by Servicer, (ii) are conducted in accordance with the terms and conditions and privacy policy governing the Fanfare Registered Customer's participation in Company's Fanfare Loyalty Program; and (iii) are consistent with any other disclosure made by Company to a Fanfare Registered Customer concerning Company's marketing and information use practices generally.

E-mail marketing and communication. Servicer provides Company with the ability to send marketing and communication e-mails to its Fanfare Registered Customers through the Fanfare Platform. Such e-mails must follow any format specifications provided to Company by Servicer. Servicer does not review the content of any e-mail message requested to be sent by Servicer on behalf of Company to its Fanfare Registered Customers. Company acknowledges and agrees that it is solely responsible for the content of any such e-mail message, and that all e-mail messages sent using the Fanfare Platform will relate to Company's Fanfare Loyalty Program relationship with the Fanfare Registered Customers. Nonetheless, Servicer reserves the right to refuse to send

any e-mail communication requested by Company that the Servicer deems, in its sole discretion, to be in violation of any Law, that is unrelated to the Company's business, that is infringing, obscene, threatening, defamatory, fraudulent, abusive, unlawful, tortious, threatening or inappropriate for children, or that is outside the scope of the Fanfare Loyalty Services.

Customer "Unsubscribe" Option. All marketing and communication e-mails sent by Company through the Fanfare Platform will contain an "unsubscribe" link, which will direct the Fanfare Registered Customer to a Fanfare-hosted "landing page" where the Customer can register his/her election to stop receiving marketing e-mails from Company. Servicer will track the marketing preferences specified by Company's Fanfare Registered Customers, including those who have elected to unsubscribe or opt-out from marketing e-mails from Company, which information will be accessible by Company through the Fanfare Web Portal. In addition, the Fanfare Web Portal will enable Company to manually "unsubscribe" Fanfare Registered Customers who have communicated their opt-out election to Company outside of the Fanfare Platform.

IMPORTANT: COMPANY REQUIREMENTS FOR E-MAIL MARKETING TO CUSTOMERS

The Federal CAN-SPAM Act of 2003 (CAN-SPAM) places certain responsibilities on "senders" of e-mail. As a Company sending e-mails to Fanfare Registered Customers through the Fanfare Loyalty Program, it is your responsibility to comply with these CAN-SPAM requirements. Among these requirements, when a customer responds to a commercial e-mail from a sender, and requests that the sender not send future commercial e-mail communications to the customer, this request must be promptly honored. This is true *regardless* of whether these requests are in response to an e-mail sent to a customer by Company through the Fanfare Loyalty Program, or *outside of* the Fanfare Loyalty Program.

For Fanfare Registered Customers who opt-out/unsubscribe from receiving future Company marketing e-mails through the Fanfare Platform, the Fanfare Platform will automatically "block" further marketing e-mails from Company to those Fanfare Registered Customers. However, it is the Company's sole responsibility to ensure that these customers are also blocked (i.e., unsubscribed) from receiving any future commercial e-mails which Company may send *outside of* the Fanfare Platform. Additionally, when a Fanfare Registered Customer responds to a commercial e-mail sent by the Company *outside of* the Fanfare Platform, and opts-out/unsubscribes from receiving further commercial e-mails from Company, it is Company's sole responsibility to record such opt-out request within the Fanfare Platform to ensure that future Fanfare marketing e-mails from the Company to the Fanfare Registered Customer are blocked.

To help facilitate your compliance with these requirements, Fanfare provides Companies with access to all relevant opt-out/unsubscribe information within the Fanfare Platform at all times. With this access, it is Company's responsibility to:

(1) Review the list within the Fanfare Web Portal of those Fanfare Registered Customers who have opted-out/unsubscribed from receiving commercial e-mails from Company through the Fanfare Loyalty Program and ensure that these Fanfare Registered Customers are similarly blocked (or removed) from any other commercial e-mail list that Company maintains or utilizes outside of the Fanfare Loyalty Services; and

(2) Regularly access the Fanfare Web Portal to manually block any Fanfare Registered Customer from receiving marketing e-mails from Company through the Fanfare Platform, when such Fanfare Registered Customer has provided Company with a request, *outside of* the Fanfare Platform, to opt-out/unsubscribe from receiving future commercial e-mails from Company.

Additional information regarding CAN-SPAM can be found at the Federal Trade Commission's Business Center, a website designed to help small businesses understand and comply with various laws, including CAN-SPAM. The business center can be found at http://business.ftc.gov/ and a CAN-SPAM guide for business can be found at http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business. We particularly encourage those Companies that conduct e-mail marketing campaigns *in addition to* those conducted by the Company through the Fanfare Loyalty Services to understand the compliance obligations imposed by CAN SPAM, and to seek legal guidance on this issue if necessary.

FANFARE GIFT CARD SERVICES

Companies that elect to use the Fanfare Gift Card Services will have access to the Fanfare Services and Fanfare Platform made available by Servicer for Company's deployment and maintenance of its Fanfare Gift Card Program.

PROCESSING FANFARE GIFT CARD TRANSACTIONS

In connection with processing Fanfare Gift Card Transactions, Company must comply with the following requirements:

- Supply Servicer with all information and data required by Servicer to perform services related to Company's acceptance of Fanfare Gift Cards, including the location of POS Devices and Customer Data.
- Maintain all Transaction Receipts and any other receipts as required by Laws.
- Comply with all Laws applicable to the sale, distribution, redemption and escheat of prepaid gift cards and related balances, specifically including the Prepaid Access Rule (31 CFR Parts 1010 and 1022) and all other rules promulgated and guidelines published by the Financial Crimes Enforcement Network division of the United States Department of the Treasury.
- Ensure that no fees or expiration dates apply to the Fanfare Gift Cards.
- When Company sells a Fanfare Gift Card from its physical location or locations, including sales completed via electronic commerce, Company is responsible for the collection and settlement of all funds relating to the sale of the Fanfare Gift Card, including processing costs associated with such purchase (such as any Credit Card transaction fees or bank service fees, where applicable).

Fanfare Gift Card Processing Services

- **Electronic processing of Transactions and purchases made by Customers using Fanfare Gift Cards.** Servicer will confirm electronically that the Cardholder presenting the Fanfare Gift Card for the purchase of goods or services through Company has an active Fanfare Gift Card account on the Fanfare Platform and that there is sufficient value associated with the Fanfare Gift Card to allow the Customer to complete the purchase. Servicer will adjust the Customer's Fanfare Gift Card account through either a debit or credit, as applicable, in the amount of any approved Transaction.
- **Transaction Record Maintenance**. Servicer will maintain an accessible electronic record of the Transactions conducted using a Fanfare Gift Card for the lifetime of the card balance and after the balance on the card has been depleted for a period not less than sixty (60) days.
- **Downtime.** Company will not process Fanfare Gift Card Transactions if the Fanfare Platform or Fanfare Services is down and not able to verify the validity and available balance on a Fanfare Gift Card. If Company's system are unable to communicate electronically with the Fanfare Platform, Company may call Fanfare Services customer service at 1-800-725-1243 to verify the validity and available balance on a Fanfare Gift Card. Company will be solely liable for any losses or damages incurred if Company processes a Fanfare Gift Card Transaction without receipt of such verification.

ELECTRONIC GIFT CARD ARTWORK

Electronic Artwork. If applicable, Company is responsible for submitting electronic artwork to Servicer for approval, as described in the Graphic Specifications and Procedures manual provided separately by Servicer (the "**Graphic Specifications and Procedures**"). Company understands that the card proof cannot be created without the submission of artwork, if requested or required. Failure to submit artwork or comply with the

Graphic Specifications and Procedures may result in additional fees charged to Company for design work performed to correct the artwork and will result in the delay of the card production process. Servicer cannot be held responsible for the quality of cards produced using artwork that does not meet the Graphic Specifications and Procedures. Digital artwork should be submitted to:

Artwork@elavon.com

OR

Elavon, Inc.

Attn: Boarding - EGC

7300 Chapman Highway

Knoxville, TN 37920

When sending in artwork, please include:

1. Company name and MID
2. Indicate standard or custom card order
3. Name and telephone number of graphic contact should there be any questions or issues with the artwork submitted

For complete detailed specifications, please send a request for Graphic Specifications and Procedures to Artwork@elavon.com. In your request please indicate that you want standard card or custom card specifications.

Proofing and Production Procedure. Proofs for custom card orders are provided electronically and sent to the e-mail provided. Please print the proof, sign and fax back pursuant to the instructions on the proof. One proof is included in the card production costs. Each additional proof will be billed at thirty-five dollars ($35) each. All proofs for standard card orders are provided electronically as an Adobe pdf document. The proof will be sent to the e-mail address then currently on file with Servicer. If the proof is acceptable, simply reply to the e-mail and indicate approval. Provide detailed information if changes are required. In some instances you may also receive a printer's proof and you will be required to follow the instructions included with the proof. **IMPORTANT: Incorrect graphics WILL delay your order. After you approve the proof, normal production timeframe for card delivery is 2-3 weeks for standard cards and 6-8 weeks for custom cards.**

Chapter

23

MerchantConnect

MerchantConnect, an online reporting system, allows a Company to access Transaction data at any time, from any standard web browser (e.g., Internet Explorer). MerchantConnect supports delivery of Authorization, Settlement, Chargeback, Interchange, adjustment/rejection and additional reporting via an online tool for viewing and/or exporting, as well as access to additional customer support. MerchantConnect can help streamline your daily reconciliation of your Transactions, help answer your questions about your point-of-sales equipment and provide an overview of products and services that Servicer can provide to you.

MERCHANTCONNECT CONNECTION OPTIONS

MerchantConnect Basic: includes a single log-on to access information for a single Company location. You can view up to six (6) months of past statements, Chargeback and retrieval reporting, and can review batch reporting for up to thirty (30) days of settled Batch activity. In addition, you can access up to three (3) years of analytic data (average ticket, volume and Transaction counts) and have industry comparison capabilities. You can also link to report sites for our Electronic Gift Card and Electronic Check Service programs. Terminal quick reference guides are available for your reference, as well as tips and best practices to help prevent fraud in your business.

Transaction data is available twenty-four (24) hours per day, seven (7) days per week, three hundred sixty-five (365) days per year. Authorization data is refreshed on an hourly basis. Settlement data is refreshed multiple times a day, but data availability it contingent on your scheduled settlement time.

MerchantConnect Premium: provides all of the data and information as MerchantConnect Basic, plus users can consolidate reporting for multiple locations. Enhanced information is available in MerchantConnect Premium; where users can access up to a year's worth of reporting information and have the ability to view batches of Transactions grouped by Card type or Batch reference number. Hierarchical reporting allows users the ability to aggregate data from multiple locations, and users can also export files into Excel or CSV formats for use with users' own software systems.

External Partner Access: provides all of the data available with MerchantConnect Premium and adds the ability to control multiple users' access to data, add and/or delete users, and set users' level of access at a single location, group of locations or all locations. In addition, users can control which reports users have access to in an easy to use portal.

NOTE: *Additional fees may apply for MerchantConnect Premium and External Partner Access.*

ACCESSING MERCHANTCONNECT

To access MerchantConnect, you can register at www.merchantconnect.com where you will be prompted to create a user ID and password. You must authenticate your account by entering your Merchant Identification Number and the last four (4) digits of your checking account number at the time of registration. To request access for MerchantConnect Premium or External Partner Access, simply complete the request form, which can be found at https://www.merchantconnect.com/forms/MCPUserSetupForm.doc.

ADDITIONAL INFORMATION AVAILABLE VIA MERCHANTCONNECT

MerchantConnect will provide you with the latest version of your Terms of Service and Operating Guide. Information is available to help you understand Interchange qualifications and how you can obtain the best Interchange rate for your Transactions. Also, MerchantConnect contains information that will help you mitigate risk and provides tips regarding the latest fraud scams are added as they become known to Servicer. Information on compliance and data security is also available on MerchantConnect.

Take a moment to browse the portal to learn all of the features available.

Chapter

24

Transend Pay Services

This Chapter describes certain services that are available to Companies that have been approved by Servicer to receive the Transend Pay Services. The Transend Pay Services allow a healthcare provider Company to streamline its revenue cycle management and provides an efficient and secure way for Company to receive healthcare-related and benefit payments from Healthcare Payers.

In addition to the requirements set forth in the Agreement and other applicable procedures set forth in the Operating Guide, Companies that use the Transend Pay Services will adhere to the requirements set forth in this Chapter.

PROVISIONS APPLICABLE TO THE TRANSEND PAY SERVICES

Overview of Transend Pay Services. Company has elected to receive the Transend Pay Services from Servicer. Company's receipt of Transend Pay Services is subject to the Agreement, the Operating Guide and the materials made available to Company by Servicer that relate to the Transend Pay Services, including any quick reference guides and best practices guides. Company agrees to review and to comply with any materials made available by Servicer, or by any of Servicer's vendors or subcontractors, to Company from time to time in connection with Company's use of the Transend Pay Services.

Transend Pay Services Website. Servicer, through Servicer's vendor, will provide Company with access to the Transend Pay Services Website. Servicer is not responsible for the form, format or content of the Transend Pay Services Website or any Remittance Data. Company agrees to abide by any terms of use and/or end user license(s) provided by Servicer or Servicer's vendor in connection with the Transend Pay Services Website.

Questions regarding Payments made via the Transend Pay Services. Questions regarding payments received from Healthcare Payers, including remittance advice, identity of the relevant Healthcare Payer and related questions should be directed to Servicer's vendor using the procedures outlined in the agreement between Company and Servicer's vendor or as otherwise indicated on the Transend Pay Services Website. Questions regarding the Transend Pay Services provided by Servicer, including funding settlement and Company reporting, should be directed to Servicer via the general customer service process.

Waiver of Claims. Company expressly acknowledges and agrees that, immediately upon Servicer's receipt of funds that are to be processed via the Transend Pay Services in connection with a payment owed to Company by a Healthcare Payer, Company's claim relating to such payment from the Healthcare Payer will be

extinguished, and Company automatically waives any and all claims against the applicable Healthcare Payer in connection with such payment.

Fraud Prevention. Company will take reasonable steps to reduce, detect and manage any fraud-related issues related to Company's receipt of the Transend Pay Services and Company's access to the Transend Pay Services Website. Company will appoint a representative available to Servicer or its vendors or subcontractors to promptly respond to any fraud-related matters.

Warranties and Limitation of Liability. Company acknowledges that Servicer will engage third party service providers to assist with the provision of the Transend Pay Services, including, but not limited to, the provision of the Transend Pay Services Website. Company acknowledges and agrees that Company may be required to enter into a user agreement with, or agree to be bound by certain terms and conditions provided by, Servicer's vendor in order for Company to access the Remittance Data.

Termination of Transend Pay Services. Servicer may terminate the Transend Pay Services at any time, in Servicer's sole discretion, upon notice to Company.

Participation of Healthcare Payers. Participating Healthcare Payers may change from time to time. Participation by a Healthcare Payer in the Transend Pay Services is at the discretion of the individual Healthcare Payer, and Servicer is not responsible for the participation (or lack thereof) of any Healthcare Payer in the Transend Pay Services.

Protected Health Information. No Protected Health Information (as such term is defined in HIPAA) will be provided to, or transmitted by, Servicer in connection with the Transend Pay Services. Company acknowledges and agrees that Company will not deem Servicer to be a Business Associate and that Servicer will not be required to enter into a Business Associate Agreement in connection with the provision of the Transend Pay Services.

Disclosure of Information. Notwithstanding any other provisions in the Agreement, Servicer may disclose information related to Company's receipt of the Transend Pay Services, including Transaction Data, to third parties to the extent necessary to allow Servicer to provide such services to Company.

Chapter

25

Payment Navigator Services

This Chapter describes the Payment Navigator Services available to Companies. The "Payment Navigator Services" include Payment Navigator, Healthcare Payment Processing Services and, if selected, Healthcare Administration Services, all as described in this Chapter.

In addition to the requirements set forth in the Agreement and other applicable procedures set forth elsewhere in the Operating Guide, Companies that use the Payment Navigator Services will adhere to the requirements set forth in this Chapter.

Provisions Applicable to the Payment Navigator Services

Definitions.

"**Healthcare Administration Services**" means (as selected by Company):

- the eligibility services (insurance eligibility/benefit inquiries for patient health plan status, deductible, co-pay information);
- patient payment estimates (estimate of patient responsibility based on planned healthcare services);
- patient statements (production and fulfillment of patient billing statements); and
- electronic bill presentment services (online presentment of patient bills/statements).

"**Healthcare Payment Processing Services**" means the acceptance and processing of payment by cash, check, Electronic Check Service, Credit Card, or Debit Card, acceptance of scheduled payments from checking or savings accounts, Credit Cards, or Debit Cards; the maintenance of a patient portal for online payment; posting of payments to patient accounts; and related customer support.

"**Payment Navigator**" means a hosted web based patient payment application that enables transactions at the point-of-care including a patient payment portal for online payments, streamlines back office collections, and automates posting of patient accounts.

Business Associate Services. Company is a covered entity as defined in 45 C.F.R. § 160.103 and the regulations codified at 45 C.F.R. Parts 160 and 164 ("**HIPAA Privacy Rule**") promulgated under Subtitle F of Title II of HIPAA. In connection with its performance of services other than certain Payment Navigator Services under the Agreement, Servicer is processing customer card transactions, not performing a HIPAA-covered function on behalf of Company, and is not functioning as a business associate even if Servicer has access to "individually identifiable health information" or "protected health information" as defined in HIPAA. The Healthcare Administration Services are, and some other Payment Navigator Services such as customer support may be, considered business associate services as defined in HIPAA. With respect to any business associate services, the business associate agreement ("**BAA**") found at Appendix B will apply. Company agrees that the BAA applies only to those Payment Navigator Services provided by Servicer that are business associate services, and not any Healthcare Payment Processing Services or other financial services provided by Servicer under the Agreement.

1. **Payment Navigator License Grant.** Servicer grants to Company a nonexclusive, nontransferable license (without a right of sublicense) to access and use, as applicable, the Payment Navigator application services and documentation exclusively for Company's internal business use to receive the Payment Navigator Services. Company acknowledges and agrees that it has no right in or license grant to any source code contained in or related to Payment Navigator pursuant to this Chapter.

2. **Payment Navigator Application Services Restrictions.** Company will not, and will ensure that its employees, agents, contractors, and vendors do not:

   a. Copy (other than maintaining one backup or archival copy for Company's internal business use only), re-sell, republish, download, frame or transmit in any form or by any means Payment Navigator, or any part thereof;

   b. Rent, lease, subcontract, operate or otherwise grant access to, or use for the benefit of, any third party, Payment Navigator;

   c. Decompile, disassemble, reverse engineer or translate Payment Navigator;

   d. Change, modify, alter or make derivative works of Payment Navigator;

   e. Without Servicer's prior written consent, grant any third party access to the computers, hardware, system or equipment on which Payment Navigator is accessible, provided, however, that only written notice (not consent) will be required with respect to billing services organizations acting as Company's agent for the collection of patient accounts;

   f. Attempt to interfere with or disrupt Payment Navigator or attempt to gain access to any other services, hardware, or networks owned, maintained or operated by Servicer or its suppliers;

   g. Disclose any passwords or other security or authentication device with respect to Payment Navigator to any person other than the person to whom it was issued;

   h. Remove, conceal or alter any identification, copyright or other proprietary rights notices or labels on Payment Navigator;

   i. Directly or indirectly, ship, export or re-export Payment Navigator;

   j. Directly or indirectly resell or re-offer Payment Navigator; or

   k. Act as a gateway through which a third party may gain access to the Payment Navigator Services.

3. **Payment Navigator Implementation.** Company will, at its own expense, pay for any preparation of its facilities necessary for it to access and use Payment Navigator in connection with this Chapter.

4. **Use of Payment Navigator by Third Parties**. Company may allow one or more third parties to access and use Payment Navigator, but only for Company's benefit and in connection with Company's internal business operations and activities, including access to and use of Payment Navigator from backup equipment at a secure off-site backup location and for testing purposes, subject to the restrictions of this Chapter and provided such third parties have agreed to be bound by the licensing terms and restrictions of this Chapter.

5. **Upgrades.** Servicer will make available to Company any updates, upgrades or modifications to Payment Navigator that Servicer generally makes available to its other customers, and each such update, upgrade or modification will be deemed to be part of Payment Navigator and will be governed by the terms of this Chapter.

6. **Termination of Payment Navigator Services.** Upon Termination of the Payment Navigator Services, Company's license to access and use Payment Navigator will terminate.

7. **Settlement of Transactions**. Transactions settled via the Healthcare Payment Processing Services provided under this Chapter are "net" settled as that term is described in Chapter 2 of the Operating Guide.

HEALTHCARE ADMINISTRATION SERVICES

The terms of this Section apply to Company's use of any of Healthcare Administration Services that Company has elected to receive.

1. **Termination.** The Healthcare Administration Services may be terminated by Servicer upon 30 calendar days' prior written notice if Servicer no longer has the rights to license Payment Navigator.

2. **Expenses and Reimbursement for Third Party Transaction Charges**. Company will, at its own expense, pay for any preparation of its facilities necessary for the implementation of, access to and use of the Healthcare Administration Services. Company will reimburse Servicer for all third-party Transaction charges incurred by Servicer in connection with healthcare claim data and other Transaction data and Transactions submitted by Company in connection with the Healthcare Administration Services (the "**Third Party Costs**"). For the avoidance of doubt, the parties intend that Company will reimburse Servicer for any Third Party Costs imposed on, or incurred by, Servicer in processing Transactions through third parties where such third parties will charge Servicer a fee to process Company's Transactions, such as Transactions destined for the following: Medicare, Medicaid and other government or government-related payers; most Blue Cross Blue Shield plans; some non-participating commercial plans; and all Transaction submissions that cannot be completed electronically and must be submitted and processed and otherwise "dropped" to paper. Please note that the fees for Healthcare Administration Services will include all known Third Party Costs as of the effective date of Company's use of the Healthcare Administration Services.

3. **Pass Through for any Future Taxes/Levies**. Any applicable sales tax, use tax, duty, tariffs, levies or other governmental charge arising from the sales, export, import or use of Payment Navigator in connection with the Healthcare Administration Services (other than taxes levied on the income of Servicer) and any related interest and penalties resulting from any payments made under this Section will be the responsibility of Company and will be paid by Company in the ordinary course and on a timely basis.

4. **Business Associate Agreement**. In connection with its performance of the Healthcare Administration Services, Servicer will have access to "protected health information" as defined in HIPAA. Accordingly, the terms of the BAA set out in Appendix B apply to Company's use of the Healthcare Administration Services.

5. **Terms of Payment**. Servicer will invoice Company on a monthly basis for the Healthcare Administration Services. Company will pay the amounts indicated on such invoice no later than thirty (30) days after the date of such invoice.

Chapter

26

Gateway Services

This Chapter describes the Gateway Services available to Companies. In addition to the requirements set forth in the Agreement and other applicable procedures set forth elsewhere in the Operating Guide, Companies that use the Gateway Services will adhere to the requirements set forth in this Chapter.

DESCRIPTION OF THE GATEWAY SERVICES AND FUNCTIONALITY

The following Services are the "**Gateway Services**:"

1. General.

a. The Gateway Services will support Payment Device authorization data and facilitate the transmission of authorization and settlement information related to Transactions to and from various Origination Points (e.g., POS Devices or other integrations) used by Company. A list of Payment Devices and Transaction types supported by the Gateway Services is available from Servicer upon request. Company must obtain and maintain certification from Servicer, as set forth in this Chapter, with respect to each supported Payment Device that Company wants to accept.

b. The Gateway Services include a browser-based user interface operated by Servicer and located at the URL designated by Servicer (the "**Service Web Site**"), that provides Company with the functionality for batch management, settlement balancing, and research and reporting of Transactions. System reporting will be available to all Authorized Users via secure password and log-on access. The Service Web Site application features and services available to Company vary depending on the Gateway Services used by Company.

c. The Gateway Services will submit Transactions received from an Origination Point in accordance with this Chapter for authorization to the Destination Point designated by Company, and will return to the Origination Point the authorization response message received from such Destination Point.

2. Settlement Functions.

a. The Gateway Services will facilitate the following settlement functions in connection with Transactions:

i. Upon Servicer's receipt through the Gateway Services of a settlement file from Company, the Gateway Services will initiate the transfer of the settlement file to the designated Destination Point(s) for Company's Transactions. Company understands that Servicer receives the settlement file from Company as-is for transmission to the designated Destination Point(s) and Company hereby agrees that Servicer will not be responsible for the content or accuracy of the settlement file Company provides except that Servicer will accurately communicate the settlement file to the Destination Point(s) as received from Company. In no event will Servicer be responsible for the content or accuracy of Transactions received from Company, and Servicer will not be responsible for the actions or inactions of the designated Destination Point(s) regarding processing the settlement file or any Transactions.

ii. Within one business day of receiving written notice from Company of a Transaction settlement discrepancy (which notice must include details of the asserted discrepancy), Servicer will initiate an investigation, make a preliminary assessment of the situation and recommend a plan for resolution to Company to resolve the discrepancy.

b. Company is responsible for reconciling settlement on a daily basis to ensure proper transmission and deposit of funds. If Company discovers a discrepancy in Transaction settlement batch amounts, interchange rates, late fees or any other element during Company's daily reconciliation process, Company must notify Servicer in writing (via email to gatewaysupport@Servicer.com) and provide supporting detail within two business days of the expected funding of the affected settlement file. Servicer will not be responsible for any damages, costs, claims, fees, fines or penalties suffered by Company, even if resulting from errors caused by the Gateway Services, if Company does not satisfy the obligations contained in this Chapter.

GATEWAY SERVICES GENERAL TERMS AND CONDITIONS

The following terms and conditions apply to the Gateway Services:

1. Gateway Services and Hosted System.

a. **Company Access to and Use of Gateway Services and Hosted System.** Servicer grants Company the right to access and use the Hosted System and Gateway Services as provided in this Chapter. Specifically, subject to the terms, conditions and limitations set forth in this Chapter, Servicer grants Company a limited, revocable, non-exclusive, non-assignable, non-transferable right in the Territory during the term to

i. use the Gateway Services to exchange information with the Hosted System, and

ii. access and use the Service Web Site solely for Company's own internal business purposes in accordance with the terms and conditions of this Chapter.

All such access and use of the Gateway Services and the Hosted System will be from systems and facilities located within the Territory.

b. **Servicer Certification.** In order to provide Gateway Services with respect to a certain Destination Point, Servicer must be certified with that Destination Point for the applicable Gateway Services and Transactions requested by Company. Company acknowledges that

i. all Gateway Services may not be available for all Destination Points, and

ii. Servicer may not be certified with, or remain certified with, each Destination Point in order to provide the Gateway Services in connection with or to submit Transactions to that Destination Point.

Where Servicer is the Destination Point, Servicer will remain certified to provide the Gateway Services and to submit Transactions to itself as the Destination Point.

c. **Updates.** Servicer may provide Updates to the Gateway Services, the Hosted System and applicable Servicer materials from time to time. Any such Update will be provided to Company at no additional cost, provided that such Update is provided to other Servicer merchants generally at no additional cost.

d. **Hosting Facilities.** As further described herein, Servicer will:

i. host the Gateway Services and Gateway Data at a facility operated by or on behalf of Servicer;

ii. maintain the operation, communications infrastructure, and security of such facility in accordance with this Chapter; and

iii. provide access to and use of the Gateway Services and Gateway Data by Company under the terms of this Chapter.

e. **Settlement Funds.** Servicer has no responsibility for Company's receipt of settlement funds in connection with any Transaction pursuant to this Chapter, whether or not the Transaction or other data in connection with such Transaction was transmitted through the Gateway Services. It is Company responsibility to reconcile funds received in settlement of Transactions against actual Transaction activity, including any Transaction Receipts transmitted using the Gateway Services. Further, Servicer has no responsibility under this Chapter for the characterization or classification of any Transaction by any Transaction Processor or Payment Services Entity for interchange or other fee purposes.

f. **Monitoring.** Company acknowledges and agrees that the Gateway Services may allow Servicer to monitor access to the Gateway Services and Hosted System and to prohibit any access or use of data or information within the Gateway Services and Hosted System that Servicer reasonably believes is unauthorized, may violate Law or Payment Network Regulations or that may pose an unacceptable risk of material harm to Servicer, other Servicer Companies or the Hosted System. Servicer has no obligation to detect or prevent, and will not be liable for failing to detect or prevent, any unauthorized access to or use of the Gateway Services using any password or user ID assigned to or by Company.

g. **Company Location Set-up and Boarding.** Company will cooperate with Servicer in the Company Boarding and the Company Validation Process and provide to Servicer all specifications, information and data required by Servicer in the process of assimilating the information and data necessary to confirm that the Hosted System and each Company Location and Origination Point are configured to make use of the applicable Services and to process Transactions through the Hosted System. Servicer is entitled to rely on the information provided by Company in connection with Servicer's set-up and boarding of a Company Location and Origination Point in the Hosted System and in Servicer's performance of the Gateway Services, including identification and set-up of Destination Points, Payment Services Entities, Company ID, Company category code, and any other information that may impact the Gateway Services or the processing of Transactions by Servicer or any Payment Services Entity. Company will notify Servicer of any changes to any Company Location information, including, without limitation, any Company ID, in writing at least ten (10) days prior to the effective date of such changes and will identify in the notice the date as of which Servicer should implement the change within the Hosted System. Servicer will use commercially reasonable efforts to implement any such changes in accordance with Company's reasonable instructions. In no event will Servicer be liable for any errors in the handling of Gateway Data, the processing of Transactions or in the performance of the Gateway Services that are attributable to (i) inaccurate or incomplete information or data provided by Company or (ii) Servicer's reliance upon Company's instructions with respect to Company Boarding.

h. **Demand Deposit Account.** Unless otherwise indicated in the Agreement, Servicer may debit any fees Company owes to Servicer via ACH or similar direct transfer from Company's DDA within 30 days of the occurrence of the Transaction or other event that caused such fees to be payable to Servicer, and Servicer will submit a statement showing the amounts owed and debited within 30 days of debiting any DDA. If invoicing is indicated in a schedule or addendum to the Agreement, instead of direct debiting of DDAs when fees are owed, Servicer will submit to Company an invoice for such fees owed by Company in connection with the Agreement on a monthly basis. Company will pay amounts reflected in such invoices within the time period set forth in the applicable schedule or the invoice.

i. **Conflict of Provisions.** The provisions of this Chapter will govern and prevail as to any purchase orders, statements of work or order forms signed in connection with this Chapter regardless of when signed.

2. Company Resources.

a. **Access to Gateway Services and Connectivity.** Company is responsible for implementing and maintaining Company's access to the Gateway Services and Connectivity, including with respect to all Company Connectivity Software, in accordance with Servicer's specifications and requirements. Company is responsible for the physical and technical security and safeguards for Company Resources and Connectivity. If Company is using a third party provider to host any of its equipment, resources or software necessary to access or interface with the Hosted System or Connectivity, or if Company will access the Gateway Services or transmit data to the Hosted System or the Connectivity through a third party hosting provider, Company will be responsible for compliance by that third party hosting provider with the terms and conditions of this Chapter and for the acts and omissions of that third party hosting provider.

b. **Gateway Data; Retention and Delivery.**

i. Servicer will not be liable for Company's use of Company's or a third party's telecommunications services and related networks, including failure of Connectivity or any erroneous transmission, corruption or loss of data, or inability to access the Gateway Services, the Hosted System, or Connectivity as a result of the failure of Company's or a third party's telecommunications systems, equipment, resources, or software. Servicer will not be responsible for the reconstruction of any information or data lost in transmission to or from the Hosted System due to any malfunction of Company's or Company's third-party service provider's systems. Company acknowledges that the ability of the Gateway Services to convert Gateway Data into formats that can be used by the Gateway Services, other Servicer service offerings, any Destination Point or any other Payment Services Entity is based on the integrity of the Gateway Data in its systems, and Servicer is not responsible for ensuring or verifying the accuracy of the content or format of any Gateway Data received by it.

ii. COMPANY ACKNOWLEDGES AND AGREES THAT THE GATEWAY SERVICES RELY ON THE DATA AND DIRECTIONS PROVIDED BY COMPANY AND ITS AUTHORIZED USERS. SERVICER DOES NOT GUARANTEE THE ACCURACY, COMPLETENESS OR ADEQUACY OF ANY DATA OR OTHER INFORMATION PROVIDED OR MADE AVAILABLE BY COMPANY OR ITS AUTHORIZED USERS, AND SERVICER WILL NOT BE LIABLE FOR ANY ERROR, OMISSION, DEFECT, DEFICIENCY, OR NONCONFORMITY IN DATA OR RESULTS OBTAINED THROUGH COMPANY'S USE OF THE SOFTWARE OR THE GATEWAY SERVICES, EXCEPT TO THE EXTENT CAUSED BY SERVICER'S BREACH OF THIS CHAPTER.

iii. Servicer may rely on instructions and approvals submitted by Company regarding access to and use of Gateway Data. Servicer will store and retain for 24 months Gateway Data, including Cardholder Data, received by Servicer in connection with Company's use of the Gateway Services. Company may view and retain certain Gateway Data stored by Servicer in accordance with the functionality of the applicable Gateway Services and the terms and conditions of this Chapter. The Gateway Services enable Company (and its Authorized Users) to view and transmit certain Gateway Data via the Service Web Site. If Company wants to access or receive copies of Gateway Data that is not accessible or downloadable via the Service Web Site, Company may request that Servicer provide such Gateway Data and Servicer will work with Company to provide such Gateway Data on mutually agreed upon terms, but Servicer will provide access to clear-text Cardholder Data only upon Company's execution of a completed clear card request form, which is available from Servicer upon request. Following the expiration of the term or the termination of this Chapter, if Company wants to access or receive copies of Gateway Data stored by Servicer, Company will be required to (a) enter into a data access agreement to be separately executed by the parties and (b) pay any fees imposed by Servicer in connection with such access.

iv. Subject to Servicer's obligations under this Chapter, Servicer will not be responsible for any Gateway Data that Company accesses or downloads from the Hosted System. Company will be responsible for maintaining "backups" of information and data (e.g., Transaction Receipts or

detailed reporting) as Company deems necessary in order to permit Company to reconstruct any information or data lost due to any malfunction of Company's or Servicer's systems, including the Gateway Services, the Hosted System or Connectivity.

v. The Gateway Services or the Hosted System may permit Authorized Users to send and receive Gateway Data to and from third parties in connection with the viewing and transmission of Gateway Data pursuant to this Chapter. Servicer does not regulate or track the viewing, transmittal or receipt of any data to or by such third parties and will not be liable or responsible for

1. the viewing or use of Gateway Data by a third party who has accessed or received such data (a) from Company or any Authorized User, or (b) using any user ID assigned to Company; or

2. Any transmission of Gateway Data outside of the Hosted System by Company, an Authorized User or any third party using any user ID assigned to Company or any Authorized User.

By transmitting any data to any third party or providing any third party with access to data, Company warrants that it has the right and authority to transmit or provide access to that data to each such third party.

3. **Confidential Information.** Irrespective of the confidentiality obligations set forth in the Agreement, Servicer will not be responsible for the confidentiality obligations of, or the maintenance of confidentiality of any information by, any Payment Services Entity (other than Servicer) or any other third party to whom Servicer may transmit information at the direction of Customer or as part of performing the Gateway Services.

4. **Effect of Termination or Expiration.** If the Gateway Services terminate or expire, all permissions granted to Company to use the Gateway Services will immediately cease, and Servicer may disable Connectivity and all access by Company and Authorized Users to the Gateway Services, any Service Web Site(s) and the Hosted System, including all user IDs and passwords. Upon Company's request, subject to Law and Payment Network Regulations, Servicer will forward all Gateway Data in Servicer's possession (except data contained in Servicer's backup files or required to be maintained under Law or otherwise permitted to be retained by Servicer under this Chapter) in the then-current format maintained by Servicer. Company will promptly pay Servicer all fees due to Servicer up to the effective date of termination or expiration. If Company continues accessing the Hosted System or using the Gateway Services following the expiration or the termination of this Chapter, Company will be subject to all of its duties and obligations under this Chapter consistent with such access or use, including Company's obligation to comply with Law and Payment Network Regulations and pay the fees and other amounts due to Servicer for such access and use, until Servicer or Company terminates such access and use.

CONNECTIVITY EQUIPMENT LOCATION TERMS

1. **Company Obligations**

a. Installation. Company hereby grants Servicer (or its designated subcontractor) the right to implement, configure, operate, and maintain the Connectivity Equipment at the Designated Space. Company will install, or cause to be installed, the Connectivity Equipment in the Designated Space after obtaining the appropriate instructions from Servicer for installation. The Implementation Date will be mutually agreed upon by the parties. Company acknowledges that the scheduled date for installation of the Connectivity Equipment and Implementation Date are of the essence and failure to meet the Implementation Date mutually agreed upon may cause delay in the provision of Connectivity by Servicer to Company.

b. Access. Company will provide, or cause to be provided to, Servicer (or its designated subcontractor) access to the Designated Space on a twenty-four (24) hour, seven (7) day a week, three-hundred-sixty-five (365) day a year basis in order to perform the Services, including, without limitation, access to

replace and remove Connectivity Equipment and to provide Maintenance Services. Notwithstanding the foregoing, Company acknowledges and agrees that implementation, set-up and initial configuration, support and maintenance for the Connectivity Equipment may be performed by Servicer (or its designated subcontractor) by remote access to the Connectivity Equipment unless otherwise agreed by the parties in writing. Onsite installation and configuration by Servicer of the Connectivity Equipment at the Designated Space may result in additional installation and services fees.

c. Company Cooperation. Company will provide to Servicer such information as Servicer may reasonably require in order to enable Servicer (or its designated subcontractor) to instruct Company (or its third party hosting provider) in the installation of the Connectivity Equipment, and to enable Servicer to operate and maintain the Connectivity Equipment at the Designated Space, including, without limitation, information on size limitations, power consumption levels, infrastructure support requirements and similar requirements. In addition to installation of the Connectivity Equipment by Company (or its third party hosting provider) at Servicer's instruction, at the request of Servicer, Company (or its third party hosting provider) will assist and cooperate with Servicer in performing light duties or correcting minor problems such as circuit problems and/or outages, which may include:

   i. Rebooting of equipment.

   ii. Pressing of reset or other readily accessible buttons or switches.

   iii. Reconfiguration of non-restricted cables with push-on type connectors.

   iv. Working cooperatively with Servicer and/or Servicer's designated subcontractors to locate and correct circuit problems.

d. Relocation of Connectivity Equipment. Company (or its third party hosting provider) will not arbitrarily or capriciously require Servicer to relocate the Connectivity Equipment; however, upon at least one hundred twenty (120) days' written notice or in the event of any emergency, Company may require Servicer to relocate Connectivity Equipment; provided however, the site of relocation will afford comparable space and environmental conditions for the Connectivity Equipment and comparable accessibility to the Connectivity Equipment. In the event that Company requires Servicer to relocate Connectivity Equipment, all reasonable costs incurred by Servicer associated with such relocation, and all costs incurred by Company, will be borne by Company. Company will notify Servicer in advance in writing of any changes to the infrastructure, power, cabling or electrical requirements, network connectivity or similar requirements of the Designated Space that may affect the maintenance or operation of the Connectivity Equipment.

2. **Designated Space.** Company (or its designated third party hosting provider, as applicable) will provide and maintain the Designated Space in a manner suited for proper storage and operation of the Connectivity Equipment with appropriate space, power and environmental controls to protect and preserve the Connectivity Equipment and in compliance with applicable city ordinances, building codes, and laws, including, without limitation: (i) A/C power to the outbound port on the Connectivity Equipment serving power distribution unit (PDU) 100% of the time; and (ii) HVAC (Heating, Ventilation and Air Conditioning) with industry standard target ambient room temperature and fire suppression measures in the area where the Connectivity Equipment is located. Company will further adhere to and enforce, and cause to be enforced at the Designated Space, those physical and logical security and access standards and monitoring practices regarding access to the Designated Space and Connectivity Equipment that Company applies to its own equipment and data centers, and no less than commercially reasonable industry standards, in order to maximize the security of the Designated Space and Connectivity Equipment.

3. **Connectivity Services**. Company will permit Servicer and each applicable telecommunications carrier to install circuits necessary to enable the operation of the Connectivity Equipment to receive data transmissions from Company and to transmit data in order to perform the Services. Company will cooperate with Servicer to notify Company's telecommunications carriers when Servicer wishes to terminate or modify circuits associated with the Connectivity Equipment and Connectivity. As between the parties, Company is responsible for providing all telecommunications and network connectivity, including,

without limitation, internet, local and long-distance telecommunications lines and any and all necessary cross-connects between the Company's systems and equipment and the Connectivity Equipment.

4. **Connectivity Equipment.** Company acknowledges and agrees that Company will have no right, title or interest (ownership or otherwise) in any of the Connectivity Equipment and will have no right to grant a security interest in or otherwise encumber any of the Connectivity Equipment or to cause or permit any Connectivity Equipment to become subject to any security interest, lien or encumbrance. The Connectivity Equipment will not be deemed or become fixtures of the Designated Space. During the Term, Servicer (or its designated subcontractor) will provide Maintenance Services for the Connectivity Equipment. Company will promptly notify Servicer at any time that Company becomes aware that any of the Connectivity Equipment is not operational or has been damaged or destroyed. Notwithstanding anything else to the contrary in this Chapter or the Agreement, Company will be liable and responsible for any loss, damage or destruction to the Connectivity Equipment or for repair and replacement costs relating to the Connectivity Equipment caused by the negligence or acts or omissions of Company, its employees, representatives or agents (including, without limitation, any third party hosting provider). Company will not remove, alter, deface or obscure any legends, notices, identification or identifications of ownership or any disclaimer of warranty or security or safety notices provided on or with the Connectivity Equipment. This is a services agreement and is not intended to and will not constitute a lease of any real or personal property. In particular, Servicer acknowledges and agrees that Servicer has not been granted any real property interest in the Designated Space, and Servicer has no rights as a tenant or otherwise under any real property or landlord/tenant laws, regulation or ordinances.

Chapter

27

Biller Direct Services

This Chapter describes the Biller Direct Services available to Companies. In addition to the requirements in the Agreement and other applicable procedures included elsewhere in the Operating Guide, Companies that select the Biller Direct Services will adhere to the requirements in this Chapter, the applicable Biller Direct Services Enrollment Form, and the applicable portions of the ECS MOG.

General Provisions Applicable to the Biller Direct Services

Overview of the Biller Direct Services. The "**Biller Direct Services**" are the electronic bill presentment and payment platform offered by Servicer pursuant to this Chapter that allows a Company to accept Payment Devices in an online, telephone or Integrated Point of Sale environment in connection with the Company's sale of goods or services or its receipt of bill payments.

1. **Transactions.**

   a. **Company Compliance**. Company's obligation to comply with Laws includes the obligation to comply with all requirements under the Electronic Signatures in Global and National Commerce Act in connection with the Biller Direct Services. Other than for Integrated Point of Sale Biller Direct Services, Company will not receive Transaction Information and therefore does not need to comply with the requirements governing Company receipt and handling of payment information from Customers when using Biller Direct Services.

   b. **Transaction Requirements**. Before Servicer processes a Transaction on Company's behalf, the Customer must affirmatively agree to engage in the Transaction through the Biller Direct Services web site, via the telephone, or in an Integrated Point of Sale environment.

      i. **Customer Authentication**. Company will provide to Servicer such Customer information as Servicer reasonably requests to perform their obligations under the Agreement and this Chapter.

         (1) If Company has selected Secure Handoff Customer authentication for the Biller Direct Services, Company will authenticate the identity of each Customer prior to allowing the Customer to access the Biller Direct Services to initiate a payment to Company. Servicer may rely on such authentication and the accuracy of the Customer information Company provides. Servicer will not be responsible for authenticating the Customer or for any Transaction (whether or not the result of fraud or other unauthorized access) processed with respect to a Customer that accesses the Biller Direct Services after a Company Secure Handoff.

         (2) If Company has selected Bill Load File Customer authentication for the Biller Direct Services, Servicer will authenticate the identity of each Customer on Company's behalf based solely on the Customer information Company provides and using the authentication criteria as Company directs. Servicer may rely on the accuracy of the Customer information

provided by Company, and Servicer will only be responsible for authenticating each Customer as directed by Company in writing.

(3) Company will be responsible for, and will indemnify Servicer against, any losses that may result from: (a) errors in the authentication of a Customer or in the processing of Transactions that result from incorrect Customer information provided to Servicer; and (b) inaccurate or incomplete authentication of a Customer that does not result from Servicer's errors or omissions. Company grants Servicer and its designated agents access to and use of Customer information and such other data as is necessary for Servicer to perform its obligations under this Chapter. Company represents that Company's provision of such Customer information to Servicer will not breach any agreement to which Company is a party or violate Laws.

ii. **Transaction Risk**. Servicer will attempt to collect from each Customer the payment-related information necessary for Servicer to process a payment Transaction from the Customer to Company in connection with the Biller Direct Services. Servicer will not be responsible for incomplete or inaccurate payment information that a Customer may provide in connection with the Biller Direct Services. Company acknowledges that additional Transaction verification and fraud prevention data elements and processes may be available through a particular Payment Network, including address verification, to reduce Transaction risk, and that Servicer will only be responsible for implementing any such Transaction risk controls that Company specifically requests in writing. The use of such Transaction risk controls does not constitute a guarantee of payment or prevent a Transaction from being disputed or subject to Chargeback. Regardless of any additional Transaction risk mitigation options Company elects, Company will remain responsible for monitoring Customer account activity for suspicious or fraudulent activity, as more fully described in Section 3 of the General Provisions of this Chapter.

c. **Transaction Controls**. Company will notify Servicer of any material change or anticipated material change in daily dollar activity or type of Transaction processing in connection with the Biller Direct Services, and Company will obtain Servicer's consent to any such change. Servicer will not be responsible for any losses or expenses incurred by Servicer or Company arising out of any material change or anticipated material change in Transaction activity that Company does not promptly report.

d. **Processing Limits**. Servicer may impose a limit on the aggregate dollar amount or individual dollar amount of Transactions that it will process for Company and may change the limit from time to time without prior notice to Company. If Company exceeds the established limit, Servicer may suspend the processing of Transactions in excess of the limit or may process Transactions in excess of the limit but hold the excess funds in a separate account or Reserve Account.

e. **Recurring Transactions**. For recurring Transactions (e.g., recurring or preauthorized payment of insurance premiums or subscriptions), the Customer must consent to the initiation of the recurring charges using the Customer's designated Payment Device. Servicer will not process recurring Transactions after Servicer receives (i) a cancellation notice from the Customer provided through the Biller Direct Services interface; (ii) a notice from Company through the Biller Direct Services interface that authority to accept recurring Transactions has been revoked; or (iii) a response from the issuer of a Payment Device that the Payment Device is not to be honored. If a Customer advises Company that the Customer wishes to revoke its recurring payments authorization, Company will immediately notify Servicer by cancelling the recurring payment instruction through the Biller Direct Services interface. Any notices that are not fully processed through the Biller Direct Services interface prior to 5:00 p.m. Eastern time one business day before the day a Transaction is scheduled to be processed will not affect that Transaction but will be effective for subsequent Transactions.

f. **Retrieval Requests and Chargebacks**. Company is responsible for all Retrieval Requests and Chargebacks under the Payment Network Regulations in connection with Transactions processed using the Biller Direct Services. Servicer will forward to Company any received Retrieval Requests or documentation related to a Chargeback from a Credit Card Association, an ECS Association or an EFT

Network. Company is responsible for appropriately responding to each Retrieval Request or Chargeback, including by retrieving a copy of the relevant Transaction Receipt from the Biller Direct Services interface. Company also will cooperate with Servicer to comply with the Payment Network Regulations regarding Retrieval Requests and Chargebacks.

2. **Biller Direct Services; Fees; Other Amounts Owed; Taxes**.

   a. **Implementation Fees**. Company acknowledges that Servicer will incur significant costs integrating Company's billing process with the Biller Direct Services. As a result, Company will pay to Servicer the implementation fee set forth on the Biller Direct Services Enrollment Form upon the effectiveness of this Chapter. Payment of the implementation fee is not contingent upon use of the Biller Direct Services, and Company will be responsible for payment of the full implementation fee regardless of whether Company discontinues implementation or use of the Biller Direct Services.

   b. **Billing**. Company acknowledges that the minimum annual Transaction fees it pays to Servicer for Transactions processed using the Biller Direct Services will be at least equal to the "Minimum Annual Fees" amount identified on the Biller Direct Services Enrollment Form. The Minimum Annual Fees requirement becomes effective on the first day of the first month that begins following the earlier of (i) the date Servicer processes the first Transaction for Company using the Biller Direct Services, or (ii) ninety (90) days from the effectiveness of this Chapter. For any partial period of less than a full calendar year, the actual amount of fees Company paid to Servicer for Transactions processed using the Biller Direct Services will be annualized to determine if Company has satisfied this obligation. At the end of each year (the first year beginning on the effective date of the Minimum Annual Fees requirement), Servicer may notify Company if the actual Transaction fees Company paid in respect of the Biller Direct Services are less than the Minimum Annual Fees amount. If Company's actual Biller Direct Services Transaction processing fees for such period are less than the Minimum Annual Fees, Company will promptly pay Servicer the difference.

3. **Fraud Controls and Responsibility for Fraud**. Company acknowledges that Servicer monitors Transactions systematically using fraud and risk parameters to minimize Servicer's financial exposure, and such monitoring may result in a financial benefit for Company. Servicer may suspend processing of Transactions or decline to process one or more individual Transactions if, based upon fraud detection and prevention controls or other security or Transaction verification or validation procedures, Servicer reasonably believes that such Transactions submitted to Servicer are the result of fraud or error. Servicer may suspend the disbursement of funds related to any Transaction for any reasonable period of time required to investigate suspicious or unusual Transaction or deposit activity and that Servicer will not be liable for any losses Company may attribute to a suspension of funds disbursement. Company will be responsible for all fraudulent Transactions unless such fraud results from Servicer's failure to authenticate a purported Customer as required under the Agreement using information provided to Servicer by Company under Section 1(b) of the General Provisions of this Chapter. Servicer may refer perpetrators of fraudulent Transactions to law enforcement officials.

4. **Suspension of Biller Direct Services**. Servicer may suspend Company's or a Customer's access to (or temporarily restrict the use of) the Biller Direct Services if Servicer determines there is a security, credit or legal risk that may interfere with providing the Biller Direct Services. Servicer may also permanently terminate a Customer's access to the Biller Direct Services upon notice to Company if Servicer reasonably determines the Customer is misusing the Biller Direct Services or is engaged in suspicious or illegal activity. Servicer may refuse any Transaction where Servicer reasonably believes that the Transaction involves a material probability of legal, fraud, or credit risk. Company will cooperate in resolving any claims or errors alleged by a Customer and in investigating any claims of fraud consistent with Laws and Payment Network Regulations.

PAYMENT CARD SERVICE PROVISIONS

1. **Authorization**. Servicer will attempt to obtain an Authorization Code before completing a Transaction. Servicer will only process Transactions that receive a positive authorization. An Authorization Code does not

   a. guarantee Company final payment for a Transaction;

   b. guarantee that the Transaction will not be disputed later by the Cardholder as all Transactions are subject to Chargeback;

   c. protect Company in the event of a Chargeback regarding unauthorized Transactions or disputes involving the quality of goods or services; or

   d. waive any provision of the Agreement or otherwise validate a fraudulent Transaction.

2. **Credit Transaction Receipt**. If Company agrees to grant a Cardholder a refund of a Payment Card Transaction processed by Servicer, Company will request a Credit Transaction Receipt through the Biller Direct Services interface and will issue the credit using the Credit Transaction Receipt. Company will not issue cash or a check as a refund for any previous Transactions processed on a Payment Card. Servicer will debit the DDA for the total face amount of each Credit Transaction Receipt Servicer processes. Servicer will not process a Credit Transaction Receipt relating to any Transaction Receipt that Servicer did not originally process, and Servicer will not process a Credit Transaction Receipt that exceeds the amount of the original Transaction Receipt.

3. **Interchange.** Servicer is not responsible for the Interchange category or pricing (including discount rate, fees and surcharges) applied by the Credit Card Associations, EFT Networks or otherwise owed by Company with respect to any Transaction processed using the Biller Direct Services, except to the extent that Company has to pay greater Interchange with respect to a Transaction solely because Servicer fails to comply with the Transaction processing requirements agreed to between Company and Servicer.

ECS AND ACH PROVISIONS

1. **General.** A Customer must provide authorization to Servicer before Servicer will initiate an ACH debit to the Customer's account, in accordance with the ECS MOG. Servicer will record the Customer's ACH debit authorization. Servicer will either retain the original or a duplicate record of the Customer's authorization for the period required by the applicable ECS Rules, and will make a copy of such record available to Company for a fee as indicated on the Biller Direct Services Enrollment Form.

2. **Additional Representations**. Company represents, with respect to all ECS and ACH Transactions accepted and processed by Servicer under this Chapter, that

   a. for prearranged payment or deposit (PPD) entries or recurring debit entries, the Customer has duly authorized the debiting of the Customer's account in writing in accordance with Laws and ECS Rules,

   b. the business transaction represents an obligation of the Customer who is initiating the ECS or ACH Transaction, and

   c. the ECS or ACH Transaction is for amounts actually owed by the Customer to Company (including tax) and does not involve any element of credit

Chapter

28

Equipment

PROVISIONS APPLICABLE TO RENTAL EQUIPMENT

This section describes certain terms and conditions that apply to Companies that have elected to receive Rental Equipment from Servicer. In addition to the requirements set forth in the Agreement and other applicable procedures set forth in the Operating Guide, Companies that receive Rental Equipment from Servicer will adhere to the requirements set forth in this Chapter. For the avoidance of doubt, the provisions of this Chapter will not apply to Leased Equipment.

Rental Term. Company agrees to the rental term and to pay the fees for Rental Equipment set forth in the Agreement. Company may terminate the rental term at any time upon written notice to Servicer, provided that rental payments will not be prorated. Company will pay the full monthly rental payment for each full or partial month until the Rental Equipment is returned to Servicer in good repair, condition and working order.

Ownership. Servicer will at all times retain title to the Rental Equipment. Company will not create, incur, assume or suffer to exist any mortgage, lien, pledge or other encumbrance or attachment of any kind whatsoever upon, affecting or with respect to the Rental Equipment.

Care and Use; Risk of Loss. Company will maintain the Rental Equipment in good operating condition, repair and appearance, and protect the same from deterioration other than normal wear and tear. Company will only use the Rental Equipment in the regular course of its business, and will comply with all laws, ordinances, regulations and rules with respect to Company's use, maintenance and operation of the Rental Equipment. Company will bear all risk of loss of and damage to the Rental Equipment while in Company's possession. In the event of a loss of, or damage to, the Rental Equipment, Company will pay to Servicer the then current full purchase price of the Rental Equipment.

Rental Equipment Replacement. Servicer will replace any inoperable or non-functioning Rental Equipment during the rental term; provided, that (i) such Rental Equipment is not inoperable or non-functioning due to any act of Company or any damage for which Company is responsible, (ii) Company has paid all rental payments due and owing to Servicer, and (iii) Company pays the standard swap fee for the shipping and handling of the replacement Rental Equipment. Rental Equipment replacement will constitute Company's sole remedy and Servicer's sole obligation with respect to any inoperable or non-functioning Rental Equipment.

Return of Rental Equipment. Within ten (10) days of the expiration or termination of the rental term, Company will return the Rental Equipment, freight prepaid, to Servicer in good repair, condition, and working order, ordinary wear and tear excepted, to a location designated by Servicer. If Company fails to return the Rental Equipment to Servicer within the time period specified, Company will pay to Servicer the then current full purchase price of the Rental Equipment.

PROVISIONS APPLICABLE TO APPLE, INC. EQUIPMENT

This section describes certain terms and conditions that apply to Companies that have received Apple, Inc. Equipment from Servicer.

Support. Servicer will provide Company with full support and assistance with any troubleshooting or any other help-desk function as may be needed or required in connection with Company's use of Apple, Inc. Equipment. Company may also purchase AppleCare to provide additional support for its Apple, Inc. Equipment, although Apple Care does not apply to any components used in connection with the Apple, Inc. Equipment that are not produced by Apple, Inc.

Warranty. Company understands and acknowledges that Apple, Inc., its officers, affiliates and subsidiaries make no warranties or endorsements with respect of Company's use of Apple, Inc. Equipment as a POS Device, nor any other POS Device, third-party product, or combination of any Apple, Inc. and any such third-party product or POS Device.

Chapter

29

Supplies

We can provide supplies necessary to complete your Card Transactions. To replenish your stock, go online to http://www.merchantconnect.com or select the “Supplies” option from the merchant services telephone menu. These supplies include:

- Card Transaction Receipts and Credit Transaction Receipts
- Imprinter
- Batch Header receipts and envelopes
- Company plate
- Electronic printer paper
- Stickers containing Voice Authorization numbers
- Visa and MasterCard window decals and cash register signs
- Quick Reference Guide (QRG) supporting your POS Device

We suggest that you check your supplies frequently to ensure you have an adequate quantity on site. Requesting a “rush” shipment will cause you to incur additional charges.

Chapter

30

MasterPass™ Wallet Services

Companies using the Converge Payment System also are enabled to participate in MasterCard's MasterPass™ digital wallet service, an integrated digital wallet platform designed and provided by MasterCard to enable customers to pay for goods and services in e-commerce transactions (the "**MasterPass Wallet Services**"). The MasterPass Wallet Services enable online acceptance of digital wallets that have integrated features, including (i) MasterCard's proprietary digital wallet product, which is an electronic means of storing and transmitting payment card and related information on behalf of a Cardholder, and (ii) third-party digital wallets that have integrated into MasterCard's MasterPass Wallet Services. By using the Converge Payment System and the integrated MasterPass Wallet Services, Company agrees to the terms and conditions set forth herein and to the terms and conditions MasterCard has established for its MasterPass Wallet Services in the MasterPass Operating Rules, currently available at https://masterpass.com/SP/Company/OperatingRules, as the same may be updated from time to time. Additional details regarding the operation and use of the MasterPass Wallet Services are set forth in the MasterPass Operating Rules and in related technical and operational specifications provided or made available by MasterCard.

Company agrees to maintain all MasterCard and MasterPass branding, trademarks, and logos in accordance with the MasterPass™ Company Branding Requirements, currently available at:

https://masterpass.com/SP/Merchant/OperatingRules

Chapter

31

PayPal Acceptance

Companies participating in our PayPal Program will be enabled to accept PayPal Payment Devices. All participating Companies will be able to accept PayPal Cards. Participating Companies utilizing compatible POS Devices may also accept PayPal Mobile Transactions.

TERMS APPLICABLE TO PAYPAL ACCEPTANCE

1. PayPal Marks. Company may use the PayPal Marks only to promote PayPal products, offers, services, processing and/or acceptance. Company use of the PayPal Marks is restricted to the display of decals, signage, advertising, and marketing materials provided or approved by PayPal in writing pursuant to the process set forth in the PayPal Program Documents. Company will not use the PayPal Marks in such a way that customers could believe that the products or services offered by Company are sponsored or guaranteed by the owners of the PayPal Marks. Company recognizes that it has no ownership rights in the PayPal Marks. Company will not assign to any third party any of the rights to use the PayPal Marks. Company is prohibited from using the PayPal Marks, not permitted by the PayPal Program Documents, unless expressly authorized in writing by PayPal. Company will only use and display the PayPal Program Marks in accordance with the PayPal Program Documents.
2. POS Devices. Company must ensure that it utilizes POS Devices capable of accepting PayPal Cards in accordance with the PayPal Program Documents.
3. Merchandise on Display; Inventory. Company must ensure that it has merchandise on display at the point of sale that is related and relevant to the MCC assigned to the Company, and that there is sufficient inventory on premises to transact business.
4. Evidence of Being an Operating Business. Company must provide to Servicer upon request such documentation reasonably required by Servicer to verify that Company is actually operating a business, such as bank or supplier documentation.
5. Telephone and Storefront. Company must maintain a working telephone and retail storefront.
6. Compliance with the PayPal Program Documents. Company must comply with all applicable terms of the PayPal Program Documents in the course of its participation in the PayPal Program, including the acceptance of PayPal Cards and/or PayPal Mobile Transactions.

Chapter

32

Additional Resources

Visit our web site at http://www.merchantconnect.com to obtain customer support, retrieve account information, order supplies, and more.

PAYMENT NETWORK COMPANY INFORMATION

For Payment Network-specific Company information, visit the following websites:

- American Express - http://www.americanexpress.com/merchantopguide
- Discover Network - http://www.discovernetwork.com/getstarted/merchant/merchant.html
- MasterCard - http://mastercard.com/us/merchant/index.html
- Visa - https://usa.visa.com/run-your-business/accept-visa-payments.html

For information regarding the operating rules and regulations of the various Payment Networks, visit the following websites:

- American Express - http://www.americanexpress.com/merchantopguide
- Discover Network - http://www.discovernetwork.com
- MasterCard - http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf
- Visa - http://usa.visa.com/merchants/operations/op_regulations.html

PCI DATA SECURITY STANDARDS INFORMATION

For PCI Data Security Standards information and requirements, visit the following websites:

- PCI Security Standards Council – https://www.pcisecuritystandards.org/#
- American Express - http://www.americanexpress.com/merchantopguide
- Discover Network - http://www.discovernetwork.com/fraudsecurity/disc.html
- MasterCard SDP -https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html
- Visa - https://usa.visa.com/support/small-business/security-compliance.html#3

Appendix

A

Glossary

ACH: Automated Clearing House, the funds transfer system governed by the rules of NACHA. ACH allows financial institutions to clear interbank entries electronically.

ACH Network: The funds transfer system governed by the ACH Rules. The ACH Network allows participating depository financial institutions to clear interbank entries electronically.

ACH Rules: The NACHA Operating Rules and Operating Guidelines, which govern the interregional exchange and settlement of ACH transactions.

ACS: See Automated Customer Service.

Activation Date: the date that Company activates the configuration and connection to the Connectivity in a production environment after installation of the Connectivity Equipment in the Designated Space.

Address Verification Service (AVS): A fraud-reduction service that allows the Company to verify a Cardholder's billing address prior to completing a Card Not Present Transaction.

Agreement: The Master Services Agreement, Payment Device Processing Agreement, or Terms of Service, as applicable, any addendum to the foregoing, the Company Application, this Operating Guide, any other guides or manuals provided to Company from time to time, and all additions to, amendments and modifications of, and all replacements to any of them.

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

Apple, Inc. Equipment: The Equipment produced by Apple, Inc. that is specified on Schedule A to the Payment Device Processing Agreement, an Additional Equipment Form, or any other form or Agreement and is obtained by Company from Servicer.

Approval Code: An Authorization Code indicating that the Transaction is approved and the Card may be honored.

Automated Customer Service (ACS): A desktop application used as a reporting and accounting reconciliation tool for viewing detailed reports of Transaction activity, statement detail, Card type history, and qualification detail.

Authorization: A required procedure by which a Company requests approval of a Transaction from the Issuer. Authorization is initiated by accessing the authorization center by telephone or POS Device. See also *Magnetic Swipe Authorization*, *Manual Entry Authorization*, or *Voice Authorization.*

Authorization Code: The code sent by the Issuer in response to an Authorization request that indicates whether the Transaction is approved. Responses may include: "Approved," "Declined," "Declined Pick-Up," or "Referral" ("Call Auth").

Authorization Code: The code sent by the issuer of a Payment Card in response to an authorization request (the procedure by which Servicer requests approval of a Transaction involving a Payment Card from the issuer of the Payment Card), which indicates whether the Transaction is approved by the issuer.

Autofax: A program offered to Companies for receiving Retrieval Request and Chargeback notices via a dedicated 24-hour fax line.

AVS: See Address Verification Service.

Balance: The amount of money owed by the Cardholder to the Issuer for charges on a Credit Card. On a Debit Card this is the amount of money available in the Cardholder's demand deposit or savings account

Bank Identification Number (BIN): The identification number assigned to a Member that is used for Card issuing, Authorization, clearing, and Settlement processing.

Bankruptcy Proceeding: With respect to a Person means (i) that the Person or any subsidiary of such Person will: (a) commence a voluntary case under the Bankruptcy Code of 1978, as amended, or other federal bankruptcy laws (as now or hereafter in effect); (b) file a petition seeking to take advantage of any other applicable laws, domestic or foreign, relating to bankruptcy, insolvency, reorganization, winding up or composition or adjustment of debts or any other similar conservatorship or receivership proceeding instituted or administered by any regulatory agency or body; (c) consent to or fail to contest, in a timely and appropriate manner, any petition filed against it in an involuntary case under such bankruptcy laws or other applicable laws; (d) apply for or consent to, or fail to contest in a timely and appropriate manner, the appointment of, or the taking of possession by, a trustee, receiver, custodian, liquidator, or similar entity of such Person or of all or any substantial part of its assets, domestic or foreign; (e) admit in writing its inability to pay its debts as they become due; (f) make a general assignment for the benefit of creditors; (g) make a conveyance fraudulent as to creditors under any applicable law; or (h) take any action for the purpose of effecting any of the foregoing; or (ii) that a case or other proceeding will be commenced against the Person or any subsidiary of such Person in any court of competent jurisdiction, or through any regulatory agency or body, seeking: (a) relief under the Bankruptcy Code of 1978, as amended, or other federal bankruptcy laws (as now or hereafter in effect) or under any other applicable laws, domestic or foreign, relating to bankruptcy, insolvency, reorganization, winding up or composition, or adjustment of debts; or (b) the appointment of a trustee, receiver, custodian, liquidator or the like of such Person or of all or any substantial part of the assets, domestic or foreign, of such Person or any other similar conservatorship or receivership proceeding instituted or administered by any regulatory agency or body.

Batch: The accumulated Card Transactions stored in the POS Device or Host computer.

Batch Header: A summary, similar to a deposit slip, of a group of Card Transactions accepted by a Company who does not process Transactions electronically. It is attached to the Transaction Receipts when they are sent to the paper processor.

Bill Load File: A file of data in a Biller Direct Services-specified format that is provided by Company to Servicer via data transmission or upload to the Biller Direct Services platform on a regularly scheduled basis. The data passed to the Biller Direct Services platform will include information used to identify the Customer, amount due, and other data relevant to the effective processing of the Transaction.

Bill Payment: PIN-less Debit Card payment Transactions resulting in funds transfer from Cardholders to Companies in connection with payments for recurring services (excluding casual or occasional purchases) for which a corresponding invoice is periodically presented to the Cardholder by the Company, and which Transaction is initiated via a telephone (Voice Recognition Unit, Interactive Voice Recognition) or Internet device.

BIN: See Bank Identification Number.

Business Associate: Has the meaning ascribed to it in HIPAA.

Business Associate Agreement: A contract between a Business Associate and a covered entity as required by HIPAA.

Card: A plastic card issued by a bank or other financial institution, or by a Card company (e.g., Discover Network, Visa and MasterCard Credit Cards and Debit Cards), that allows a Cardholder to pay for purchases by credit, charge, or debit.

Cardholder: the individual in whose name a Payment Device has been issued and any authorized user of such Payment Device.

Cardholder Information Security Program (CISP): The data security regulations required by Visa to protect Cardholder account data and other data security best practices. The exact requirements for CISP can be found at www.visa.com/cisp.

Card Identification Number (CID) or Card Validation Code (CVV2/CVC2): A number printed on a Card and used as additional verification for Card Not Present Transactions. For American Express this is a four-digit code printed above the Card account number. For Visa, MasterCard and Discover Network this is a three-digit card code value printed on the signature panel of the Card.

Card Imprint: See Imprint or Imprinter.

Card Not Present: The processing environment where the Payment Device is not physically presented to the Company by the Cardholder as the form of payment at the time of the Transaction. Card Not Present includes, but is not limited to, Mail Order (MO), Telephone Order (TO), and Electronic Commerce (EC).

Card Present: The processing environment where the Payment Device is physically presented to the Company by the Cardholder as the form of payment at the time of Transaction.

Card Rules: The Credit Card Rules and Debit Card Rules, collectively.

Card Validation Code: See Card Identification Number.

Cash Advance: A Transaction in which a Cardholder receives cash from a financial institution or an ATM.

Chargeback: A Transaction disputed by a Cardholder or Issuer pursuant to the Payment Network Regulations.

Chip: A microchip that is embedded in a Card that contains Cardholder data in an encrypted format.

Chip and PIN Technology: Any technology in whatever form introduced by any Payment Network which employs Chip embedded Cards and/or the use of a PIN in conjunction with, or in replacement of, a manual signature of Cardholder.

Chip Card: A Card embedded with a Chip that communicates information to a Chip-Reading Device.

Chip-Reading Device: A POS Device capable of reading, communicating and processing Transaction data from a Chip Card.

CID: See Card Identification Number.

Code 10 Authorization: An Authorization or an "additional verification step" obtained for a suspicious or questionable Transaction, Card, or Cardholder.

Company: The business entity that provides goods and/or services to Customers (formerly referred to as "**Merchant**", or, with respect to Gateway Services, "**Customer**")).

Company Application: The Company Application and any additional document containing information regarding Company's business that is submitted to Servicer in connection with Company's application for the Services, including documents submitted by Company as a part of the bid process, if applicable.

Company Connectivity Software: any software provided by or on behalf of Company, whether integrated at Company's or a third party hosting or service provider's operating environment, and the associated interfaces and data collection routines implemented by or on behalf of Company to access and use the Gateway Services, including plug-ins, agents, and operating system components.

Company Identification Card: A plastic card issued to the Company that contains the Merchant Identification Number, name, location, and DDA number.

Company Location: a designated location at which a Company uses the Gateway Services.

Company Plate: A plastic or metal plate affixed to the Imprinter that contains Company information such as the Company name, MID, city and state, and a Discover or American Express account number, if applicable.

Company Statement: A monthly summary of activity in a Company account.

Compliant Chip Card: A Chip Card that complies with all Payment Network Regulations.

Connectivity: the Servicer-controlled non-public network connectivity and interfaces for transmitting data between the Origination Point and the Hosted System.

Connectivity Equipment: all computer router equipment, accessories, peripherals, software and other materials provided by Servicer that are designated on a schedule or addendum to the Agreement to be installed in the Designated Space and provide Connectivity, and shall include replacement or updated equipment as may be provided by Servicer from time to time during the Term of the Agreement.

Contactless: A payment card or key fob equipped with a chip and antenna that securely communicates Cardholder account information via radio frequency to a POS Device.

Convenience Fee: A fee charged by Company for an added convenience to the Cardholder for the use of a Payment Device in a Transaction in accordance with the Payment Network Regulations.

Converge Services: The delivery of payment acceptance and processing services by Servicer through Servicer's Converge interface in accordance with this Operating Guide and the Converge documentation provided by Servicer to Company, as the same may be updated by Servicer from time to time.

Copy Request: See Retrieval Request.

Coverage Area: The geographic area in which wireless Transaction processing is available to Company.

Credit Card: A card or device associated with a revolving line of credit that may be used to purchase goods and services from Company or to pay an amount due to Company or to obtain cash advances. A "Credit Card" includes any of the following cards or devices that are associated with a line of credit extended to the Person to whom the card or device is issued: (i) a Visa card or other card or device bearing the symbol(s) of Visa U.S.A., Inc. or Visa International, Inc. (including Visa Gold cards); (ii) a MasterCard card or other card or device bearing the symbol(s) of MasterCard International Incorporated (including MasterCard Gold cards); (iii) a Discover Network card or other card or device bearing the symbol(s) of Discover Network; or (iv) any card or device bearing the symbol of any other Credit Card Association.

Credit Card Associations: (i) Visa; (ii) MasterCard; (iii) American Express; (iv) Discover Network; (v) Diners Club International Ltd.; (vi) JCB International Co., Ltd.; (vii) China UnionPay Co., Ltd; and (viii) any other organization or association that hereafter contracts with Servicer to authorize, capture, and settle Transactions effected with Credit Cards issued or sponsored by such organization or association, and any successor organization or association to any of the foregoing.

Credit Card Rules: All applicable rules and operating regulations of the Credit Card Associations, and all rules, operating regulations, and guidelines for Credit Card Transactions issued by Servicer from time to time, including, without limitation, all amendments, changes and revisions made thereto from time to time.

Credit Transaction Receipt: A document, in paper or electronic form, evidencing a Company's refund or price adjustment to be credited to the Cardholder's account and debited from the Company's DDA. This is also known as a credit slip or credit voucher.

CVV2/CVC2: See Card Identification Number.

Customer: A client of Company who elects to conduct a payment Transaction with Company through presentation of a Payment Device (including a Cardholder) or who participates in Company's Fanfare Loyalty Program.

Customer Data: Any information or data related to a Customer, including personal information, personally identifying information and information about a Customer's purchase Transactions at Company, collected by Company and provided to Servicer or received by Servicer from a Customer in connection with the Fanfare Loyalty Program or Servicer's provision of the Fanfare Loyalty Services.

DDA: See Demand Deposit Account.

Debit Card: A card or device bearing the symbol(s) of one or more EFT Networks or Credit Card Associations, which may be used to purchase goods and services from Company or to pay an amount due to Company by an electronic debit to the Cardholder's designated deposit account. A "Debit Card" includes (i) a card or device that bears the symbol of a Credit Card Association and may be used to conduct signature-based, offline debit Transactions, and (ii) a card or device that bears the symbol of an EFT Network and can be used to conduct PIN-based, online debit Transactions.

Debit Card Rules: All applicable rules and operating regulations of the EFT Networks and Credit Card Associations, and all rules, operating regulations, and guidelines for Debit Card Transactions issued by Servicer from time to time, including, without limitation, all amendments, changes, and revisions made thereto from time to time.

Declined Code: An Authorization Code indicating that the Transaction is declined and the Card is not to be honored

Declined Pick-Up Code: An Authorization Code indicating that the Transaction is declined and the Card should be retained by the Company.

Demand Deposit Account: The commercial checking account at a financial institution acceptable to Servicer designated by Company to facilitate payment for Transactions, Chargebacks, returns, adjustments, fees, fines, penalties, and other payments due under the Agreement. In the instance of a Debit Card or ATM Card, this refers to the Cardholder's deposit account.

Designated Space: the location on the premises of Company (or its third party hosting provider) at which the Connectivity Equipment is installed.

Destination Point: a location of a Payment Services Entity designated by Company with respect to which Company has requested Servicer to provide the Gateway Services or to which Company has requested Servicer submit Transactions.

Diners: Diners Club International Ltd.

Discount: A type of fee paid by a Company to process its Card Transactions. Discount is calculated by multiplying the Discount rate by the volume of Card Transactions.

Discover: DFS Services LLC.

Discover Network: The payment network operated and maintained by Discover.

Doing Business As (DBA): The trade name of a Company that may appear on business signs, customer literature, or other documents.

Domestic Internet PIN-Based Debit Card Transaction: A PIN-based Transaction conducted over the internet using a Debit Card and processed over an EFT Network.

Dynamic Currency Conversion (DCC): The conversion of the purchase price of goods or services from the currency in which the purchase price is displayed to another currency as agreed to by the Cardholder and Company. That currency becomes the Transaction currency, regardless of the Company's local currency.

EBT: See Electronic Benefits Transfer Service.

EBT Card: A card utilized for electronic benefits transfers.

ECS: See Electronic Check Service.

ECS Association: NACHA, any regional ACH association or network, and any other organization or association used by Servicer or Member in connection with the ECS that is hereafter designated as an ECS Association by Servicer from time to time.

ECS Rules: All applicable rules and operating regulations of or applicable to the ECS Associations (including the ACH Rules) and the ECS MOG, in each case including without limitation, all amendments, changes, and revisions made thereto from time to time.

EFT Networks: (i) Interlink Network Inc., Maestro U.S.A., Inc., STAR Networks, Inc., NYCE Payments Network, LLC, PULSE Network LLC, ACCEL/Exchange Network, Alaska Option Services Corporation, Armed Forces Financial Network, Credit Union 24, Inc., NETS, Inc., SHAZAM, Inc., and Interac and the Interac Direct Payment service; and (ii) any other organization or association that hereafter authorizes the Servicer or Member to authorize, capture, and/or settle Transactions effected with Debit Cards, and any successor organization or association to any of the foregoing. For purposes of Chapter 2, heading Special Requirements Applicable to Internet PIN-Based Card Transactions, ETF Networks will only include networks in the United States.

EGC: See Electronic Gift Card.

EGC Cardholder Data: One or more of the following data elements pertaining to a Cardholder's account: Electronic Gift Card number, Cardholder name (if applicable), Electronic Gift Card account activity, Cardholder account balance, and such other data applicable to the Company's EGC program.

Electronic Benefits Transfer Service (EBT): A service that allows electronic transfer of government funds to individuals through the use of a plastic debit-like Card and a Personal Identification Number (PIN). The federal government requires all states to distribute food stamps and cash benefits in this manner. The EBT Card may then be used for qualified purchases at company locations.

Electronic Check Service (ECS): The service offering by Servicer pursuant to which Transactions effected via an ACH Payment Device are presented for clearing and settlement through the ACH Network or alternate clearing channel as described in the ECS Merchant Operating Guide (ECS MOG).

Electronic Commerce Transaction: A Transaction that occurs when the Cardholder uses the Internet to make a purchase from a Company or Company uses the Internet to submit the Transaction for processing.

Electronic Gift Card (EGC): A special stored value card provided by or on behalf of Company that is redeemable for merchandise, services or other Transactions.

Electronic Gift Card (EGC) Services: Services provided by Servicer that allow a Company to sell Electronic Gift Cards redeemable for in-store merchandise or services.

Embossing: The process of printing data on a Card in the form of raised characters so the Card may be used in the imprinting of Transaction Receipts.

Encryption: A security or anti-fraud technique that scrambles data automatically in the POS Device before the data is transmitted. For example, PINs are encrypted when transmitted for Authorization.

Equipment: All equipment identified on Schedule A (Schedule of Fees) to the Agreement, including: (i) for Satellite Services, satellite communication services equipment, and VSATs; (ii) for SmartLink Services, SmartLink payment gateway devices; or (iii) for Voyager Card Acceptance or Wright Express Card Acceptance, Fleet terminals.

Factoring (Laundering): Processing Transactions for another person or business through a Company's account.

Fanfare Basic Registration: A Customer's completion of registration in Company's Fanfare Loyalty Program at the Company's Fanfare Loyalty Website in which the Customer does not elect to permit Servicer to communicate with the Customer about products and services outside of Company's Fanfare Loyalty Program.

Fanfare Enrolled Customer: A Customer of Company that has enrolled to participate in Company's Fanfare Loyalty Program.

Fanfare Full Registration: A Customer's completion of registration in Company's Fanfare Loyalty Program at the Company's Fanfare Loyalty Website in which the Customer elects to permit Servicer to communicate with the Customer about products and services outside of Company's Fanfare Loyalty Program.

Fanfare Gift Card: A special card, code or device purchased by or provided to a Customer (including any promotional card, code or device) that is redeemable for merchandise, services or other Transactions with Company.

Fanfare Gift Card Program: A program established and managed by Company using the Fanfare Platform in accordance with the Agreement and the Operating Guide.

Fanfare Gift Card Services: Fanfare Gift Card Program setup and Services provided by Servicer to Company as described in the Agreement and the Operating Guide.

Fanfare Loyalty Card: A plastic card obtained from Servicer and branded with the Company's logo displayed within one of Servicers pre-defined styles, which card is encoded with a magnetic stripe for use with Company's Fanfare Loyalty Program.

Fanfare Loyalty Program: A program established and managed by Company, using the Fanfare Platform, through which Company may endeavor to promote Customer loyalty and increased spending by offering promotions, rewards and incentives to Fanfare Enrolled Customers.

Fanfare Loyalty Program Account: The Fanfare Loyalty Program account established within the Fanfare Platform for each Fanfare Enrolled Customer, which account may be managed by the Fanfare Enrolled Customer through the Fanfare Loyalty Website when such Fanfare Enrolled Customer becomes a Fanfare Registered Customer.

Fanfare Loyalty Services: A loyalty program platform that supports Company establishment of a Fanfare Loyalty Program, Customer enrollment in the Fanfare Loyalty Program, establishment and maintenance of the Fanfare Loyalty Website, the ability to generate marketing campaigns and offer promotions to Customers, and Services related to redemption of Customer rewards, in each case as more fully described in the Agreement and the Operating Guide.

Fanfare Loyalty Website: A Customer-facing website hosted by Servicer and co-branded by Servicer (Fanfare) and Company through which (i) Customers that have not enrolled in Company's Fanfare Loyalty Program may enroll online as part of the registration process, (ii) Fanfare Enrolled Customers may access Company's Fanfare Loyalty Program disclosures, (iii) Fanfare Enrolled Customers may un-enroll in the Fanfare Loyalty Program, or (iv) Registered Customers may manage their Fanfare Loyalty Program Accounts, in each case as more fully described in the Agreement and the Operating Guide.

Fanfare Platform: The systems hosted directly or indirectly by Servicer through which (i) Company establishes its Fanfare Loyalty Program and/or Fanfare Gift Card Program, and (ii) the Fanfare Services are provided to Company.

Fanfare Registered Customer: A Fanfare Enrolled Customer that has also completed Fanfare Basic Registration or Fanfare Full Registration at Company's Fanfare Loyalty Website.

Fanfare Services: The Fanfare Loyalty Services and/or Fanfare Gift Card Services provided by Servicer and used by Company in accordance with the Agreement and the Operating Guide.

Fanfare Web Portal: A web-based portal provided by Servicer through which Company may obtain information and guides pertaining to the Fanfare Services and Fanfare Platform, and may access Company-specific program metrics via dashboards, view information about a Customer's purchase Transactions at Company, create additional Customer offers and retrieve reports regarding Company's Fanfare Gift Card Program and/or Fanfare Loyalty Program, in each case as applicable to the Fanfare Services elected by Company hereunder.

Gateway Data: all Cardholder Data and Transaction Information provided to Servicer by or on behalf of Company in order for Servicer to provide the Gateway Services.

Healthcare Payer: Any third party administrator, payer of healthcare benefits and healthcare-related payments, health plan or self-insured entity that remits a payment to Company in connection with the Transend Pay Services.

High-Risk Payment Service Provider: A Payment Service Provider that facilitates Transactions on behalf of high-risk Sponsored Companies, as specified in Chapter 19 of this Operating Guide.

HIPAA: The Health Insurance Portability and Accountability Act of 1996.

Hologram: A three-dimensional image included on a Card to discourage counterfeiting.

Host: The central server we use to store Company information and to route information between the Company and the Issuers.

Hosted System: the Servicer proprietary switch technology, operating systems and software platform operated by Servicer for the Gateway Services.

Implementation Date: the date that Servicer has notified Company the Connectivity Equipment is available for configuration and activation with the Connectivity.

Imprint: The physical impression made from a Card on the Transaction Receipt, which may be used to prove that the Card was present when the sale was made.

Imprinter: A device used by Companies to make an Imprint on a Transaction Receipt.

Integrated Point of Sale: A Company-operated Point of Sale environment that is integrated with Servicer's Biller Direct Services offering

Interac: Interac Association.

Interac Online: The service provided by Interac to permit Customers to pay for goods and services over the Internet and directly from the Customer's bank account.

Interac Online Rules: All applicable rules and operating regulations of the Acxsys Corporation, including, but not limited to, the Interac Online Functional Specifications, the Interac Online Operating Regulations, the Interac Online Customer Service Rules, and the Interac Online By-laws, the Trade-mark License Agreement, the Canadian Code of Practice for Consumer Protection in Electronic Commerce (http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00064e.html) and any other directive, guideline or policy passed by resolution and promulgated by the Acxsys Corporation and all applicable federal and provincial laws, and all rules, operating regulations, and guidelines for Interac Online Transactions issued by Servicer from time to time, including, without limitation, all amendments, changes, and revisions made thereto from time to time.

Interchange: The clearing and settlement system for Visa and MasterCard Credit Cards and Debit Cards and, where applicable, Discover Network Credit Cards and Debit Cards, where data is exchanged between the Servicer and the Issuer.

Interchange Fees: The amount paid by the Servicer to the Issuer on each Transaction. Interchange Fees vary according to the type of Company and the method of processing.

International Credit Card: A Credit Card issued for acceptance on or accessible through an International Network.

International Debit Card: A debit card or device bearing the symbol(s) of one or more International Networks, which may be used to purchase goods and services from Company or to pay an amount due to Company by an electronic debit to the Cardholder's designated deposit account.

International Debit Card Transaction: A PIN-based Transaction conducted over the internet using an International Debit Card and processed over an International Network.

International Internet PIN-Based Card Transaction: An International PIN-Based Credit Card Transaction or an International Debit Card Transaction.

International PIN-Based Credit Card Transaction: A PIN-based Transaction conducted over the internet using an International Credit Card and processed over an International Network.

International Network: An organization or association based outside the United States and that operates or sponsors a payments network, with respect to which Servicer is authorized, directly or indirectly, to process, capture, and/or settle Transactions effected with Payment Devices issued or approved for use on the payments network operated or sponsored by such organization or association.

International Network Requirements: All applicable rules and operating regulations of the International Networks, including, without limitation, all amendments, changes, and revisions made thereto from time to time. References to "Payment Network Regulations" in the Operating Guide will be understood to include International Network Requirements.

Internet Payment Screen. The screen displayed to a Cardholder during an Internet PIN-less Bill Payment Transaction payment process which allows the Cardholder to select the payment method and to confirm understanding and agreement with payment terms, shipping and return policy.

Internet PIN-Based Card Transaction: A Domestic Internet PIN-Based Debit Card Transaction or an International Internet PIN-Based Card Transaction.

Internet PIN-Based Card Transaction Documentation: The rules, regulations, and guidelines for Internet PIN-Based Card Transactions issued by Servicer from time to time, as amended, revised, or supplemented.

Internet PIN Pad: A secure program that displays and **allows** entry on a virtual numeric keyboard that conforms with the applicable Card Rules and/or International Network Requirements and the PCI Data Security Standard, and requirements established from time to time by Servicer, and through which a Cardholder may enter a PIN.

Issuer: The financial institution or other entity that issued the Credit Card or Debit Card to a Cardholder.

JCB: JCB International Co., Ltd.

Laundering: See Factoring.

Laws: All applicable local, state, and federal statutes, regulations, ordinances, rules, and other binding law in effect from time to time.

Leased Equipment: The Equipment specified in the Agreement that is leased from Servicer pursuant to the terms of such Agreement. For the avoidance of doubt, Rental Equipment does not constitute Leased Equipment.

Loyalty Card: A device used to hold a currency or points value in a stored value program.

Magnetic Stripe: A stripe of magnetic material affixed to the back of a Card that contains Cardholder account information.

Magnetic Swipe Authorization: An electronic Authorization request generated when a Company swipes the Cardholder's Card through the POS Device. The POS Device reads the Cardholder information from the Magnetic Stripe on the Card and then dials out to the Authorization Center to obtain an Authorization Code.

Mail Order/Telephone Order (MO/TO) Transaction: For MO, a Transaction that occurs when the Cardholder uses the mail to make a payment to a Company and for TO, a Transaction that occurs when the Cardholder uses a telephone to make a payment to a Company.

Maintenance Services: the routine support and maintenance services provided by Servicer (or its designated subcontractor) for the Connectivity Equipment.

Manual Entry Authorization: An Authorization request generated when the Company key-enters the Cardholder's Card number, expiration date, and sales amount into the POS Device (e.g., when the POS Device is unable to read the Cardholder information from the Magnetic Stripe on the Card). The POS Device then dials out to the appropriate Authorization Center to obtain an Authorization Code.

Master Account: The account (e.g. funds pool) used to hold the value of Electronic Gift Cards that have been issued among a group or chain of Companies; alternatively, this may refer to the back-up account used to offset electronic payment, ACH or Canadian Payments Association rejects, if applicable.

MasterCard: MasterCard International Incorporated.

Member: A financial institution designated by us that is a principal, sponsoring affiliate or other member of Visa, MasterCard or other member of the applicable Payment Network. The Member may be changed by Servicer at any time and the Company will be provided notice of same.

Merchant Category Code (MCC): The four-digit code and corresponding definition assigned to each Company that describes the type of business in which the Company is engaged.

MerchantConnect: A Web-based Transaction reporting and reconciliation system used to manage Transaction data from multiple locations or multiple merchant accounts via any standard Web browser (e.g., Internet Explorer).

Merchant Identification Number (MID): A unique identification number assigned to a Company to identify its business.

MO/TO: Mail Order/Telephone Order.

Model Documents: A sample set of customer terms and conditions and a privacy policy provided by Servicer to Company for Company's use in developing its own Customer-facing terms and conditions and privacy policy governing Customer participation in the Fanfare Loyalty Program.

Multi-Currency Pricing (MCP): A Transaction in which Company displays the price of goods or services in a currency other than, or in addition to, Company's local currency. No Dynamic Currency Conversion (DCC) is conducted.

NACHA: The national association that establishes standards, rules, and procedures governing the ACH Network, including the ACH Rules.

Negative Deposit: When the dollar amount of Credit Transaction Receipts exceeds the dollar amount of Transaction Receipts submitted for processing.

No Signature Required Program: A specific program offering by a Credit Card Association that includes required criteria that must be met by the Company in order to submit No Signature Required Transactions and obtain some protection from Chargebacks.

No Signature Required Transaction: A Card Transaction that does not require Company to obtain a Cardholder signature on a Transaction Receipt because the Company and the Transaction satisfy the requirements of a No Signature Required Program.

Operating Guide: Servicer's Operating Guide (formerly the "Merchant Operating Guide" or "MOG"), located at www.merchantconnect.com (or such other website that Servicer may specify), that prescribes rules and procedures Transactions and Company's use of the Services. Servicer may amend the Operating Guide from time to time, which amendments will be effective upon notice to Company.

Origination Point: either (i) the Company central origination location that transmits data between the Company and the Hosted System or (ii) if the Company is integrated with the Gateway Services directly, the point-of-sale (POS), property management system (PMS), terminal central location, equipment or system from which the Company transmits data to or receives data from the Hosted System.

Payment Card: A Credit Card, Debit Card or Prepaid Card, as the context requires.

Payment Card Industry (PCI) Data Security Standard: The data security regulations, including maintaining Cardholder account data in a secure environment, and other data security best practices endorsed by the major card associations including Visa and MasterCard, as such may be amended from time to time. Visa requires that Companies and their agents comply with CISP and MasterCard requires that Companies and their agents comply with SDP.

Payment Device: Any device or method used for the purpose of obtaining credit or debiting a designated account including a Credit Card, Debit Card, and any other financial transaction device or method, including an Electronic Gift Card, check (whether converted into electronic form or used as a source document for an electronic fund transfer), EBT Card, stored value card, "smart" card, or other device created to be used for the purpose of obtaining credit or debiting a designated account.

Payment Network: Any Credit Card Association, EFT Network, ECS Association or automated clearing house association, governmental agency or authority, and any other entity or association that issues or sponsors a Payment Device or PayPal Payment Device or operates a network on which a Payment Device is processed.

Payment Network Regulations: The rules, operating regulations, guidelines, specifications and related or similar requirements of any Payment Network.

Payment Service Provider: A company that is registered by Servicer or Member with the Payment Networks to facilitate Transactions on behalf of Sponsored Companies.

Payment Services Entity: any third party (which may include Servicer if Company has engaged Servicer to provide Payment Device or Transaction processing services) that Company has designated as a Destination Point for receipt of Transactions and to which Servicer is certified to submit Transactions, including but not limited to, Transaction Processors, Payment Networks, third party service providers, program managers and other third parties associated with Payment Device acceptance or other programs of Company.

PayPal: PayPal, Inc.

PayPal Card: A valid payment card bearing the PayPal logo that is linked to a Customer's account with PayPal. Company may accept PayPal Cards in the same manner as any Credit Card.

PayPal Marks: The brands, emblems, trademarks, and/or logos that identify acceptance of PayPal Payment Devices. The PayPal Marks are described in Appendix A of the PayPal Operating Regulations.

PayPal Mobile Transaction: A term used to encompass the various means by which a Customer with a PayPal account may initiate a Transaction with a Company utilizing an application on the Customer's mobile device that is linked to the Customer's account with PayPal. PayPal Mobile Transactions are described in further detail in the PayPal Program Documents.

PayPal Payment Devices: PayPal Cards and PayPal Mobile Transactions.

PayPal Program: The program through which Companies may accept PayPal Payment Devices.

PayPal Program Documents: The PayPal Operating Regulations, the PayPal Dispute Rules Manual, and the PayPal Technical Specifications, including all appendices, exhibits, and attachments.

Person: Any individual, firm, corporation, business trust, partnership, governmental agency or authority, or other entity and will include any successor (by merger or otherwise) of such entity.

Personal Identification Number (PIN): A number that must be entered by a Cardholder in order to complete certain types of Transactions (e.g., online debit, EBT).

Petroleum Services: Services provided by Servicer to Companies engaging in Transactions related to petroleum products or services, including Satellite Services, SmartLink Services, Voyager Card Acceptance, and Wright Express Card Acceptance.

PIN: See Personal Identification Number.

PIN Pad: A secure device with an alphanumeric keyboard which conforms with the Debit Card Rules and applicable standards administered by the Payment Card Industry Security Standards Council, and requirements established from time to time by Servicer, and through which a Cardholder may enter a PIN.

POS Device: A terminal, software or other point-of-sale device at a Company location that conforms to the requirements established from time to time by Servicer and the applicable Payment Network.

Pre-authorized Order: A written or electronic authorization by a Cardholder allowing a Company to charge his or her Card at a future date.

Prepaid Card: A card having available funds paid for in advance by the Cardholder.

Primary Company: The Merchant Identification Number (MID)/location originally enrolled for Electronic Gift Cards and set up to be billed for the card orders placed or designated as the corporate or headquarter location.

Priority Check-Out and Express Return Service: A Visa service provided by lodging Companies, hotels, cruise lines, or car rental companies that allows a Cardholder to authorize the use of their Card for payment of the total obligation to the Company, with or without prior knowledge of the total amount, by signing a completed agreement.

Program: The processing services and other related products and services received by Company pursuant to the Agreement.

Proper Authorization: Receipt of an authorization approval code by use of a POS Device or the telephone authorization center provided for authorization referrals.

Quasi-Cash Transactions: Transactions representing a Company's sale of items that are directly convertible to cash.

Recurring Payments: A Transaction charged to the Cardholder (with prior written or electronic permission to a Company) on a periodic basis for recurring goods and services (e.g., monthly membership fees, utility bills, subscriptions).

Referral Code: An Authorization Code indicating that the Issuer is requesting that the Company call the Voice Authorization Center, which will either provide an Approval Code or ask the Company to request additional information from the Cardholder (e.g., mother's maiden name).

Remittance Data: Remittance information that is (i) supplied by a Healthcare Payer to Company, and (ii) connected to each of the payments made to Company by a Healthcare Payer via the Transend Pay Services.

Rental Equipment: The Equipment specified on Schedule A (Schedule of Fees) to the Agreement or an Additional Equipment Form that is rented by Company from Servicer on a month-to-month basis. For the avoidance of doubt, Leased Equipment does not constitute Rental Equipment.

Reserve Amount: The amount established pursuant to the calculation set forth in the Agreement.

Retrieval Request: A request initiated by a Cardholder or Issuer that requires the Company to produce a legible copy of the Cardholder's signed Transaction Receipt within a specified period of time.

Satellite Services: Satellite operations for electronic payment processing including but not limited to Payment Card Transactions, provision of the space segment, and Equipment maintenance services.

Secure Handoff: A data string in a Biller Direct Services-specified format that is passed securely to the Biller Direct Services platform after Company's authentication of a Customer on Company's website. The data passed to the Biller Direct Services platform includes information used to identify the payer, amount due, and other data relevant to the effective processing of the Transaction.

Service Provider: any entity that stores, processes, transmits or accesses Cardholder Data or Transaction Information on behalf of Company or that provides software to Company for transaction processing, storage, or transmission, except to the extent such services are performed by the entity in its capacity as a third-party contractor of Servicer performing Servicer's obligations under the Agreement.

Servicer: The entity that processes Transactions on behalf of the Company.

Servicer Debit System: Servicer's electronic Debit Card Transaction processing system for provision of Debit Card authorization, data capture, and settlement services.

Settlement: The process of submitting Transactions to the Servicer for processing.

Site Data Protection Program (SDP): MasterCard's data security regulations to protect Cardholder account data and other data security best practices. The exact requirements for SDP can be found at https://sdp.mastercardintl.com.

SmartLink Services: Internet based operations for electronic payment processing utilizing Equipment or Software, and including Software support and Equipment maintenance services.

Software: The software identified on Schedule A (Schedule of Fees) to the Agreement, including for SmartLink Services, SmartLink Access Module or other programs supplied by Servicer and used for Internet-based electronic payment processing.

Split Sale: A prohibited process by which Companies use multiple Transaction Receipts to avoid Authorization for a single Transaction.

Sponsored Company: A company that, pursuant to an agreement with a Payment Service Provider, is authorized to accept Payment Devices when properly presented.

Sponsored Company Agreement: An agreement between a Payment Service Provider and a Sponsored Company which will be in a form disclosed to, and approved by Servicer and Member.

Supported Hardware: The equipment, systems and hardware, including POS Devices, necessary for Company to make use of the Company's selected Fanfare Services.

T&E Company: A Company whose primary function is to provide travel and entertainment related services.

Transaction: Any action between Company and a Cardholder using a Payment Device that results in activity on the Cardholder's account (e.g., payment, purchase, refund, or return).

Transaction Data: All data regarding the Transaction including, without limitation, the Cardholder account number, dollar amount of the Transaction, and the information stored in the Card's Magnetic Stripe.

Transaction Date: The date that a Transaction occurs.

Transaction Processor: service bureaus and other Persons that provide transaction processing services, including authorization and settlement services, to Company. The authorization services may support processing of credit, debit, check or other types of transaction services as may be available through the Gateway Services. In order to provide Gateway Services with respect to a Transaction Processor designated by Company for a Company Location, Servicer must be certified with the selected Transaction Processor for the applicable Gateway Services.

Transaction Receipt: The paper or electronic record evidencing the purchase of goods or services from, or payment to, a Company by a Cardholder using a Payment Device.

Transend Pay Services: Certain Services provided by Servicer to Companies in connection with Companies' receipt of healthcare-related and benefit payments from a Healthcare Payer, as more fully described in the Agreement.

Transend Pay Services Website: A Company-facing website hosted by Servicer's vendor through which Company can access Remittance Data.

UnionPay: China UnionPay Co., Ltd.

Visa: Visa U.S.A., Inc.

Voice Authorization: An Authorization process whereby a Company calls the Voice Authorization Center and provides Cardholder and purchase information over the telephone. The Voice Authorization Center then provides an Authorization Code to the Company.

Voice Authorization Center: The center that conducts Voice Authorization for Card Transactions.

Voyager Card Acceptance: The program whereby Company may accept Voyager® commercial fleet cards.

VSAT: Very Small Aptitude Terminal.

Wireless POS Device: A POS Device that allows wireless processing.

Wireless Services: The wireless data services used by Company to submit Transactions at Wireless POS Devices to Servicer in accordance with the requirements set forth in the Operating Guide.

Wright Express Card Acceptance: The program whereby Company may accept Wright Express commercial fleet cards.

Appendix

B

Business Associate Agreement

1) **DEFINITIONS.** Capitalized terms used and not otherwise defined herein have the meanings ascribed to them in the Agreement or the Operating Guide. The following terms used in this BAA have the same meaning as those terms in HIPAA: Breach; Designated Record Set; Disclosure; Health Care Operations; Individual, Minimum Necessary; Notice of Privacy Practices; Required by Law; Secretary; Security Incident; Subcontractor; Unsecured Protected Health information; and Use.
   a) "**Agreement**" means the Master Services Agreement, Payment Device Processing Agreement, or Terms of Service, as applicable, between Company and Elavon under which Elavon is providing services that require the execution of a business associate agreement under HIPAA. The term Agreement will not include any arrangements or agreements for services that are exempted from HIPAA's business associate agreement requirements because they are described in Section 1179 of HIPAA, including without limitation the remainder of the Master Services Agreement, Payment Device Processing Agreement, or Terms of Service, as applicable.
   b) "**Business Associate**" means U.S. Bank National Association and Elavon, Inc.
   c) "**Covered Entity**" means the Company selecting the Payment Navigator Services, and, if applicable, any and all affiliates listed as Affiliated Entities under the Agreement for which Business Associate is providing services that require the execution of a Business Associate Agreement under HIPAA.
   d) "**Disclose**" and "**Disclosed**" means, as appropriate, the present or past release, transfer, provision of access to, or divulging of information outside the entity holding such information.
   e) "**HIPAA**" means the Standards for Privacy and Security of Individually Identifiable Health Information at 45 CFR part 160 and part 164.
   f) "**Protected Health Information**" has the same meaning as the term "Protected Health Information" in 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity in connection with services that require the execution of a Business Associate Agreement under HIPAA.

2) **OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.**
   a) Business Associate agrees not to Use or Disclose Protected Health Information other than as permitted or required by the Agreement, this BAA, or Required by Law.
   b) Business Associate agrees to use appropriate safeguards to prevent the Use or Disclosure of the Protected Health Information other than as provided for by this BAA. With respect to any and all electronic Protected Health Information, Business Associate agrees to comply with Subpart C of 45 CFR part 164 and implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic Protected Health Information it receives, maintains, or transmits on behalf of Covered Entity.
   c) Business Associate agrees to report to Covered Entity within 15 days any Use or Disclosure of Protected Health Information not provided for by this BAA of which it becomes aware, including Breaches of Unsecured Protected Health Information as required by 45 CFR §164.410, and any Security Incident. For the purposes of this reporting requirement, a Security Incident will not include inconsequential incidents that occur on a daily basis such as scans or "pings" that are not allowed past Business Associate's or its Subcontractor's firewall.

d) Business Associate agrees to ensure that any Subcontractor to whom it provides Protected Health Information agrees in writing to the same restrictions and conditions with respect to such information that apply through this BAA to Business Associate.
e) Upon reasonable notice, Business Associate agrees to make Protected Health Information and books and records relating to the Use or Disclosure of Protected Health Information available to the Secretary in a reasonable time and manner, for purposes of the Secretary determining Covered Entity's compliance with HIPAA.
f) Business Associate agrees to document Disclosures of Protected Health Information to the extent required for Covered Entity to respond to a request by an Individual for an accounting of Disclosures of Protected Health Information in accordance with 45 CFR § 164.528. Business Associate agrees to provide to Covered Entity, in a reasonable time and manner, information collected in accordance with this paragraph to the extent required to permit Covered Entity to respond to the Individual's request for an accounting. Business Associate will refer to Covered Entity all requests by Individuals for information about or accounting of Disclosures of Protected Health Information. The parties agree to work together in good faith to resolve any disagreement over the requirements of 45 CFR § 164.528.
g) Business Associate agrees to provide access to Covered Entity of Protected Health Information maintained in a Designated Record Set to enable Covered Entity to meet the requirements of 45 CFR § 164.524. Business Associate agrees to make any amendments to Protected Health Information in a Designated Record Set that Covered Entity agrees to pursuant to 45 CFR § 164.526. If Business Associate receives a request from an Individual for a copy of his or her Protected Health Information or to amend his or her Protected Health Information, Business Associate will forward each such request to Covered Entity within five business days to enable Covered Entity to respond to the Individual's request.

3) **PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.**
a) Except as otherwise provided in this BAA, Business Associate may Use or Disclose Protected Health Information to perform functions, activities, or services for, or on behalf of Covered Entity, provided that the Use or Disclosure would not violate HIPAA if undertaken by Covered Entity and is consistent with applicable Minimum Necessary requirements of HIPAA.
b) Business Associate may Use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of Business Associate.
c) Business Associate may Disclose Protected Health Information for the proper management and administration of Business Associate, provided that the Disclosures are Required by Law, or that Business Associate obtains reasonable assurances from any person to whom the information is Disclosed that (i) such information will remain confidential and be Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and (ii) that the person will notify the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
d) Business Associate may Use and Disclose Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

4) **OBLIGATIONS OF COVERED ENTITY.**
a) Covered Entity will notify Business Associate of any changes in Covered Entity's notice of privacy practices that may affect Business Associate's Use or Disclosure of Protected Health Information. Business Associate will have a reasonable period of time to act on such notice.
b) Covered Entity will provide Business Associate with any changes in, or revocation of, permission by an Individual to Use or Disclose Protected Health Information, if such changes affect Business Associate's permitted or required Uses and Disclosures thereof. Business Associate will have a reasonable period of time to act on such notice.
c) Covered Entity will notify Business Associate of any restriction on the Use or Disclosure of Protected Health Information prior to acceptance of such restriction by Covered Entity in accordance with 45 CFR § 164.522 so that Business Associate can determine whether it is feasible to comply with such restriction. Once agreed to, Business Associate will have a reasonable period of time to act on such notice.
d) Covered Entity will not Disclose any Protected Health Information to Business Associate unless Covered Entity has obtained any consents and authorizations that may be Required by Law or otherwise necessary for such Disclosure.
e) Covered Entity will not use the names or any trademark or tradename of Business Associate in any written

or oral communication to the public, including any notices provided under HIPAA, without the advance written consent of an authorized representative of Business Associate, which consent will not be unreasonably withheld or delayed.

5) **TERM AND TERMINATION.**
   a) This BAA will be effective as of the effective date of the Agreement, and will terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.
   b) Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity will provide an opportunity for Business Associate to cure the breach in accordance with the Agreements. Covered Entity may terminate this BAA and the Agreement between Covered Entity and Business Associate which is the subject of any material breach of this BAA by Business Associate if Business Associate does not cure the breach as provided in the Agreement. If Business Associate has breached a material term of this BAA and cure is not possible, Covered Entity may immediately terminate this BAA. This provision will be in addition to and will not limit any rights of termination or obligations set forth in the Agreement.
   c) Except as otherwise provided in this BAA, upon termination of this BAA for any reason, Business Associate will return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. Except as otherwise provided in this BAA, Business Associate will retain no copies of the Protected Health Information.
   d) If Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate will notify Covered Entity of the conditions that make return or destruction infeasible, extend the protections of this BAA to such Protected Health Information, and limit further Uses and Disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible for so long as Business Associate maintains such Protected Health Information.

6) **CHANGE IN LAW.** The parties acknowledge that amendments to applicable law may necessitate future changes to this BAA. In such event, the parties agree to negotiate in good faith toward a written amendment to comply with applicable law.

7) **MISCELLANEOUS.**
   a) The terms of this BAA are in addition to any agreement that Covered Entity has with U.S. Bank National Association or Elavon, Inc., including the Agreement. The provisions of this BAA will supersede the provisions of the Agreement only to the extent the provisions herein are inconsistent with the Agreement, and in all other respects, the Agreement will remain in full force and effect. Further, this BAA will supersede in its entirety any existing Business Associate Agreement or addendum between the parties with respect to the Agreement.
   b) Covered Entity represents and warrants that: (i) it is a duly authorized agent of the entities it listed as Affiliated Entities to the Agreement and it is signing for itself and on behalf of those entities in its authorized capacity; (ii) it has taken all action required by all relevant organizational documents to enter into this BAA for itself and on behalf of all its Affiliated Entities; and (iii) each entity listed Affiliated Entity is a covered entity as defined under 45 CFR § 160.103. This BAA will be null and void with respect to any entity listed as an Affiliated Entity that does not meet, or ceases to meet, the definition of a covered entity under HIPAA, or to which Business Associate is not providing services that require a Business Associate Agreement under HIPAA.