CARD ACCEPTANCE GUIDE

Released July 2015
This Guide contains information protected by copyright. No part of this material may be duplicated, reproduced or disclosed in any form without prior written consent from Global Payments.

The information contained in this guide is proprietary and confidential to Global Payments and merchants who have executed an Agreement with Global Payments for card payment services.

Global Payments reserves the rights to add, modify, update, or cancel any and all provisions described in this Guide as it deems appropriate, from time to time, with or without advance notice.

You are responsible for ensuring that you obtain and are using the most up to date copy of the Guide.

For the latest version of this guide, please visit our Web site:

globalpaymentsinc.com/canada

This Guide is part of your Merchant Agreement with Global Payments Direct, Inc. (hereinafter referred to as “Global Payments” or “Global”) and you must follow the instructions and procedures in this Guide to comply with your agreement.
Your Global Payments Merchant Number

Global Payments’ Customer Care Centre Telephone Number

Your Global Payments Sales Representative Telephone Number

Authorization Telephone Number
1.800.268.8241

For more information on additional products and services from Global Payments, contact 1.800.263.2970 or visit our website at:
globalpaymentsinc.com.canada

Please refer to the American Express OptBlue Program Merchant Guide: www.americanexpress.ca/optblueguide

For more information about VISA®, MasterCard®, American Express®, Interac® Direct Payment, Discover® or UnionPay® please visit the applicable websites at:
www.visa.ca
www.mastercard.com.canada
www.americanexpress.com.canada
www.interac.ca
www.discover.com
en.unionpay.com
Global Payments — Your Advocate in Payment Processing…… 1
Our Role ........................................................................................................... 1
Your Role ....................................................................................................... 1
Need Assistance? ....................................................................................... 2

Introduction ....................................................................................................... 3
The Parties Involved in the Transaction......................................................... 3
How the Transaction Process Works ............................................................... 5
Our Business Model ........................................................................................ 5

Retention of Sales Drafts .............................................................................. 9

Protecting Cardholder Privacy ..................................................................... 11

Data Security Standard (PCI DSS) ................................................................. 13
Qualified Security Assessors (QSA) ............................................................... 13
Third Party Service Providers ................................................................. 14
Third Party Payment Applications ............................................................... 14
Merchant Levels and Validation Requirements ............................................. 14

Operating Procedures ................................................................................... 19
General ........................................................................................................ 19
Proper Use of Marks .................................................................................. 20
Proper Display of Signage ........................................................................ 20
Card Acceptance Restrictions ................................................................ 20
Sales Procedures – EMV Chip .................................................................... 23

Other Important Facts ................................................................................ 25
Sales Procedures – Contactless (proximity) ................................................ 25
Sales Procedures – Credit ........................................................................... 26
Sales Procedures – VISA Easy Payment Service ...................................... 26
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express No Signature Program</td>
<td>27</td>
</tr>
<tr>
<td>Electronic Data Capture Merchants</td>
<td>28</td>
</tr>
<tr>
<td>Processing Paper Drafts</td>
<td>32</td>
</tr>
<tr>
<td>Using the Imprinter</td>
<td>33</td>
</tr>
<tr>
<td>Authorizations</td>
<td>34</td>
</tr>
<tr>
<td>Code 10 Authorization</td>
<td>34</td>
</tr>
<tr>
<td>Sales Procedures – <em>Interac</em> Direct Payment (Debit)</td>
<td>35</td>
</tr>
<tr>
<td>Depositing Your Sales Drafts</td>
<td>37</td>
</tr>
<tr>
<td>Returns and Exchanges</td>
<td>38</td>
</tr>
<tr>
<td>UnionPay (UP) Card Transactions</td>
<td>40</td>
</tr>
<tr>
<td>Delayed Sales</td>
<td>40</td>
</tr>
<tr>
<td>“Card Not Present” Transactions</td>
<td>41</td>
</tr>
<tr>
<td>Forgotten Credit Cards</td>
<td>47</td>
</tr>
<tr>
<td>Month-End Settlement Adjustments</td>
<td>48</td>
</tr>
<tr>
<td><strong>Other Available Services</strong></td>
<td>49</td>
</tr>
<tr>
<td>Tele-Deposit</td>
<td>49</td>
</tr>
<tr>
<td>Pay@Pump</td>
<td>49</td>
</tr>
<tr>
<td>Push Funds</td>
<td>50</td>
</tr>
<tr>
<td>Lodging Merchant Procedures</td>
<td>51</td>
</tr>
<tr>
<td><strong>Draft Retrieval Requests</strong></td>
<td>53</td>
</tr>
<tr>
<td>Sample Sales Draft Retrieval Request</td>
<td>53</td>
</tr>
<tr>
<td><strong>Chargebacks</strong></td>
<td>55</td>
</tr>
<tr>
<td>Examples</td>
<td>55</td>
</tr>
<tr>
<td>Precautions</td>
<td>57</td>
</tr>
<tr>
<td>Your Right to a Rebuttal</td>
<td>58</td>
</tr>
<tr>
<td>How to Help Reduce Chargebacks</td>
<td>58</td>
</tr>
<tr>
<td><strong>Special Sale Circumstances</strong></td>
<td>61</td>
</tr>
<tr>
<td>Mail Orders, Telephone Orders and Internet Orders</td>
<td>61</td>
</tr>
</tbody>
</table>
# Table of Contents

**POS Solutions** ................................................................................................. 63  
POS Solutions and Security .................................................................................. 63  
Communication Lines ......................................................................................... 63  
Supplies .................................................................................................................. 64  
VISA and *Interac* Supplies .................................................................................. 64

**Understanding Your Statement** ........................................................................ 65  
Questions about Your Statement .......................................................................... 65  
Sample Statement ................................................................................................. 66

**Customer Service** ............................................................................................. 69  
Dispute Resolution ................................................................................................. 69

**Card Acceptance Best Practices** ...................................................................... 73  
Working Together to Prevent Fraud ...................................................................... 75  
Prohibited Transactions ....................................................................................... 75  
Take Charge of Chargebacks .............................................................................. 77  
Processing Transactions Manually with an Imprinter ......................................... 77  
Processing Transactions through an Electronic Point-of-Sale Terminal .............. 78  
Mail and Telephone Orders ................................................................................. 78  
Protecting your Internet Business ........................................................................ 78  
Factoring or Credit Card Draft Laundering .......................................................... 79  
Spotting Counterfeit/Altered Cards ...................................................................... 79  
MasterCard Formats ............................................................................................. 80  
Visa Card Formats.................................................................................................. 85  
Discover Formats .................................................................................................... 88  
American Express Card Security Features ......................................................... 89

**Fraud Protection** ............................................................................................... 91

**Termination of Service** .................................................................................... 103

**Exhibits** ........................................................................................................... 105  
Exhibit A. Visa Debit Services ............................................................................ 105
| Exhibit B. UnionPay (UP) Card Services | 106 |
| Exhibit C. Mail and Telephone Orders | 107 |
| Exhibit D. Ecommerce/Internet Services | 108 |
| Exhibit E. Tele-Deposit Service | 112 |
| Exhibit F. Pay@Pump Service | 112 |
| Exhibit G. Push Funds Service | 113 |
| Exhibit H. Lodging Merchants | 114 |

**Glossary of Terms** .......................................................... 123
Welcome, and thank you for choosing Global Payments as your partner for all your payment processing needs.

Each and every day, more than one million merchant locations across North America, including hundreds of thousands in Canada, rely on Global Payments to process millions of credit and debit transactions through our data networks. Global Payments also handles merchant settlement and accounting needs, and Global Payments Canada GP (“Global Canada”) provides point-of-sale (POS) terminal management.

Our goal is to ensure that you have the information, card payment options and flexibility you need to help your business grow.

Our Role
Serving as your advocate is one of Global Payments’ most important roles. We are committed to providing service and value for fast, reliable processing and settlement.

Global Payments also offers four decades of expertise in payment processing and is a full-service provider of merchant processing services for all major credit and debit cards.

Your Role
As a Global Payments merchant it is important that you:

- Read, understand, and abide by your Merchant Agreement and this Guide to accepting cards for payment;
- Take all necessary steps to prevent fraud;
- Follow best practices in accepting electronic payment methods;
- Advise us of any changes related to your business such as changes in status, changes in business structure, address or contact information;
- Notify Global Canada upon cancelling or returning equipment;
- Call our Customer Care Centre or your sales representative to make any changes or cancellations;
- Keep up to date on industry news and policy changes.
Need Assistance?

Global Payments, your transaction processor and advocate, is here to help with fast and courteous, 24-hour, seven-day-a-week customer care. For assistance, contact your Global Payments Customer Care Representative.

Be sure to check the Industry Initiatives section of our website for information about payment networks, regulations and industry updates.

To access our website go to: www.globalpaymentsinc.com/canada.

The Global Payments website is also a source of information about its products and services. For more information about obtaining additional services from Global Payments or products from Global Canada, talk to your Global Payments sales representative or visit us at: www.globalpaymentsinc.com/canada.
Congratulations! Your decision to accept credit and debit cards as a valid form of payment offers a valued service to your customers.

This Guide is part of your Global Payments Merchant Agreement. You must follow the instructions and procedures in this Guide to comply with your Merchant Agreement. Please keep this Guide handy for reference. We recommend that you keep your Merchant Agreement and other paperwork, including telephone numbers associated with your Merchant Agreement, with this Guide and Welcome Kit.

You are taking an important step in enhancing customer service and increased sales volume when you offer your customers the payment flexibility of VISA, MasterCard, American Express, Interac Direct Payment, Visa Debit, Discover and UnionPay (UP) cards.

Additionally, when you accept payment with credit and debit cards, you gain a competitive edge, maintain a positive image and have the potential to increase your bottom line.

We want you to be familiar with your Global Payments card acceptance program and take advantage of all its features to help your business grow and prosper. The information in this Guide has been provided to supplement your Merchant Agreement and will assist you in the operation of your business.

We’ve included answers to the questions most frequently asked by card-accepting businesses like yours. If you have additional questions not covered in this Guide, we encourage you to call and speak with our Customer Care Centre or your Global Payments sales representative.

Our goal is to provide you with a card acceptance program that is designed to grow with your business. Your comments and ideas help us to constantly develop new ways to meet your needs.

The Parties Involved in the Transaction

Customer/Cardholder
The process of paying for goods and services begins when the customer submits an application to a bank that issues VISA, MasterCard, American Express or Discover cards or other credit cards processed by Global Direct and covered by your Merchant Agreement and/or is provided with an Interac Direct Payment, Visa Debit or other debit cards processed by Global and covered by your Merchant Agreement that is tied to the customer’s bank account. The cardholder becomes an authorized user of VISA, MasterCard, American Express and/or Discover payment products and/or can use the Interac Direct Payment, Visa Debit or UP cards to make purchases from merchants accepting such cards for payment.
Introduction

In order for you to accept any new type of card not previously accepted by you and issued by a Canadian card issuer, you must provide your express consent to Global. This includes any new product or service, even if your POS equipment has the capability of acceptance.

Bankcards, Debit Cards and Issuers
VISA, MasterCard, American Express and Discover cards are sometimes known as bankcards because individual financial institutions issue them, banks for example, instead of the credit card company itself, such as American Express® or JCB®.

In Canada, if the financial institution or credit card company (issuer) accepts the customer’s application for a credit card, it issues the VISA, MasterCard, American Express or Discover card. A credit card signifies that the bank or credit card company has authorized a line of credit against which the customer may draw.

Another type of card is an Interac Direct Payment or Visa Debit card, sometimes referred to as a debit card because payments for the transactions are withdrawn (debited) directly from the cardholders’ bank accounts at their financial institutions. A debit card is therefore tied to the amount of money actually on deposit for the cardholder at his/her financial institution.

With respect to VISA, MasterCard, American Express or Discover products, (i) merchants who accept credit card payments from a particular payment network are not obligated to accept debit cards issued by Canadian issuers belonging to such payment network, and (ii) merchants who accept debit card payments from a particular payment network are not obligated to accept credit cards issued by Canadian issuers belonging to such payment network. UnionPay (UP) cards may be debit cards or credit cards.

Merchant
Meanwhile, you or your business has opened a payment card transaction deposit account with your bank, and your business has been approved for card acceptance by Global Payments. You are an authorized acceptor of cards for the payment of goods and services. Now you’re ready for that first payment card customer.
How the Transaction Process Works

Any payment card transaction ultimately begins and ends with the cardholder. The illustration below shows the steps involved in an electronic payment transaction, and how the various organizations interact to create a smoothly executed process.

The cardholder presents the card as payment for goods or services, either at the point-of-sale (POS) or via telephone, mail, fax or over the Internet.

Our Business Model
Authorization and Electronic Data Capture
Once the electronic information is captured from the magnetic stripe or chip on the card, an electronic imprint of the card number and other relevant information are passed to Global Payments for authorization. Global Payments then electronically routes the data from the card to the card issuer through the payment card brand networks.

The card issuer checks the cardholder account status, and the requested authorization amount is compared to the cardholder’s available spending limit or funds on deposit and reviewed with fraud protection tools.

If the card is approved, the issuer posts the approved amount against the cardholder’s credit line or funds on deposit and the card issuer provides the authorization approval.

At this point, the authorization response is returned by the card issuer to the merchant and routed through Global Payments, the processor.

Funding
The process of moving the funds from the cardholder’s account to the merchant’s account is called funding. During funding, the card issuer funds/credits the merchant’s bank, which then funds/credits the merchant’s account with the amount of the transaction.

To initiate funding into their merchant bank accounts, merchants typically commence an “end of day” transaction on their point-of-sale terminals. This type of transaction sends to Global Payments the relevant electronic details about a merchant’s day. Global Payments reconciles such credit card and debit card transactions, provided by the merchant, and then deposits the appropriate funds into the merchant bank account at the merchant’s designated financial institution.

On the cardholder side, in the case of a credit card transaction, the electronic draft is routed to the cardholder’s issuing bank or credit card company, which records the transaction as a charge against the cardholder’s account, and sends the cardholder’s monthly statement for payment. In the case of an Interac Direct Payment or Visa Debit transaction, the cardholder’s bank account was debited immediately at the time of the transaction, and the relevant transaction information will appear on the merchant’s bank account statement.
Introduction

Settlement
The process of moving the transaction information from your business to the cardholder’s financial institution is called settlement. VISA, MasterCard, American Express, Discover, Interac and UnionPay maintain authorization and settlement networks for card processing and charge a fee for their use. For credit cards, this fee is a percentage of the transaction, and it is the foundation for your discount rate.

Remember that your deposit account is not just for deposits. This account is also used for paying Global Payments its applicable fees; Global Payments will subtract accumulated discount fees and other charges from your deposit account.

Merchant must provide Global with the bank’s name and bank routing information, and Merchant’s Bank Account number, and Merchant must notify Merchant’s bank that Global Payments will have access to Merchant’s account for debiting and crediting the Bank Account.

Merchant must immediately notify Global of any changes to Merchant’s Bank Account information. Failure to notify Global of such changes may cause delay to Merchant’s Settlement until updated.

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

Global will not be responsible for any obligations, damages, or liabilities in excess of the amount of applicable debit, credit, or adjustment to Merchant’s Bank Account in the event that Merchant’s bank does not honour any such item or improperly applies it to Merchant’s Bank Account.

Occasionally, a credit cardholder will have a question about a sales draft that has already been deposited in your account. In that case, Global Payments may debit your account for the amount of the sale until the customer’s question is resolved. This is called a chargeback and is described in more detail later in this Guide.
In order to properly address credit card chargeback issues, merchants must retain swiped/inserted and/or imprinted signed copies of credit card sales drafts bearing cardholder signature to address cardholder inquiries and requests for copies. Global Payments requires retention of your VISA, MasterCard, Discover, Interac and UnionPay transactions for a minimum of 18 months (or such longer period as mandated by local law); a 24-month retention period applies to American Express transactions.

The original draft or a legible copy is to be stored for 18 months from the date you were paid for the transaction – even if you have ceased to be a Global Payments customer before the retention period has expired. Be sure the stored copy is legible, in the event a copy is needed to defend against a chargeback.

Stored sales drafts and other transaction data should be safeguarded with limited access. You must keep all systems and media containing cardholder, account or transaction information (whether physical or electronic) in a restricted, secure manner so as to prevent access by or disclosure to any unauthorized party, and you are liable for any failure to do so.

At the end of the 18 month retention period (or such longer period as mandated by local law), transaction data such as sales drafts, reports, and other media with cardholder account data must be rendered unreadable prior to being discarded. If you have PC access to transaction information, then you must not dispose of the PC until information has been rendered unreadable.

Always keep complete records of all credit card transactions for chargeback requests. Do not store sales drafts in alphabetical order by customer. The cardholder name is not part of the retrieval request record. We recommend using a storage system that is sorted chronologically by date, amount and then by cardholder account number.
The addition of personal or confidential cardholder information on the payment card sales draft can open the door to fraud or other criminal activity. Merchants must understand and acknowledge the importance of complying with payment network security requirements and best practices related to the processing, receiving, storage, and disclosure of transaction information.

Keep cardholder account data and personal information confidential. This information should be released only to your merchant bank or processor, as specifically required by law, or in response to a government request. Safeguard your customers by ensuring that you provide confidential cardholder account information only to authorized sources. You must have written agreements with a provider supported by Global Payments for any loyalty program.

You must not request or use a cardholder’s account number or related information for any purpose except a purpose that has been specifically authorized by the cardholder and permitted by Global Payments and the applicable payment network.

You must not sell, transfer, purchase, provide, exchange or in any manner disclose account number information, a cardholder’s name, or other personal information, even in the event of failure or other suspension of business operations. This prohibition applies to card imprints, transaction receipts, carbon copies, mailing lists, tapes or any other media obtained as a result of a payment card transaction. The payment networks may impose penalties for non-compliance, and other legal liabilities may apply as well.

You agree to allow Global Canada (on behalf of Global Payments), the Member bank(s), the payment networks and/or their authorized contractors to inspect your premises and computers for the purposes of verifying the cardholder names, account numbers and other transaction information is securely stored and processed and to cooperate with the payment networks in any investigation of suspected or confirmed account data breach, loss or theft of cardholder names, or other transaction information.

If you make arrangements with a third party (including but not limited to a payment application provider or any other downstream service provider) for the purpose of collecting, processing or storing cardholder names, account numbers or other transaction information, you must execute a written contract with such party that includes language to ensure its obligations to be compliant with the Payment Card Industry Data Security Standards Program (PCI DSS) (described later in this guide) and to validate its compliance to PCI DSS, on an annual basis. In addition, your agreement should ensure your right to inspect such third party’s premises, application systems and computers (similar to the obligations in this Guide and your Merchant Agreement).
If you use a third party terminal provider or a payment application provider and they have access to cardholder account information, then your agreement with them must indicate that you retain legal control of the data, and you must identify the third party terminal provider/payment application provider with access to cardholder data (i.e., on your application or in writing) within 3 days of first use of such third party/payment application provider.

If information can be accessed over the Internet, then adequate controls must be adhered to and a third party security audit may be necessary under PCI DSS or other payment network security regulations. If cardholder transaction account data or personal cardholder information is compromised, payment network penalties for non-compliance will be assessed, and other legal liabilities may apply as well.

**Payment Network Initiatives**
The payment networks are also implementing best practices and technologies to protect against fraud and ensure privacy.

As a Global Payments merchant, you must participate in these security programs to ensure that you are meeting the networks’ standards for cardholder account data security.
PCI DSS is a global information security standard that was formed by VISA International and MasterCard Worldwide in December 2004. PCI DSS was the result of the alignment of the data security standards included in the VISA International and MasterCard Worldwide data security programs. PCI DSS was subsequently endorsed by American Express, Discover Financial Services, and JCB. In September 2006 the five major payment card networks announced the formation of an independent body, PCI Security Standards Council, to develop and maintain the evolution of PCI DSS.

PCI DSS was created to ensure the protection of cardholder account data. Due to some high profile security breaches it became apparent that a global set of data security standards was required to assist merchants and service providers in meeting the requirements. Based on twelve principal requirements, PCI DSS requires merchants and their service providers to make their physical and virtual environments secure to ensure protection of cardholder account data.

All merchants that accept payment cards as a form of payment, and all service and payment application providers involved in the processing of credit card transactions are required to validate compliance to the applicable standards set out by the PCI Security Standards Council.

The payment networks have mandated that all POS PIN Pad devices deployed by merchants after December 31, 2007 must be compliant to the PIN Transaction Security Standards (PTS) and, in the case of Interac, such equipment must also be certified in accordance with Interac-specific technical specifications and testing requirements (TSTR).

Qualified Security Assessors (QSA)

Global Payments has preferred provider relationships with several authorized QSAs specializing in providing merchant data security and compliance services. To view a complete list, visit our website at: http://www.globalpaymentsinc.com/Canada/my-global/articles/pci.html
Third Party Service Providers

All third party service providers that store, process, or transmit cardholder account data on behalf of a merchant are required to comply with PCI DSS. In addition, all service providers are required to validate their compliance to PCI DSS through the services of a QSA.

Third Party Payment Applications

Many merchants deploy third party payment applications that are tailored to their business needs to assist them in accepting credit card payments. For a merchant to be compliant with PCI DSS, the products and payment application(s) they use ("solutions") must meet the data security requirements that are applicable to it within PCI DSS.

The Payment Application Data Security Standard (PA-DSS) was developed to assist software vendors in creating secure payment application that help support merchants in validating their compliance. A list of payment applications that have validated their compliance to PA-DSS can be found on https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

Global Payments strongly recommends that merchants discuss PCI DSS and PA DSS with their vendors and refer to the list of validated payment applications when selecting a payment application. Please note that merchants are required to contact Global Payments to update their records if they have changed solution providers, payment applications or if the vendor or equipment specified on the Merchant Agreement has changed or if they believe the solution provider or payment application is not compliant.

Merchant Levels and Validation Requirements

It is important to note that all merchants and their solution providers that store, process, or transmit cardholder data must comply with the PCI DSS regardless of the volume of transactions processed or the method in which they are processed. However, certification requirements vary by business and are contingent upon your “Merchant Level.”

See the charts on the following pages regarding the different Merchant Levels.
### Merchant Level - 1

<table>
<thead>
<tr>
<th>Validation Requirements</th>
<th>Level Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any merchant – regardless of acceptance channel – with over 6,000,000 VISA or MasterCard transactions per year.</td>
<td></td>
</tr>
<tr>
<td>Any merchant that has suffered a hack or an attack that resulted in an account data compromise</td>
<td></td>
</tr>
<tr>
<td>Any merchant that a card association, at its sole discretion, determines should meet the Level 1 merchant requirements.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Scan by Approved Scanning Vendor (ASV)</th>
<th>Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report on Compliance/Annual On-site Assessment (ROC) completed by a Qualified Security Assessor or PCI validated Internal Security Assessor (ISA) if signed by an officer of the company</td>
<td>Annually</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attestation of Compliance (AOC)</th>
<th>Annually</th>
</tr>
</thead>
</table>

### Merchant Level - 2

<table>
<thead>
<tr>
<th>Validation Requirements</th>
<th>Level Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Commerce merchant with 1,000,000 to 6,000,000 MasterCard or VISA transactions per year.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Scan by Approved Scanning Vendor (ASV)</th>
<th>Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Assessment Questionnaire if completed by a Qualified Security Assessor or PCI validated Internal Security Assessor (ISA) if signed by an officer of the company</td>
<td>Annually</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attestation of Compliance (AOC)</th>
<th>Annually</th>
</tr>
</thead>
</table>
### Merchant Level - 3

<table>
<thead>
<tr>
<th>Validation Requirements</th>
<th>Level Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Electronic Commerce merchant with 20,000 to 1,000,000 MasterCard or VISA e-commerce transactions per year.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Scan by Approved Scanning Vendor (ASV)</th>
<th>Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Assessment Questionnaire if completed by a Qualified Security Assessor or PCI validated Internal Security Assessor (ISA) if signed by an officer of the company</td>
<td>Annually</td>
</tr>
</tbody>
</table>

| Attestation of Compliance (AOC) | Annually |

### Merchant Level - 4

<table>
<thead>
<tr>
<th>Validation Requirements</th>
<th>Level Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Any merchant – regardless of acceptance channel – with under 1,000,000 VISA or MasterCard transactions per year. Electronic commerce merchant with under 20,000 VISA transactions per year.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Scan by Approved Scanning Vendor (ASV)</th>
<th>Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Assessment Questionnaire if completed by a Qualified Security Assessor or PCI validated Internal Security Assessor (ISA) if signed by an officer of the company</td>
<td>Annually</td>
</tr>
</tbody>
</table>

| Attestation of Compliance (AOC) | Annually |
PCI DSS is the global data security standard adopted by the payment networks for all entities that process, store or transmit cardholder data. It consists of common sense steps that mirror best security practices.

Follow these guidelines and the ecommerce/Internet Services Exhibit in the back of this Guide.

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

For full details of the PCI DSS program, please review the following websites:

- Visa: http://usa.visa.com/merchants/protect-your-business/cisp/index.jsp
- American Express: http://www.americanexpress.ca/dsrl
- PCI Council: https://www.pcisecuritystandards.org/
Although credit and debit cards offer two of the simplest forms of payment in existence today, there are some procedures and precautions that you must follow to process transactions properly and help prevent inaccurate or fraudulent transactions.

General

1. You must honour all valid cards for which you are contracted to accept without discrimination when properly presented for payment. It is encouraged that you maintain a policy that does not discriminate among customers seeking to make purchases with a card.

2. Clearly display standard decals, signs, service marks and promotional materials provided by Global Payments to show that you accept VISA cards, MasterCard cards, American Express cards, Discover cards, Interac Direct Payment cards, Visa Debit cards and/or UP cards, as applicable. You are expected to maintain visual parity amongst acceptance marks, symbols and logos. Each acceptance mark must be displayed as a free-standing mark, meaning that an acceptance mark must not be displayed so as to suggested that it is either a secondary means of payment or exclusively linked to another acceptance brand. All such materials must be returned promptly upon termination of service or upon receipt of notice to discontinue use of such material.

3. Obtain Global Payments’ prior approval for any advertising using the name and/or brand marks of Visa, MasterCard, American Express, Discover and/or Interac.

4. Do not alter the trademarks, trade names, design, marks, brand marks or logos in any manner.

5. Cooperate with Global Payments in recovering payment cards that they request you to recover, as applicable.

6. Follow security procedures as advised by Global, and ensure your employees are familiar with them.

7. Maintain accurate logs of employee shifts, keep such logs for a minimum of one year and provide these logs to Global Payments (with or without employee names) within 24 hours of a request to do so as part of an investigation of a payment card fraud incident.

8. Cooperate with Global or its designated representatives in any due diligence review conducted to determine your ability to comply with applicable payment network requirements. Such requirements include but may not be limited to security and technical standards. You acknowledge that additional due diligence may be conducted by Global or its designated representatives in the event of a change in control of your business. Global shall not be required to provide services to you if Global determines that to do so would pose a material risk to the security or integrity of its system or a payment network.
Proper Use of Marks
When you agree to accept VISA, MasterCard, American Express, Discover, Interac and/or UP cards at your place of business or website, you agree that any approved use of trademarks, trade names, design marks, brand marks or logos shall be in accordance with the standards, including reproduction, usage, and artwork standards, of the applicable card issuer. You further agree that use or display of any trademarks, trade names, design marks, brand marks, or logos does not give you any ownership rights or interest in any of these marks.

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

For additional guidelines on the use of the American Express Marks, contact Global Payments.

Proper Display of Signage
When you agree to accept VISA, MasterCard, American Express, Discover or Interac and/or UP cards at your place of business or website, you also agree to display the proper signage to indicate that service is available. The payment networks require that you clearly display signs at the point of interaction with the cardholder. Use the sign and decals included in your merchant welcome kit. (See “Supplies” section for information on ordering additional signs and window decals.)

Card Acceptance Restrictions
VISA regulations prohibit assigning a minimum or a maximum purchase amount or adding a surcharge to credit card transactions. According to MasterCard regulations, a merchant must not directly or indirectly require any cardholder to pay a surcharge or any part of any merchant discount or any contemporaneous finance charge in connection with a Card transaction. A Merchant may provide a discount to its customers for cash payments. A Merchant is permitted to charge a fee (such as a bona fide commission, postage, expedited service or convenience fees, and the like) if the fee is imposed on all like transactions regardless of the form of payment used, or as the Corporation has expressly permitted in writing.
For purposes of this Rule:

1. A surcharge is any fee charged in connection with a Transaction that is not charged if another payment method is used.
2. The Merchant discount fee is any fee a Merchant pays to an Acquirer so that the Acquirer will acquire the Transactions of the Merchant.

MasterCard and VISA regulations also prohibit the merchant from processing credit cards for cash disbursements (unless merchant is a financial institution with a special agreement permitting such processing), processing credit cards or debit cards for scrip disbursements, collection of bad debt (e.g., returned cheques), or damages, theft, etc., or accepting cash or cheque payment for a card transaction or a card as payment for goods or services paid using another form of payment.

Charge customers typically spend more than cash customers because of the available line of credit and the purchasing freedom credit cards represent. Encouraging patronage and not penalizing customers for paying with a credit card makes good business sense. You are allowed to provide discounts for different methods of payment (e.g. cash, debit card, credit card). You are also allowed to provide differential discounts among different payment card networks. Discounts are allowed for any payment method. Any discounts must be clearly marked at the point-of-sale. Specifically, Merchant may offer discounts to Merchant's regular posted prices to prospective buyers for other methods of payments such as cash or by electronic funds transfer, cheque or credit and debit products issued on other payment networks, provided that Merchant clearly and conspicuously disclose the terms of the discount offer to all prospective buyers at the point of purchase or checkout.

According to Discover regulations, in Canada, a minimum or maximum dollar amount is prohibited. Surcharging is permitted (where permitted by local law), provided that the following guidelines are adhered to:

- The amount of the surcharge may not exceed the Cost of Acceptance for the Card Sale
- Surcharges will be assessed on card sales conducted using the same type of cards (e.g., credit, debit, prepaid) or payment methods operating on other payment methods accepted by the Merchant
- Merchant must provide Global Payments and Discover with no less than thirty (30) calendar days advance written notice of the intention to impose a surcharge in Card Sales. For information on how to notify Discover, visit http://www.discovernetwork.com/
- Merchant will clearly and prominently disclose the following that following: At point-of-entry:
  - A statement that a surcharge imposed by the Merchant is not greater than the Cost of Acceptance
Operating Procedures

At point-of-sale:
- The amount or percentage of a surcharge
- A statement that a surcharge will be applied by the Merchant; and
- A statement that a surcharge is not greater than the Cost of Acceptance

Transaction Receipt:
- The dollar amount of the surcharge as a separate line item after the subtotal and before the total amount of the Card Sale.

With respect to American Express card acceptance, Merchant must accept the Card as payment for goods and services (other than those goods and services prohibited under the Section entitled Prohibited Transactions) sold, or (if applicable) for charitable contributions made, at all of Merchant’s Establishments, except as expressly permitted by Applicable Law. Merchant is jointly and severally liable for the obligations of Merchant's Establishments under the Agreement.

Interac regulations also prohibit assigning a maximum purchase amount or adding a surcharge to debit card transactions, unless agreed to in writing by Global Payments and in full compliance with all applicable Interac regulations. For example, Interac regulations regarding surcharges require the placement of clear signage to cardholders at the point-of-sale (POS) and the use of a POS terminal that prompts the cardholder with specific pre-approved language.

Regulations also prohibit engaging in any acceptance practice that discriminates against or discourages the use of any card in favour of another card.

Draft Laundering or Factoring
Depositing sales drafts belonging to another business is in violation of your Global Payments Merchant Agreement and payment network regulations and is against the law in many jurisdictions. “Helping out” another merchant who offers to pay you a fee or commission by depositing his/her VISA, MasterCard, or American Express drafts in your account can be very dangerous and is strictly prohibited. These transactions are often questionable or even fraudulent. Schemes such as this are often referred to as “draft laundering” or “factoring” and typically result in a flood of chargebacks. It could cause automatic funds reversal from your bank account as well as immediate termination of Global Payments' services to you. Remember, the merchant who deposits another merchant's drafts is ultimately legally responsible for any problems resulting from the deposit.

We want to help protect you from this dangerous fraud scheme and the potential devastating losses. Draft laundering will likely result in the termination of your card acceptance privileges. We urge you to educate your staff about this serious problem and report third party draft laundering propositions to Global Payments and to the appropriate law enforcement agency immediately.
HomeCurrencyPay Dynamic Currency Conversion
If you wish to offer HomeCurrencyPay currency conversion (DCC) or any other currency conversion services to cardholders, you must:

• notify Global Payments prior to offering DCC services;
• inform cardholders that DCC is optional;
• not impose any additional requirements on the cardholder to have the transaction processed in the local currency;
• not use any language or procedures that cause the cardholder to choose dynamic currency by default;
• not misrepresent, either explicitly or implicitly, that DCC is a service of the payment networks;
• comply with all requirements issued by Global and/or payment networks from time to time pertaining to dynamic currency conversion, including but not limited to transaction receipt requirements.

Sales Procedures – EMV Chip
A chip card is a payment card that contains an embedded computer chip. This increases protection against payment card fraud as the data stored on the chip is encrypted and virtually impossible to copy or change. The chip on the card securely stores confidential information including the cardholders’ account number and PIN.

Chip cards and chip-enabled POS terminals work together to ensure a more highly secure payment transaction by validating the card and the cardholder in a variety of methods. In addition, the computer chip makes a card more difficult to copy, thereby reducing counterfeit fraud.

Chip represents the most secure technology available today to protect payment information that may help to prevent fraud generated by counterfeit activities. Chip infrastructure also provides a payment platform that can evolve as needed to provide continued security in the future. Chip cards will continue to carry the magnetic stripe to allow cardholders to use their chip cards in other countries that do not use chip technology or on terminals that are not chip-capable.

Note
After December 31, 2010, any newly installed AFD equipment must be fully compliant and chip-enabled in accordance with Interac’s testing standards with the following schedule: (i) 75% of AFDs by December 31, 2014; and (ii) 100% of AFDs by December 31, 2015. You acknowledge that non-compliance with the foregoing timelines is subject to sanctions and/or disconnection of non-chip enabled devices from the IDP Service.
Completing an EMV Chip Electronic POS Transaction

- **Your customer** inserts their chip card into your POS terminal or PIN Pad
  - chip side up
  - chip in first

- **You** will be prompted by your POS device as to the correct processing of the card that is presented.

- **Your customer** will now maintain control over their card, depending on the POS configuration.

- **Always follow the prompts directed by the terminal.**

- **Your customer** will follow the terminal prompts to complete the transaction.

- The chip card must remain in the terminal or PIN Pad until the transaction is completed.

- **Your customer** may be prompted to select the application payment method at time of insertion, if there are multiple applications on the card.

- **Your customer** will be prompted to remove their card from the terminal upon completion of the transaction.

- **You** will need to check the receipt to see if a signature is required.
Most chip cards (including credit cards) will use a Personal Identification Number (PIN) to identify the cardholder, similar to Interac Direct Payment transactions today. PIN is a more secure form of consumer identification and will therefore replace card holder signature, in most cases.

Chip terminals will recognize both chip and magnetic stripe cards in order to continue seamless payment processing during the transition to chip.

If a chip cannot be read, some cards may allow the transaction to occur via the magnetic stripe or manual entry but you must always use the chip reader wherever possible.

Sales Procedures – Contactless (proximity)

Contactless (or proximity payment) is a payment functionality that uses radio frequency (“RF”) technology to exchange transaction data between a chip card and an RF-enabled POS terminal, permitting card or device transactions without swiping the magnetic stripe or using a contact chip interface. A contactless payment solution provides increased speed and convenience for your customer. Contactless functionality can be used at any merchant location that has terminals which support this functionality.

The payments networks’ proprietary names for such programs are VISA payWave, MasterCard PayPass, Amex ExpressPay and Interac Flash.

The current threshold for contactless/proximity transactions is $100 CDN; however, this threshold is subject to change at any time by the applicable payment network or networks. A transaction amount that exceeds the then-current threshold established by the applicable payment network is not eligible as a contactless/proximity transaction and standard cardholder verification and receipt printing procedures apply.

Contactless/proximity transactions have a floor limit of zero.

Completing a contactless proximity transaction:

- Your customer waves or taps their card or device in the appropriate area of the terminal to initiate authorization of the transaction.
- Your customer maintains control over their card or device.
- You are not required to visually determine if the card is valid.
- The terminal will indicate when the transaction has been processed.
- You will follow the terminal prompts to complete the transaction.
- You must always provide a receipt when requested by your customer. For American Express transactions, specifically, a receipt must always be provided. You will prominently display at least one sign advising your customers that a receipt is available. A receipt is only required to contain the total transaction amount and date of
the transaction. NOTE: A transaction amount that exceeds the then-current threshold established by the applicable payment network is not eligible as a contactless/proximity transaction; in such event, the card must be processed as it would be for a regular transaction, and a receipt must be given.

- Your customer’s signature is not required. PIN may be required for debit transactions.
- You may be required to retain receipts unless otherwise directed through payment network regulations and/or guidelines

**Sales Procedures – Credit**

When a cardholder or authorized user presents a credit card for payment, you will:

- sell goods and/or services at prices not in excess of the ticketed or posted price
- swipe/insert or imprint the card only for the purposes of completing the credit card transaction and not for any other purposes
- when required obtain a signature that matches the one on the signature panel of the payment card presented
- not spread a purchase over more than one sales draft
- not impose any fees or other charges for the use of a card as the means of payment unless local law requires that merchants be permitted to engage in such practice
- not require a minimum or maximum purchase amount before you will accept the card for payment
- if you have a point of sale terminal, you agree to follow the instructions displayed on the terminal and to record the authorization code on the sales draft, where applicable

**Note**
The chip card must remain in the terminal or PIN Pad until the transaction is completed. Always follow the prompts directed by the terminal.

**Sales Procedures – VISA Easy Payment Service**

VISA Easy Payment Service (VEPS) is the new global name for the No Signature Required (NSR) program and Small Ticket Transaction program available for certain quick-pay industry-specific merchant categories requiring rapid check-out and where the point of service is traditionally cash-based. VEPS transactions are face-to-face.

**Note**
Splitting the sale into multiple transactions is strictly prohibited.
American Express No Signature Program
Merchant’s Establishment may participate in American Express’ No Signature Program. The No Signature Program allows Establishments not to request a signature from Cardmembers on the Charge Record.

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

Establishment Criteria
If Merchant’s Establishment is classified in an industry that accepts In-Person Charges, then the Establishment may participate in the No Signature Program with the exception of the following categories:
• Merchants who do not conduct In-Person Charges (i.e., internet, mail order or telephone order)
• Prohibited Merchants or Prohibited Transactions (or both)
• High Risk Merchants (e.g., internet electronic services or nightclubs/lounges)
• Merchants placed in American Express’ Fraud Full Recourse Program

VEPS streamlines the merchant acceptance procedures by removing certain requirements such as the need for cardholder verification and generation of receipts unless requested by the cardholder.

VEPS is targeted at low value transactions under certain limits. The current VEPS limit is $25 CDN for EMV or magnetic stripe ‘contact’ transactions and $100 CDN for ‘contactless’ transactions. A transaction amount that exceeds the then-current limit is not eligible as a VEPS transaction and standard cardholder verification and receipt printing procedures apply.

VEPS transactions have a floor limit of zero.

When completing a VEPS transaction:
• You will swipe/insert or imprint the card only for the purposes of completing the transaction.
• The terminal will indicate when the transaction has been processed.
• You will follow the terminal prompts to complete the transaction.
• You will not be required to provide your customer a receipt, unless one is requested by your customer. You will prominently display at least one sign advising your customers that a receipt is available. A receipt is only required to contain the total transaction amount and date of the transaction.
• Your customer’s signature is not required. PIN may be required for debit transactions.
• You are not required to retain a receipt.
Other Important Facts

Electronic Data Capture Merchants
Electronic Data Capture (EDC) merchants use a terminal or other electronic device (e.g., cash register or PC) to authorize and settle their transactions. Using EDC is preferable to using paper drafts since an electronic record of your credit and debit card transactions is maintained throughout the business day. The terminal can be used to validate your totals before settling with Global Payments at the end of the day. In addition, using a terminal helps reduce errors often associated with manually calculating, processing and depositing drafts.

Global Payments strongly recommends that merchants discuss PCI DSS and PA-DSS with their vendors and refer to the list of validated payment applications when selecting a payment application. Please note that merchants are required to contact Global Payments to update their records if they have changed solution providers, if the vendor or equipment specified on the Merchant Agreement has changed or if they believe the solution provider is not compliant.

If you currently do not use Electronic Data Capture, contact Global Canada for information on how you can improve your business with newer, more effective technology.

Completing an Electronic Transaction
It is very important to complete a transaction accurately and fully. The quality of the transaction is critical to the financial success of your business and your customer’s satisfaction. Furthermore, completing a transaction accurately and fully helps avoid potential retrieval requests and chargebacks.

Steps to complete an electronic transaction:

- Determine card validity
- Swipe/insert the card (if you are presented with a card with a chip on it, insert the card in the chip reader with the chip facing up and in. Leave card in the reader until the transaction is completed)
- Compare account numbers
- Request authorization
- Print the sales draft
- Obtain and compare signatures

Charge criteria
- The amount of Charge must meet the established threshold
- The Charge Submission must include a valid Approval

For more information, please refer to the American Express OptBlue Program Merchant Guide: www.americanexpress.ca/optblueguide

If the payment card does not swipe (or, if applicable, the chip is not readable) and you must manually key the transaction, you must obtain a manual sales draft imprint of the card presented and complete it as required.
Determine Card Validity
Check the credit card to make sure the card is valid and has not been altered in any way. Verify that the transaction date falls within the dates embossed on the card. Some cards have two dates – an effective date and any expiry date. The second date shown is always the expiration date. Do not accept a transaction occurring before the first date or after midnight on the second date. Utilize the card’s many “fraud control” features to verify that the card number contained in magnetic stripe data matches the number embossed on the card.

See “Spotting Counterfeit/Altered Cards” section for additional instructions on how to be sure a card is valid.

Swipe/Insert the Card
- Swipe the card to request the transaction authorization
- Hold the card through the entire transaction
- Avoid sliding the card back and forth
- Slide the card only once unless prompted to do otherwise by the device
- If you are presented with a card with a chip on it, insert the card in the chip reader with the chip facing up and in. Leave card in the reader until the transaction is completed
- Use the manual or call the help desk if the system develops problems

If a terminal swipe/insert is unsuccessful, you must nevertheless secure authorization for the card transaction and obtain a manual imprint of the card on a standard sales draft and the cardholder’s signature. Follow the procedures under “Processing Paper Drafts.” Complete the sales draft, including a signature, and attach a copy to the printer-generated draft for your records.

Compare Account Numbers
Compare account numbers displayed on the terminal or printed on the sales draft to the embossed number on the customer’s card. If the numbers match, enter the amount of the transaction into the terminal and request authorization. If the numbers do not match, call Authorizations for a “Code 10.” Follow the instructions the operator gives over the telephone.

Some point-of-sale (POS) devices offer additional built-in fraud control features that can help you identify counterfeit cards, and assist in avoiding potential chargeback losses. If the controls are activated, you will be prompted to input the last four or five digits of the card number after initially swiping the card. If no issues are identified, the transaction will proceed as normal. If a problem is detected, the POS device will display a “mismatch” message.

If the “mismatch” message appears, re-enter the 4 or 5 digits as requested. If the message appears again, the card is potentially counterfeit or fraudulent. In this case, follow Code 10 procedures, and do not accept the card as a form of payment.
Request Authorization

In the authorization process, the issuer approves or declines a transaction based on a number of factors. In most cases, transactions are quickly processed electronically. However, to protect against fraud, the issuer may request information about the transaction.

When requesting authorization, you may receive one of the following or similarly worded responses:

- **Approved:** This response means the issuer approves the transaction. If you have a terminal printer, the approval is noted automatically. If you do not have a terminal printer, write the authorization code clearly on the sales receipt.

- **Declined or Not Approved:** Issuer does not approve the transaction. Do not process this transaction. Quietly inform the customer that the card has been declined. Ask if the customer would prefer to use an alternative form of payment. Do not attempt to authorize for lower amounts.

- **Call or Call for Auth or Referral:** This means that the issuer wants the sales associate to call to obtain some additional information prior to approving the transaction. Most of these transactions are subsequently authorized, and you may want to inform the customer that this is a process designed to protect the cardholder and issuer against fraud. Call the Voice Authorization Centre and follow the operator's instructions.

- **Pickup Card or Hold Card Call:** Means that the issuer wants the sales associate to keep the card. If you can, try to retain the card; however never put yourself in any danger.

- **Invalid Account Number or Fraud Check Digits are Invalid:** When using built-in fraud control features (see “Compare Account Numbers” above), the POS device may display this message if the required digits that you entered do not match the information embedded on the magnetic stripe. Re-enter the required digits as requested. If the message appears again, the card is potentially counterfeit or fraud. In this case, follow Code 10 procedures, and do not accept the card as a form of payment.

Obtaining an authorization does not guarantee against chargebacks.

To reduce your risk of incurring a chargeback on a fraudulent card, when receiving a referral response, the issuing bank requests an authorization through a voice operator. Contact our voice authorization centre and speak directly to an operator. Do not use the Interactive Voice Response (IVR) on these voice referral transactions.
Print the Sales Draft; Obtain and Compare Signatures

Follow these steps if you are using a printer. (If, however, your terminal is not connected to a printer, or if your printer is not working, follow the operating procedures under “Using the Imprinter.”)

1. Have the customer sign the printer-generated sales draft (magnetic stripe transactions only).
2. Hold the card in your hand while you compare the signature on the sales draft with the signature on the back of the card. Make sure that the signatures match. If they don’t match, ask for additional information, such as a driver’s license or other government approved documents like a birth certificate, and call the Authorization Centre for instructions. If there is no signature, ask for additional information, have the customer sign the card and then compare signatures.
3. If the signatures match, hand the customer the customer copy of the sales draft and return the card. Your sale is now complete. Retain a copy of the sales draft in accordance with this Guide for your records and for protection against possible disputes.
4. Remember, if the signature or card looks suspicious, or if for any reason during the card acceptance process you are suspicious that the transaction may be unauthorized or fraudulent, call for a Code 10 authorization and follow the instructions given. You must also take a manual imprint of the sale.

Note

Splitting the sale into multiple transactions is strictly prohibited.

Note

Unless you are otherwise instructed by Global and use a specially designed Global Payments service such as Tele-Deposit, all transactions authorized by phone need to be manually re-entered into your terminal in order to be electronically deposited.

Follow the instructions in your terminal procedures for Re-Entry, Telephone Authorized or Offline Transactions, located in the Global Canada Quick Reference Processing Guide or other equipment documentation that was included with your POS terminal.

Remember to always manually imprint and fully complete a sales draft, including having the customer sign the sales draft, for all sales that are forced into the terminal. If you are having terminal problems, please contact Global Payments’ Customer Care Centre for assistance.
Processing Paper Drafts

It is very important to complete a transaction accurately and fully. The quality of the transaction is critical to your business’ financial success and your customer’s satisfaction. If you are accepting credit transactions manually, you must obtain authorization from Global Payments for any purchase exceeding the floor limit (floor limit = $0 unless otherwise approved by Global Payments in writing) and complete a sales draft including the date of the purchase on a form supplied or approved by Global Payments by following these steps:

1. Verify that the card is valid and has not been altered. See the “Spotting Counterfeit/Altered Cards” section for instructions on how to be sure a card is valid.
2. Imprint the draft with the card account number and any other embossed information. Follow the procedures under “Using the Imprinter.”
3. Call for an authorization. Make sure you have both the sales draft and customer’s credit card when you call the Authorization Centre. Provide the following information to the operator:
   • Cardholder credit card account number
   • Your Global Payments merchant number
   • The total amount of the sale
   • The card expiry date
4. Write the authorization code in the provided space on the sales draft.
5. Have the customer sign the sales draft.
6. Hold the card in your hand while you compare the signature on the sales draft with the signature on the back of the card. They must match. If they don’t match, ask for additional information, such as a driver’s license or other government approved document like a passport, and call the Authorization Centre for instructions. If there is no signature, ask for additional information, have the customer sign the card and then compare signatures.
7. If the signatures match, hand the customer the customer copy of the sales draft and return the card. Your sale is now complete. Retain a copy of the sales draft in accordance with this Guide for your records and for protection against possible disputes.
8. Remember, if the signature or card looks suspicious or if for any reason you are suspicious that the transaction may be unauthorized or fraudulent, call for a Code 10 Authorization and follow the instructions given.
9. Sales Draft Requirements:
   • Only one sales draft per sale. DO NOT divide the amount onto two sales drafts. If necessary, “ring-up” another sale.
   • No changes to sale draft after customer signs. If there’s a dispute, the customer’s copy is treated as correct.
   • USE only approved Global Payments sales drafts.
   • Restaurants use special sales drafts which include another box for the customer to insert the amount of the tip. In this case, do not fill in the amount of total sale. This will be done when the customer completes the tip portion and signs the draft.
Other Important Facts

- Each sales draft completed by a Merchant for Card Present and Card Not Present Card Sales should clearly indicate the following information:
  - Card Number where permitted by applicable Requirements of Law, and truncated where required by applicable Requirements of Law
  - Quantity and brief description of the goods or service purchased
  - Card transaction date
  - Authorization Code
  - Initials of Merchant representative that conducted Card Transaction
  - Total amount of the Card Sale, including applicable taxes, surcharge and gratuity, in the Originating Currency in which the Merchant conducted the Card Sale
  - Cardholder’s signature
  - The words “Card Not Present” must be written on the sales draft in lieu of the Cardholder’s signature in Card Not Present transactions
  - Merchant’s name and location (city/town and province)

Global Payments provides you with all the materials you need if your business requires the ability to perform paper draft processing; however, we recommend Electronic Data Capture (EDC) as a safe and convenient way to accept payment and help improve processing accuracy. Contact our Customer Contact Centre or your Sales Representative to learn about the many electronic processing options available to Global Payments merchants.

Using the Imprinter

1. Make sure the imprinter handle is to the left.
2. Place the customer’s credit card on the imprinter face up, between the plastic guides (upper left corner).
3. Move the imprinter handle completely across the draft with a quick, firm motion, and return the handle to its original position.
4. Be sure that the imprinted information is legible on ALL copies of the draft. If not, print the complete information above (not over) the imprinted information.
5. Use a ball point pen (not a soft felt tip), to enter the date, description of merchandise or services, sales amount, approval code, tax, total and clerk’s initials on the draft (VERY IMPORTANT TO COMPLETE ACCURATELY).
6. Follow the procedures set out in this Guide for completing the transaction: Requesting authorization, obtaining customer signature and comparing signatures on the card and sales draft.
Authorizations

**Obtaining a VISA, MasterCard, American Express and Discover Authorization**

**Call for an authorization when:**

- You do not have an electronic point-of-sale terminal.
- The total sales amount (including tax and tips where applicable) is higher than your floor limit.
- You are at all suspicious about the VISA, MasterCard, American Express or Discover transaction.

**Authorization Procedures**

Make sure you have both the sales draft and the customer’s VISA, MasterCard, American Express or Discover card when you call the respective Authorization Centres. You will be asked for:

1. Cardholder Account Number
2. Your Merchant Number
3. The total amount of the sale
4. The card expiry date

When VISA, MasterCard, American Express or Discover authorize the charge, you will receive an authorization number which you must write on the sales draft in the appropriate box. Verify the number by reading it back to the Authorization Centre operator.

**Notes Regarding Authorizations**

a. All procedures for completing the sale slip must be followed.
b. The date on the sales draft must be the same as the authorization date.
c. The Authorization Centre never closes – open 24 hours a day, 7 days a week.
d. Remember that obtaining an authorization does not guarantee against chargebacks.

**Code 10 Authorization**

A Code 10 authorization is a special procedure for dealing with suspicious transactions. Use it any time you suspect fraud, a counterfeit card, or if you feel the transaction needs a closer look. It’s a simple way for you to alert the Authorization Centre without alarming the customer.

**How Code 10 Works**

1. Call the Authorization Centre. When the automated answering system answers, listen for the Code 10 prompt, and press #1 to route your call to operators trained to deal with Code 10 situations, and alert the operator about your suspicion. (Note: Do not use the Code 10 option to bypass the standard authorization process – it is only to be used when you suspect the transaction may be fraudulent).
2. Hold the card in your hand during the authorization process. There is no need to
suggest suspicions that might either embarrass or warn the customer.
3. Your call may be transferred to the payment card issuer for validation during the process – don’t hang up.
4. You will be asked a series of questions requiring only a “yes” or a “no” to verify the authenticity of the card. If you are disconnected, call back.
5. Follow the instructions given to you over the phone.
6. If you are asked to cut the card, do not cut the magnetic stripe, as it is needed to cancel the card. Just cut the card length-wise through the raised numbering.

Your safety is important to us. Do not try to apprehend or detain the cardholder.

Sales Procedures – Interac Direct Payment (Debit)

Interac Direct Payment and Visa Debit transactions are online, PIN-secured debit transactions that do not require the customer to sign the transaction record. Instead, the customer enters a secret PIN into the point-of-sale terminal, and the amount of the transaction is debited from the customer’s bank account. If you agree to accept Interac Direct Payment or Visa Debit cards, you must follow the procedures set out in the applicable Exhibits in the back of this Guide (which serve as an addendum to your Merchant Agreement) and any written directions issued by Global relating to debit card services.

After the date mandated by each respective payment network (the network’s “Liability Shift Date”), liability arising from transactions made with fraudulent cards (counterfeit, lost and stolen, NRI (not received as issued), or other) will be the merchant’s responsibility if such merchant has not converted its point-of-sale equipment to be chip-enabled. Visa and MasterCard implemented a domestic Liability Shift Date of March 31, 2011. American Express implemented a Liability Shift Date of October 31, 2012. Discover will introduce Fraud Liability Shift for Discover Network, effective October 1, 2015 for point-of-sale terminals and October 1, 2017 for automated fuel dispensers.

When a customer presents a card for an Interac Direct Payment or Visa Debit transaction, you must:

- sell goods and/or services at the ticketed or posted price;
- provide Interac Direct Payment service free of charge unless local law requires that merchants be permitted to engage in such practice; or unless agreed unless agreed to in writing by Global Payments and in compliance with all applicable Interac regulations;
- process a refund, if you agree to accept a return of merchandise;
• swipe/insert the card, as applicable, only for purposes of completing the debit card transaction and not for any other purposes; NOTE: Visa Debit transactions using a card issued by a Canadian issuer must be processed solely as a chip card transaction, not as a magnetic stripe transaction.;
• not require a minimum or maximum purchase amount before you will accept a Visa Debit card for payment. NOTE: Interac regulations do not prohibit a merchant from requiring a minimum purchase amount;
• only provide “cash back” to cardholders if they have made another purchase and are including this cash back as part of the total transaction;
• never ask a cardholder for his or her PIN or use any other means of capturing his or her PIN;
• never 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;
• 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 for attended operations;
• process all transactions according to the Merchant Agreement and any instructions from Global Payments.

Completing a Debit Transaction

1. Swipe/insert the debit card, as applicable, or have the cardholder swipe/insert his/her own debit card if possible.
2. Enter the information for the transaction into the point-of-sale terminal.
3. Ask the customer to follow the instruction from the PIN Pad including entering his or her PIN and verifying the amount of the transaction by using the PIN Pad. Global Payments will process the request for authorization and approval.
4. Act on the instructions displayed by the terminal (either an authorization number, a decline, a message to try again, or other similar instructions).
5. Provide the customer with the transaction record (regardless of whether the transaction was approved or declined). Retain a copy of the transaction record in accordance with this Guide for your records and for protection against possible disputes.

Interac Due Diligence Requirements

The Interac network organization requires Global Payments or its designated agents to perform a due diligence review to determine that you are able to comply with all applicable requirements for the debit services, including security and technical standards specified by Global Payments and Interac. Additional due diligence may be conducted by Global Payments or its designated agents in the event of a change in control of your business. Please note that Global Payments is not required to provide the debit services to you if Global Payments determines that to do so would pose a material risk to the security or integrity of the debit services.
Your POS Terminal and Debit Transactions

If your point-of-sale terminal malfunctions, loses its connection to Global Payments’ host computer, or is not working, ask the customer for an alternate form of payment, such as a credit card, until your point-of-sale terminal is correctly working again. (Not applicable to credit card transactions; refer to the section of this Guide entitled Using Your POS Terminal to Deposit Sales Drafts.)

You must promptly advise Global Payments, as well as Global Canada, when a POS terminal is lost, stolen or not working. If a terminal displays an “out of balance” message, telephone the Global Payments Customer Care Centre for instructions within one business day.

Global Payments assumes that all debits and/or debit refunds to your accounts initiated at a POS station were authorized by you; because your business is liable for these transactions, it is important to follow the security procedures set out in this Guide regarding POS equipment.

Depositing Your Sales Drafts

Using Your POS Terminal to Deposit Sales Drafts

1. Enter each sales transaction into your point-of-sale terminal unless the terminal is not working.
2. Perform an end-of-day balance of the sales transactions for each point-of-sale terminal, preferably every day, but in no event less frequently than once every 3 days.
3. If your point-of-sale terminal malfunctions, loses its connection to Global Payments’ host computer, or is not working, follow the manual processing procedures and input sales draft and credit voucher information for all transactions, and balance the point-of-sale terminal when it is working again. (Not applicable to debit card transactions; refer to the section of this Guide entitled “Your POS Terminal and Debit Transactions.”)
4. Keep the original VISA, MasterCard, American Express or Discover sales drafts or credit vouchers as set out in this Guide.
5. If you do not provide the original or microfilm copy of a sales draft or credit voucher within eight days of a request for it, or if the information on the sales draft or credit voucher is not exactly the same as the information entered to the point-of-sale terminal according to Global Payments’ records, then the amount on the sales draft or credit voucher constitutes a debt payable on demand, and your merchant bank account may be debited by Global Payments or Member without notice.
Manual Deposits
If you have been approved by Global Payments as a manual merchant that does not use a point-of-sale terminal to process credit card transactions, follow these procedures:

1. On a regular basis, but no less frequently than once every 3 days, except as otherwise provided in Chapter 5 of the MasterCard regulations, bundle your VISA, MasterCard, American Express and/or Discover sales drafts together and prepare a summary deposit slip in a form supplied or approved by Global Payments. Insert the summary deposit slip and manual drafts into an envelope, seal the envelope, apply correct postage and mail the envelope via Canada Post to:

   Global Payments Direct, Inc.
   P.O. Box 8050 Etobicoke B
   Etobicoke, ON M9W 7K9

2. Always ensure that you keep copies of the sales drafts for your records, properly stored in a secure and confidential manner in accordance with payment network requirements.

3. You will not receive payment for a transaction that Global Payments refused to credit or has charged back to your account.

   Many errors occur due to incorrect calculation of manual deposit slips. To avoid error fees, please double check your calculations. You are responsible for correctly calculating the summary deposit slips. Global Payments recommends Electronic Data Capture (EDC) as a safe and convenient way to accept payment and help improve processing accuracy.

   Contact our Customer Care Centre or your Sales Representative to learn about the many electronic processing options available to Global Payments merchants.

Returns and Exchanges

Returns and exchanges can be used for the return of merchandise for credit only. NO CASH OR CHEQUE REFUNDS are permitted on a credit card purchase. This also includes NO CASH BACK at the time of the original sale. (Procedures are different for Interac debit transactions; refer to the applicable sections of this Guide.)

Any conditions or requirements that limit the cardholder’s ability to return merchandise, i.e., special sale event, etc., must be clearly and legibly printed on all copies of the transaction receipt near the cardholder signature area or in an area easily seen by the cardholder, and on the order form if for mail order, in advance of the transaction being completed. In-store signs are not sufficient to establish that the cardholder is aware and accepts the special conditions and/or restrictions. Disclosure of such policies must not include a statement that a cardholder waives any right to dispute the transaction with the card issuer.
Follow these steps to process a return or an exchange transaction:

Credit Card Refunds
You are responsible for settling directly with the cardholder all cardholder disputes and claims respecting any transaction evidenced by a transaction receipt. Issue a credit voucher (for the same credit card as was used for the sale) to cover any refund or other money adjustment the cardholder may be entitled to, unless Global Payments has not credited the amount to your merchant bank account or the transaction has already been charged back to your merchant bank account.

1. Ask the customer for the card used in the original transaction, and compare the account number on that card with the full or partial account number on the copy of original sales draft. They must match.
2. If you are using a printer, follow terminal procedures for processing a refund, located in your Global Canada Quick Reference Guide. If you are not using a printer, place the credit draft on the imprinter and imprint the merchant identification plate (and bankcard, if available), and have the cardholder sign the credit draft. Be sure that the imprinted information is legible on ALL copies. If not, destroy the illegible copy and try again.

Debit Card Refunds
Returns and exchanges made with Interac debit cards should be handled at the merchant’s discretion - either cash refund or refund to the cardholder’s account. If you are refunding in cash, it is recommended that the merchant should have the cardholder sign for receipt of the cash.
If refunding the cardholder’s account, ask the customer for the card used in the original transaction, and compare the account number on that card with the account number on the copy of the original sales draft. They must be identical.

Merchant has two options for processing a refund:

1. The merchant processes the refund via their terminal using the instructions outlined in your Global Canada Quick Reference Guide.
2. Contact Global Payments’ Customer Care Centre at 1-800-263-2970. A Customer Care Analyst will take all necessary information to process a refund.

Any unauthorized use of debit or credit returns are the responsibility of the merchant.

UnionPay (UP) Card Transactions

UnionPay (UP) is a service that allows your customers to purchase goods and services from you using a CUP-branded card. UP card transactions may be credit or debit transactions. If you subscribe for the UP card transaction service, you must follow the procedures set out in this Guide for credit and/or debit transactions and those set out in the UP Card Services Exhibit in the back of this Guide (which serves as an addendum to your Merchant Agreement) and any written directions issued by Global relating to UP card transactions.

Delayed Sales

When ordering an item for a customer, you may want to complete the sale when the merchandise is delivered. There are three options available:

1. Sale upon Delivery – Complete the sales draft as usual, have the customer sign it, but leave the date blank. This will be filled-in upon delivery, at which time you will obtain authorization if required, and process the transaction. Remember to provide the customer with a copy of the draft upon delivery.
2. Fully Prepaid – Process the sales draft immediately in the usual manner, but remind the customer he could see the charge go through his account before he actually sees the merchandise.
3. Deposit Now - Balance Upon Delivery – This will require two sales drafts: one for the initial deposit, and one for the remaining balance due to be paid.
   • The “Deposit” sales draft is processed immediately in the usual fashion.
   • The second draft for the “Balance Due” is completed (except for the date) at the time of the sale, signed by the customer, and processed on the day of delivery.
“Card Not Present” Transactions

“Card Not Present” transactions are those that occur when there is no face-to-face contact with the cardholder. These transactions typically include purchases made:

- by mail (also referred to as Mail Order/MO)
- by telephone (also referred to as Telephone Order/TO)
- by fax
- over the Internet (also referred to as Electronic Commerce or ecommerce)
- as recurring bill payments

Take precautions to guard against data compromise when taking orders over the Internet, by telephone, mail, fax or recurring bill payments. Since a visual identification cannot be made for cardholders requesting fax, mail, phone, recurring payments or Internet card transactions, some personal information must be obtained in order to receive authorization from Global Payments.

When processing fax, telephone, mail, recurring payments or Electronic Commerce/Internet transactions, you should always remain aware of the increased risk of fraud, because the cardholder is not present and be particularly vigilant with respect to all payment network rules and regulations. (See “Working Together to Prevent Fraud” section for additional information.)

There are also methods available to assist in reducing fraud. One such method is to use the Card Verification Values (called Card Verification Value 2 (CVV2/CVC2) to distinguish it from CVV1/CVC1/CVV encoded on the card’s magnetic stripe), or Card Identification (CID) Number with respect to American Express Cards. CVV2/CVC2 is a three-digit code number indent-printed on the signature panel of bankcards to help authenticate that the customer has a genuine card in his/her possession. The American Express CID is four-digits, printed on the Card (usually above the Card number, on either the right or the left edge of the Card). The CID provides an extra level of Cardmember validation, as part of the Authorization process.

Merchants who submit the CVV2/CVC2 code as a part of their authorization request can reduce fraud-related chargebacks.
Also, as an ecommerce merchant, you can help reduce your risk of fraud with the Account Information Security Program (AIS) from VISA and with MasterCard’s Address Verification Service (AVS). These programs are designed to help reduce the risk of fraudulent use of account numbers in card-not-present transactions. When a customer provides an address with an order, the program automatically compares it to the billing address on file with the card issuer. This risk reduction measure is especially helpful to merchants conducting business on the Internet.

You can learn more about Internet data security at www.visa.com and www.mastercard.com. As a merchant of Global Payments, you are mandated to participate if asked to participate in these security programs to ensure that you are meeting the association’s standards for cardholder data security under the Payment Card Industry Data Security Standard Program (PCI DSS).

Mail and Telephone Order Transactions
If you have been approved by Global Payments for Mail Order/Telephone Order services, you must follow these procedures and those set out in the Mail Order/Telephone Order Exhibit in the back of this Guide (which serves as an addendum to your Merchant Agreement) and any written directions issued by Global relating to mail order and telephone order services:

1. Obtain the cardholder’s name, card account number and expiry date, and record these on your sales draft. You must also obtain the cardholder’s billing address and postal code. (You may need to provide this information when you request authorization of the transaction.)

2. Request the three-digit card authentication number (CVV2/CVC2) from the signature panel or 4-digit CID printed on the face of the American Express Card. Note: Merchant retention of this authentication number is strictly prohibited. However, you may record and retain the one-character result code.

3. Fill in a brief description of the goods sold, and show the amount of the sale in the space marked “Total.”

4. Write TO (telephone order) or MO (mail order) on the signature line of the sales draft.

5. Enter transaction information into your terminal. Refer to your Global Canada Quick Reference Guide for instructions on manually entering sales transactions.

6. Provide a copy of the sales draft to the cardholder, either with the cardholder order (if being shipped to the cardholder) or separately (i.e., if purchase is a gift). The transaction date is the date goods were shipped to the cardholder. Electronically printed sales receipts provided to cardholder should truncate or mask the account number and the expiration date.
Recurring Bill Payment Transactions

If you have been approved by Global Payments for Recurring Bill Payment services, you must follow these procedures, those set out in the Mail Order/Telephone Order section above, in the Mail Order/Telephone Order Exhibit in the back of this Guide and any written directions issued by Global relating to mail order, telephone order and recurring bill payment services.

What is a “Recurring Payment”?

A recurring payment is an arrangement in which a consumer preauthorizes a merchant to bill the consumer’s credit card account at predetermined or variable intervals (i.e., monthly, quarterly, annually). The amount can be the same each time (such as monthly fees for memberships, Internet service providers or insurance premiums) or can fluctuate from one payment to another based on usage (such as phone service or utility bills). Other recurring payments may occur for newspaper subscriptions, cable TV service, cleaning service, lawn service, etc.

How is a “Recurring Payment” different from other forms of payment?

A recurring payment agreement differs from other forms of payment because it is initiated only when the cardholder establishes an ongoing card payment relationship with a merchant. The cardholder is free to continue the arrangement for a finite period of time or until one or both parties cancel the recurring payment arrangement.

A recurring services merchant must obtain a completed written authorization from the cardholder containing a written request for the goods or services to be charged to the cardholder’s account. A written cardholder authorization is a document bearing the cardholder’s signature, either written or electronic, authorizing goods or services to be periodically charged to his/her account for recurring services. A written cardholder authorization may be any of the following:

- Mail order form
- Recurring Transaction form
- Preauthorized healthcare transaction form
- Email or other electronic record that meets the requirements of applicable law

What should be on a written cardholder authorization?

The written cardholder authorization must include, but is not limited to, the following:

- transaction amount, unless the recurring transactions are for varying amounts
- frequency of the recurring charges
- duration of time for which cardholder permission is granted

Retain the written cardholder authorization for the duration of the recurring services (plus an additional 18 months to substantiate any requests for copy). Provide a copy in the event of a retrieval request. Provide a subsequent written cardholder authorization when a recurring transaction is renewed.
Are there other requirements or prohibitions for Recurring Transactions?

- Partial payment for goods or services purchased in a single transaction is NOT allowed.
- Finance Charges are not permitted on a recurring transaction.
- A recurring transaction can NOT be deposited if the Cardholder has cancelled the payment arrangement.
- A recurring transaction can NOT be deposited if an authorization request receives a negative response. (Forced depositing of declined authorization requests is PROHIBITED.)
- An authorization approval code may be used only one time.
- The account number may not be used for any purpose other than for a recurring payment.
- The floor limit for recurring bill payments is $0. You must always obtain an authorization and identify recurring bill payments in the authorization request as required by VISA, MasterCard and American Express.
- Only deposit authorized recurring bill payment transactions. Identify recurring transactions at settlement as required by MasterCard and VISA.
- Identify recurring transactions in authorization and clearing record as required by MasterCard and VISA, and with a Recurring Billing indicator, as required by American Express.
- Clearing record for recurring transaction must contain merchant contact information in the merchant name or city field to enable the cardholder to contact the merchant directly.
- Transaction receipt for recurring electronic commerce transactions must include the frequency and duration of the recurring transactions as agreed to by the cardholder on the transaction receipt.
- “Recurring Transaction” must be written on the signature line of the transaction receipt.

**Note**

Because recurring payment transactions occur without face-to-face contact with the cardholder, the merchant assumes additional risk in processing these transactions. Remember, obtaining an authorization does not guarantee against chargebacks.
**Ecommerce/Internet Transactions**

The Internet has rapidly become an alternative-shopping destination for consumers and businesses. Offering services via the Internet presents unique opportunities for merchants to expand their businesses. At the same time, your customers want to feel safe and secure while conducting Internet transactions. Global Payments is aware of the growing popularity of web-based business and has developed or certified to many flexible Internet payment processing options to assist you and help your customers feel at ease.

VISA and MasterCard are committed to promoting more secure online programs and have introduced the Verified by VISA Program (VbV) from VISA and the SecureCode Program from MasterCard. These programs are designed to help protect merchants from fraud, improve merchant’s level of security and help promote cardholder confidence in online shopping.

Payment Network Operating Regulations define an electronic commerce (or ecommerce) or Internet transaction as a transaction conducted over the Internet or other network using a cardholder access device, such as a personal computer or terminal. This definition relates to the interaction between the cardholder and the merchant. It does not pertain to the way the merchant processes the transaction after the account information is received.

Global requires that a merchant identify their electronic commerce transactions under a separate merchant number to ensure compliance with Payment Network Operating Regulations.

Merchant transactions must properly identify electronic commerce transactions in both authorization and settlement data by providing the Electronic Commerce Indicator ("ECI") for an Electronic Commerce transaction. Failure to comply may result in fines and penalties. The accuracy of this information is essential as it may have an impact on interchange qualification and pricing. If you have been approved by Global Payments for ecommerce/Internet services, follow these procedures, and those set out in the ecommerce/Internet Exhibit in the back of this Guide and any written directions issued by Global Payments relating to ecommerce/Internet services.

**Merchant Website and Electronic Transactions Requirements**

A merchant’s website must contain the following information:

- Merchant name most recognizable to consumers;
- Merchant “doing business as” name (DBA);
- Your merchant name and DBA name must be displayed as prominently as any other information on your website, other than images of the goods or services offered;
- Your merchant outlet address;
- Your merchant outlet country and country of domicile must be disclosed prior to the cardholder accessing payment instructions;

Remember you must be approved to accept VISA, MasterCard, American Express or Discover card payment orders by mail, telephone or over the Internet.
Other Important Facts

- Complete description of the goods or services offered;
- Merchandise return and refund policy must be clearly displayed on either the checkout screen or on a separate screen that allows the purchaser to click an acceptance button. While the return and refund policy information can be displayed using a link, the link cannot take the consumer to another website;
- Your consumer data privacy policy and method of transaction security used during the ordering and payment process;
- Customer service contact including electronic mail and/or telephone number;
- Transaction currency (e.g., Canadian dollars, U.S. dollars);
- Export or legal restrictions (if known);
- Delivery policy;
- Card acceptance brand marks in full colour.

An Ecommerce Transaction Receipt Must Include:

- Merchant name most recognizable to consumers
- Merchant “doing business as” name (DBA) as used on your website
- Merchant “universal resource locator” (URL)
- Merchant name used in the Clearing Record
- Customer Service contact; including telephone number (If you deliver goods internationally, include both local and internationally accessible numbers.)
- Properly disclosed terms and conditions of the sale, if restricted
- Exact date free trial period ends, if offered
- Properly disclosed cancellation policies
- A complete and accurate description of the goods or services offered
- Merchant online address
- Description of merchandise/services
- Transaction amount
- Transaction Date
- Transaction Type (Purchase or Credit)
- Purchaser Name
- Authorization Code
- Unique transaction identification number
- Terms and conditions of sale, if restricted
- Return/refund policy (if restricted)

As an ecommerce merchant, you can help reduce your risk of fraud with the Account Information Security Program (AIS) from VISA and MasterCard’s Address Verification Service (AVS).
Other Important Facts

The programs are designed to help reduce the risk of fraudulent use of account numbers in card-not-present transactions. When a customer provides an address with an order, the program automatically compares it to the billing address on file with the card issuer. This risk reduction measure is especially helpful to merchants conducting business on the Internet.

An authorization for a telephone order, mail order, fax, recurring bill payment or Internet transaction does not guarantee against chargebacks. Please ship only to the address verified as the cardholder’s. Shipment to a different address jeopardizes your protection from chargebacks. You may verify the billing address of the cardholder with the Authorization Centre or the cardholder’s bank. The Customer Care Centre can provide you with the number of the cardholder’s bank if necessary.

Forgotten Credit Cards

Mistakes happen. The sale is complete, the customer is gone, and you still have the customer’s credit card. What now?

Perhaps you have a phone number on the draft. Or maybe you know the customer and can phone. In either case, call the customer and hold the card for pick-up. Regardless, follow the points listed below:

1. Keep the card in a safe place.
2. If the customer returns for the card while you still have it, check his or her identification before returning the card.
3. If there is no contact with the customer within 24 hours, cut the card in half (lengthways without destroying the magnetic stripe), and insert the cut up card in an envelope along with a note, indicating that the card was left at your location, plus add:
   
a. credit card number
b. expiration date
c. cardholder name
d. name of recipient
e. date card recovered
f. merchant number
g. merchant name
h. merchant address
4. Seal the envelope, apply correct postage for the U.S. and mail the envelope via Canada Post to:

   Global Payments Direct, Inc.
   Attention: Settlement Dept.
   10705 Red Run Blvd.
   Owings Mills, MD 21117

5. If the customer returns for the card after you have sent it to Global Payments, ask him to call the bank that issued the credit card.

Month-End Settlement Adjustments

Global Payments normally debits month-end fees from your deposit account during the first week of every month. One way to ensure that sufficient funds exist in your bank account to cover chargebacks or reversals and discount fees is by keeping an amount equal to your average monthly discount range on deposit in your account. When planning for the possibility of chargebacks, a good rule of thumb is to keep at least twice your average ticket amount in your account.
Tele-Deposit
Tele-Deposit is a service that allows you to request authorization for transactions through a specifically designated telephone line and interactive voice response technology to deposit sales drafts electronically. If you subscribe for this service, you must follow the procedures set out in the Tele-Deposit Exhibit in the back of this Guide (which serves as an addendum to your Merchant Agreement) and any written directions issued by Global relating to Tele-Deposit services.

Pay@Pump
Pay@Pump is a service that permits you to accept credit cards and Interac Direct Payment for pre-authorized purchases at retail oil and gas fuel-dispensing pumps. If you subscribe for this service, you must follow the procedures set out in the Pay@Pump Exhibit in the back of this Guide (which serves as an addendum to your Merchant Agreement) and any written directions issued by Global relating to Pay@Pump services.

Interac established a certification program for automatic fuel dispensers (“AFDs”) requiring that only chip-enabled certified AFDs complying with Interac’s TSTR standards be deployed after June 30, 2005 and that AFDs then-currently available did not meet the security standards required for certification under Interac’s program. Notwithstanding the foregoing, Interac permitted the deployment of non-certified AFDs between June 30, 2005 and December 31, 2010, subject to the following conditions:

• After December 31, 2010, any newly installed AFD equipment must be fully compliant and chip-enabled in accordance with Interac’s testing standards.
• AFDs not covered by the first bullet point must meet the following deadlines for being fully compliant and chip-enabled in accordance with Interac’s testing standards: (i) 75% of AFDs by December 31, 2014; (ii) 100% of AFDs by December 31, 2015. Non-compliance with the timelines above is subject to sanctions.

The Interac Association and its members must be fully indemnified for any and all losses confirmed to have been caused by an AFD’s failure to meet Interac’s security standards required for certification, if such AFD was deployed after June 30, 2005. If you are an oil and gas merchant utilizing any such AFDs, any losses incurred as described herein, including penalties and sanctions due to your failure to comply with Interac’s timelines, will be your financial responsibility.
If Merchant is classified in the oil and petroleum industry, American Express may place Merchant in the Fraud Full Recourse Program if Merchant accepts Charges originating at a Customer Activated Terminal (CAT) gas pump.

Merchant must:

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

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

American Express recommends that Merchant:

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

**Push Funds**

The Push Funds Service is a service that allows you to have your VISA, MasterCard, American Express and/or debit sales vouchers transferred by Global and the Member bank at the end of each banking day to an account specified by you at another financial institution. If you subscribe for this service, you must follow the procedures set out in the Push Funds Exhibit in the back of this Guide (which serves as an addendum to your Merchant Agreement) and any written directions issued by Global relating to Push Funds.
Lodging Merchant Procedures

Because of the nature of the lodging market, and the Travel and Entertainment (T&E) industry, lodging merchants require special authorization and transaction procedures when accepting credit cards for reservation deposits and payment for accommodations and services. If you are a lodging merchant, you must follow the procedures set out in the Lodging Merchants Exhibits in the back of this Guide (which serves as an addendum to your Merchant Agreement) and any written directions issued by Global relating to the acceptance of payment cards by lodging merchants.
Occasionally, the cardholder’s issuing institution may require a copy of a sales draft for a billing question asked by the cardholder or generated by the issuer itself without cardholder knowledge or involvement. When a request is made for a sales draft from your records, we forward a retrieval request to you listing the following information:

- Cardholder’s account number
- Reference number
- Dollar amount
- Date of the transaction
- Retrieval Request Reason Code

Forward a copy of the sales draft along with the request form to the appropriate processing centre. If the information on the sales draft or credit voucher is not exactly the same as the information entered to the POS terminal according to Global Payments’ records, then your account may be debited for such amount without notice.

To avoid chargebacks for “Copy not received,” you should always send your sales draft via mail or fax to Global within the specified time on the request. You should give requests for draft copies top priority to avoid this type of chargeback. If you are responding to a “Retrieval or Chargeback Notification” from email reporting, please ensure you provide the case number for each item you are responding to. This will help to expedite your request.

Sample Sales Draft Retrieval Request

An example is on the following page.
**SAMPLE LETTER**

**RETRIEVAL SALES DRAFT REQUEST**

Date

Merchant Name
1234 Any Street
Anytown, State Zip

Global Payments
Department CBR
10705 Red Run Blvd.
Owings Mills, MD 21117

---

**Sales Draft Request**

This is a request for copies of sales drafts. To preserve your reversal rights please respond by 00-00-00. Timely and accurate fulfillment is critical to avoid unnecessary debit to your account.

PLEASE COMPLY WITH THE FOLLOWING HANDLING PROCEDURES:

Please supply a clear and legible copy of the sales slip(s) requested. Hotel supply guest folio, car rentals include rental agreement. Be sure to list case number (given below) for each sales draft. The following items MUST be legible: cardholder account number, transaction amount, transaction date, merchant name/location, expiration date, and cardholder signature.

ATTENTION: Mail Order/Telephone Order and eCommerce merchants - Please be advised that cardholder signature is not required; however, a substitute sales draft and/or order form must be supplied.

<table>
<thead>
<tr>
<th>Merchant Reference</th>
<th>Transaction Date</th>
<th>Transaction Amount</th>
<th>Batch Amount</th>
<th>Cardholder Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000000</td>
<td>00-00-00</td>
<td>40.94</td>
<td>0.00</td>
<td>12345678901234567</td>
</tr>
<tr>
<td>Processing Reference</td>
<td>Posting Date</td>
<td>BIN/ICA</td>
<td>Case Number</td>
<td>Request ID</td>
</tr>
<tr>
<td>1234567890123456</td>
<td>00-00-00</td>
<td>0000</td>
<td>1111222223</td>
<td></td>
</tr>
</tbody>
</table>

**Retrieval Reason**

Cardholder does not recognize transaction.
A chargeback is a previous transaction that is being disputed by the cardholder or the cardholder’s issuing institution. A chargeback occurs when a cardholder disputes a charge or when proper card acceptance and authorization procedures were not followed.

If you receive a chargeback, your deposit account is debited for the indicated amount. In addition to the chargeback, you may incur a fee if you failed to follow card acceptance and authorization procedures. If you exceed MasterCard International’s or VISA International’s thresholds for chargebacks, as set from time to time, you will be subject to the appropriate Global Payments, MasterCard and/or VISA charges levied for non-compliance.

Reasons for chargebacks include a cardholder dispute or an error made by the merchant in processing the transaction. Global Payments will give you details of any sales draft which has not been accepted for payment or has been charged back to your merchant bank account. Chargebacks are rare if proper authorizations and processing procedures are followed.

Examples
The following are some examples of circumstances that can cause a chargeback:

- the signature appearing on the transaction receipt is or is claimed by the cardholder to be forged or unauthorized, provided that the signature is not reasonably similar to that on the signature panel of the card;
- the merchandise referred to in the transaction receipt has been returned to you but you are not in receipt of the merchandise, or has been claimed by the cardholder to have returned to you but has not been received by you;
- the merchandise referred to in the transaction receipt was to be shipped but has not been received by the cardholder or has been claimed by the cardholder not to have been received;
- the cardholder claims that the services were unsatisfactory;
- the cardholder claims that an Internet, fax, telephone, mail order transaction was made by someone other than the cardholder;
- the cardholder otherwise disputes a transaction;
- a sales draft exceeds the floor limit and was not approved through Global Payments;
- a sales draft provided is illegible (It is the merchant’s responsibility to ensure Global Payments receives a clear legible copy for their response to the Cardholder’s or Issuer’s retrieval request.);
- a sales draft refers to an expired card or one that you have been notified not to honour, or which you (or your employee(s) or other person(s) acting for you) at the time of processing the sales draft knew or should have known was stolen, altered or counterfeit;
- the transaction includes a cash advance from you to the customer or to yourself;
• there has been an attempt to reduce or disguise the amount of a single transaction by using more than one sales draft (known as split ticketing);
• copies of the same sales draft have been deposited more than once or your account has been credited more than once with the same sales draft;
• a transaction on a sales draft took place prior to the embossed valid date on the card;
• you have processed any transaction(s) for merchandise sold or services performed by someone other than you;
• except as permitted under the Merchant Agreement in the case of mail, fax, telephone or Internet transactions, you have not used an imprinter to manually imprint the sales draft or swiped/inserted the card through your POS station to capture an electronic imprint and complete a sales draft;
• the transaction is for any reason illegal, null, or invalid;
• the transaction is charged back for any reason pursuant to VISA, MasterCard, American Express or Discover regulations;
• the transaction is otherwise unacceptable under the regulations of VISA, MasterCard, American Express, Discover, UnionPay or other applicable credit card networks;
• you have deposited or attempted to deposit sales drafts for fictitious transactions, cash advances to yourself, or you have otherwise engaged in fraudulent conduct or attempted to do so;
• you have failed to comply with the terms of the Merchant Agreement or this Guide with regard to a transaction;
• you or your representative has made a representation, warranty or factual statement to Global or Member that is untrue in any material respect;
• you have completed any transaction the circumstances of which would cause a reasonable person to assume that the transaction was not bona fide, or that the card was stolen, altered or counterfeit;
• the circumstances or elements of a transaction are such that a reasonably prudent person would be put on inquiry as to the genuineness or good faith of the transaction, or as to whether the card was stolen, altered or counterfeit;
• a transaction is unusual (having regard to the ordinary course of your business and the average size of your transactions), but you fail to take reasonable precautions to verify the genuineness and good faith of the transaction (such as determining the customer’s identity) and that the card is not stolen, altered or counterfeit.
Precautions

You can significantly reduce the chance of receiving a chargeback notification by taking the following precautions:

<table>
<thead>
<tr>
<th><strong>DO</strong></th>
<th><strong>DON’T</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Understand that you assume all responsibility for the identity of the cardholder for all fax, Internet, mail order and telephone order sales.</td>
<td>✗ Charge a cardholder before shipping the merchandise.</td>
</tr>
<tr>
<td>✓ Understand that you are responsible for any cardholder or Issuer dispute that arises out of a fax, Internet, mail or telephone order processed.</td>
<td>✗ Accept sales that are declined, and if a sale is declined, do not attempt authorization a second time on a declined sale. The cardholder bank may collect a fee if you fail to follow card acceptance and authorization procedures.</td>
</tr>
<tr>
<td>✓ Prepare and submit a written rebuttal within the time specified on the chargeback notification.</td>
<td>✗ Accept sales that are not authorized for the exact amount.</td>
</tr>
<tr>
<td>✓ Authorize all sales.</td>
<td>✗ Accept an expired card.</td>
</tr>
<tr>
<td>✓ Verify arithmetic on sales drafts.</td>
<td>✗ Accept a card before the effective date on a dual dated card.</td>
</tr>
<tr>
<td>✓ Ensure you charge the cardholder for the correct amount.</td>
<td>✗ Process a credit as a sale.</td>
</tr>
<tr>
<td>✓ Deposit sales draft(s) before the contractual time limit.</td>
<td>✗ Deposit the sales draft more than once.</td>
</tr>
<tr>
<td>✓ Credit the cardholder for the returned merchandise.</td>
<td>✗ Deposit an incomplete sales draft.</td>
</tr>
<tr>
<td>✓ Credit the cardholder for a cancelled order.</td>
<td>✗ Accept a sales draft without a cardholder signature.</td>
</tr>
<tr>
<td>✓ Verify that the signature on the sales draft matches the signature on the card.</td>
<td>✗ Participate in a suspicious transaction.</td>
</tr>
<tr>
<td>✓ Verify the authorization code.</td>
<td>✗ Obtain an authorization by using multiple transaction/split sales drafts.</td>
</tr>
<tr>
<td>✓ Obtain a manual imprint and obtain a manual sales draft if unable to process the transaction electronically by swiping the card's magnetic stripe.</td>
<td>✗ Accept a card where the account number obtained off the magnetic stripe does not match the account number on the draft.</td>
</tr>
<tr>
<td>✓ Respond to all retrieval requests within the required time frame indicated and provide a clear and legible copy.</td>
<td></td>
</tr>
<tr>
<td>✓ Take all appropriate steps to minimize cardholder disputes.</td>
<td></td>
</tr>
</tbody>
</table>
Your Right to a Rebuttal

If you receive notification of a chargeback, you have the right to request a rebuttal. A rebuttal is a merchant’s written reply to a chargeback that provides documentation proving that the sale was valid and that proper merchant procedures were followed. Rebuttals must be completed within the number of days indicated on the chargeback notification. Contact Customer Care for more information on rebuttal procedures.

How to Help Reduce Chargebacks

In order to maximize the benefits of accepting cards, you want to minimize potential chargebacks – reversals of disputed sales transactions. You may help reduce the incidence of chargebacks by following the card acceptance and processing procedures set out in this guide.

A Few Easy Steps to Reduce Chargebacks

1. Make sure the credit card presented is a valid VISA, MasterCard, American Express or Discover card. Check the standard identification and security features described in this Guide.

2. If you are using a manual imprinter, check to ensure you have a legible imprint of the customer’s credit card on all copies of the sales draft.

3. Check to make sure your customer’s signature on the sales draft matches the signature on the back of the card. Never accept an unsigned payment card.

4. Deposit your credit card sales drafts on time. Your Merchant Agreement tells you exactly how many days you have from the date of a transaction in which to deposit your sales drafts with your financial institution.

5. Make sure you respond promptly to all copy requests. Remember your copies must be legible and show: account number, transaction date, transaction amount, card expiry date, your company name and location, and the customer’s signature (if the transaction occurred face to face with the customer). When responding to a retrieval or chargeback notification, please ensure you provide the case number for each item you are responding to. This will help expedite the process.

6. Note the authorization number on any manual sales draft. When you call for a voice authorization, write the authorization number in the space provided on the sales draft.

7. Stay on top of recurring payment arrangements. Always submit your transactions on a timely basis. A transaction submitted after a customer cancels or changes a recurring payment arrangement may result in a chargeback.
How Do Chargebacks Happen?
Here are the most common reasons for chargebacks and tips on how to avoid them:

**Non-receipt of a Requested Copy.** The credit card financial institution (Issuer) may request a copy of a transaction receipt from if your customer inquires about or disputes a sales charge. This type of request is mailed or faxed to you by Global Payments and specifies the date by which the requested copy must be received. Failure to respond by the response due date may result in a chargeback to you.

**When You Receive a Copy Request You Should:**

- Locate the transaction receipt (filing transaction receipts in date order is recommended).
- Check the receipt yourself to make sure it is legible. Can you clearly read the cardholder account number, card expiry date, transaction amount, and signature (if the transaction occurred face to face with the customer)?
- If you send the original copy by mail, be sure to keep a copy for yourself. If you’re faxing a copy of the transaction receipt, you may want to enlarge it before faxing to ensure it’s clear and legible. It is your responsibility to ensure Global Payments receives a clear and legible copy of the transaction receipt before the response due date on the retrieval request notification.

If your customer has been charged incorrectly or if you fail to respond to the copy request by the due date specified, you will be subject to a chargeback.

**Duplicate Transaction.** This is usually the result of your customer claiming he or she was billed twice for the same transaction. Always balance your terminal daily to avoid discrepancies.

**Missing Signature.** In a face-to-face transaction, if you do not obtain your customer’s signature on a sale draft, your customer may claim a transaction was completed without his or her knowledge. Always remember to have your customer sign the sales draft.

**Missing Imprint.** A transaction can be charged back to you if you do not get a clear, legible imprint of the payment card together with your customer’s signature on the sales draft. “Swiping” the payment card through an electronic terminal (or inserted a chip card into a chip-enabled terminal, where applicable) is considered the electronic equivalent of a manual imprint. If your electronic terminal cannot read the magnetic stripe card, manually key in the card number, ensure that you take a manual imprint of the card and remember to complete and have your customer sign the manually-imprinted sales draft.

**Expired Card.** If you accept an expired payment card and process a transaction without getting a valid authorization, the sale may be charged back to you. Never accept a payment card in payment for goods or services prior to the “Valid from” date shown on the card (if applicable) and do not accept an expired card.
Cancelled Recurring Transaction. If you process a recurring transaction after your customer has notified you and cancelled the arrangement, you may be charged back. Make sure you keep a file of your signed agreements with your customers. Your records should include all the information needed to complete a card sales draft: customer name, valid 16 digit card number (15-digits for American Express cards), expiry date and the amount and frequency of the recurring charge plus the period of time covered by the agreement. To avoid chargebacks due to Expired Card, you should also have proper procedures in place to update your files periodically to ensure transactions are processed with valid cards.

Authorization was Declined. Follow proper authorization procedures and always obtain an authorization number when required before processing a transaction. A transaction may be charged back to you when authorization was requested but declined, but you processed the transaction anyway.

Transaction Exceeds Floor Limit. Every time you process a VISA, MasterCard, American Express or Discover transaction through an electronic terminal, a request for authorization is sent electronically to the Authorization Centre. Unless Global Payments has contractually agreed otherwise, your floor limit is always zero and you must call in for authorization for every transaction, including in the event of technical difficulties, or if you do not process transactions electronically, you must always call the Authorization Centre for approval.

No Signature Required and Contactless Proximity Transactions. Some of the foregoing circumstances may not be valid chargeback reasons in the event that the original transaction was eligible as a “no signature required” or “contactless payment” transaction pursuant to then-current payment network regulations.

Other Processing Error. Here are examples of other possible errors that could result in a chargeback:

• When the financial institution that issued the payment card to your customer has no record of the credit card account number shown on your sales draft, the transaction may be charged back to you.
• If the chargeback is the result of manually keying the wrong account number into your electronic terminal, in the case of taking an order by telephone for example, accept the chargeback and process a new transaction with the correct account number from the original sales receipt.
• A transaction may also be charged back to you if you key in an incorrect amount or if you process a refund as a sale.

Note: If you are enrolled in a “Signature not Required” program and properly process small ticket transactions, or properly process only chip and PIN transactions, signatures may not be required.

Note: If you are experiencing technical difficulties you can still accept credit cards. Simply take an imprint of the card, fill out the manual sales draft, call for authorization, make sure to obtain your customer’s signature on the manually-imprinted sales draft and call for an authorization to ensure the credit card presented is valid.
Mail Orders, Telephone Orders and Internet Orders

If you process transactions by fax, mail, telephone or over the Internet, your customer’s credit card is not physically present at your point-of-sale. As a result you don’t have an opportunity to examine the credit card to ensure its validity or that it belongs to the authorized user.

The most common reason for chargebacks in special sale circumstances is Non-Possession of Card. This results when a cardholder claims he or she did not make, authorize, or participate in the transaction and/or was not present at the time of sale. In these circumstances the sale may be subject to a chargeback.

If you process VISA, MasterCard, American Express or Discover card transactions by fax, mail, telephone or over the Internet, you should take extra care to guard against the possibility of chargebacks. Following these simple steps will help you keep your chargebacks to a minimum:

• Ensure your customer understands your refund and exchange policy. Your refund and exchange policy should be prominently displayed on the order form in your mail order catalogue or flyer, and on your Internet commerce website.
• Obtain an authorization for every transaction regardless of the dollar amount. But remember, an authorization only confirms that funds are available on the card; it does not confirm the identity of the cardholder. If the cardholder or card Issuer disputes the transaction you may be subject to a chargeback.
• Always record your customer’s name, credit card billing address, phone number(s) and email address.
• Use a shipping or courier service that provides you with a signature of the recipient so there is no dispute over non-arrival of merchandise. Establish procedures with this service so that you are advised in the event that the intended recipient of the merchandise changes the original delivery address prior to shipping.
• If your customer opts to pick up merchandise from an agreed-upon location, take the opportunity to either “swipe/insert” your customer’s credit card through your electronic terminal or get a manual imprint of the card, complete it as required, and obtain your customer’s signature on the receipt for merchandise.
POS Solutions and Security

You are responsible for the security of all equipment you use in connection with payment card processing. That responsibility extends to any unauthorized use of the equipment, regardless of whether the unauthorized use was by you, or your employees, agents, customers or other third parties. You are also responsible for security measures to protect your customers’ PINs (personal identification numbers) and the cryptographic keys loaded in your POS terminal.

Install all equipment in such a way that your customers can enter their PINs in a confidential manner – not in a location that will allow easy visibility by third parties when the PIN pad is in use by a cardholder. For attended operations, 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.

Ensure that all POS stations are monitored during business hours to prevent unauthorized use or device tampering, and closed/turned off and unavailable for use after business hours. Change your POS terminal password immediately upon receipt and then on a frequent and regular basis – also when an individual leaves your employment. Never divulge your POS terminal password to non-authorized individuals. Be aware that Global Payments will NEVER ask you to confirm or divulge your POS password.

Advise Global Payments and Global Canada immediately if you suspect that any POS station or PIN pad has been used without your authorization, tampered with or if any POS station and/or PIN pad has been lost or stolen. Do not allow any device to be connected to your point of sale terminal, or any part of it, without Global Payments’ written permission. Any unauthorized use of your POS terminal is your responsibility and you will be responsible for any losses, claims, fine or fees that may be levied by the card associations/brands.

Be aware that Global Payments will never send a representative unannounced to your location for any type of maintenance or repair to your terminal or other equipment. Never allow anyone to use, update or alter your terminal at any time, unless specifically known and authorized by you in advance. If you are unsure and require further validation, please contact Global Payments Customer Care Centre for confirmation.

Communication Lines

You are responsible for the costs of the service charges payable to the applicable third party supplier for the installation and rental of the communication lines at your place of business. If you request Global Payments to install the communication lines, and Global agrees to do so, we will bill you for the related installation fees and service charges.
Supplies

For your convenience, you can order all your paper and ribbon supplies through Global Canada. While most orders will arrive within seven (7) days, please allow two weeks for processing and shipping times. Cost of supplies will appear on your statement.

The following additional POS supplies can be ordered from a vendor by calling Global Canada:

- authorization stickers
- transaction forms
- envelopes
- sales slips
- paper
- ribbons
- VISA/MasterCard/American Express/Discover/Interac window decals and cash register signs
- merchant plates and plastics

The following additional equipment can be ordered directly from Global Canada:

- Imprinter
- Terminal
- Printer
- PIN Pads

**VISA and Interac Supplies**
1. Before placing an order, check all supplies. Place one large order, rather than several small orders.
2. Have your merchant number handy.
3. Be ready to provide the full mailing address and postal code.
4. Supplies are generally provided at no cost. Excess use may incur a charge.
5. Form #s are listed on each form

**MasterCard Supplies:**
To order free POS materials such as signs, decals, presenters and more, visit mcstore.ca or call the MasterCard POS Preference Hotline at 1-888-MC-STORE (1-888-627-8673).

**Discover Supplies:**
Visit discoversignage.com to order complimentary items, including decals, clings, billfolds, tip trays and more

**American Express Supplies:**
To select the complimentary promotional materials you would like, visit americanexpress.ca/signage
The following section provides instructions, contact information and a sample statement, to help you better understand the monthly statement you will receive.

Questions about Your Statement

If you think your statement is incorrect, or if you need more information about a transaction on your statement, please contact us immediately. After speaking with the Customer Care Centre, if you still dispute the fees, please send us written notice in a letter. We must hear from you no later than 60 days after we sent the first bill on which the error or problem appeared. You can phone us, but doing so will not preserve your rights.

In your letter, please provide the following to help Global Payments provide you with a prompt and accurate response:

• Your Global Payments merchant number and business name
• Your name
• A telephone number where you can be contacted
• The amount of suspected error
• Describe the error and explain, if you can, why you believe there is an error. If you need more information, describe the item in question.

Please note that chargebacks require a response with appropriate rebuttal information within 10 days from the date your account has been debited. Chargebacks are not considered a “billing error.”

Merchant must notify Global within 60 days of the date of the applicable statement, invoice or billing-related document; otherwise, Merchant is deemed to have accepted these fees and charges set out therein.
Understanding Your Statement

Sample Statement

How to read your statement

1. **Mailing Information** Always check your business mailing and contact information on your statement to ensure that it is accurate. If there are any changes to your business, please contact Customer Care or your Account Representative.

2. **Merchant Profile Information** Once you become a Global Payments’ merchant, a business profile is created for you which contains your merchant number, all of your pertinent business information and mailing information.

3. **Deposits** See your daily Sales and Returns for all card types at a glance. The Non-Funded section features the net amount of all cards authorized by your Point of Sale (POS) solution but not deposited by Global Payments. The Net Deposit section summarizes your daily net totals for card types deposited by Global Payments on your behalf and into your bank account.

4. **Deposit Item Summary** (DB (debit) and CR (credit)) Adjustment sections apply solely to merchants who are still processing card transactions manually.

5. **Card Summary** To help you keep track of the types of cards your customers are using, we’ve added an easy-to-read section that summarizes your daily sales by major card type, including VISA®, Interac® Direct Payment (debit), MasterCard®, American Express®, Diners Club® and other cards.

6. **Chargebacks** This section lets you quickly identify VISA and MasterCard chargebacks and rejects processed through your account. Chargebacks are itemized by day with an item count and total daily dollar amount. This section will appear only if you’ve had chargeback activity.

7. **Discount** This section not only shows you what consumers spend by major card type, it also indicates the average amount that they are spending. At the same time, you can also see the Discount Rate and Item Rate for cards processed through Global Payments.

---

**GLOBAL PAYMENTS’ STATEMENT @DVANTAGE**

LEADING-EDGE SERVICES AND SOLUTIONS, ALL IN ONE MONTHLY STATEMENT

---

**How to read your statement**

1. **Mailing Information** Always check your business mailing and contact information on your statement to ensure that it is accurate. If there are any changes to your business, please contact Customer Care or your Account Representative.

2. **Merchant Profile Information** Once you become a Global Payments’ merchant, a business profile is created for you which contains your merchant number, all of your pertinent business information and mailing information.

3. **Deposits** See your daily Sales and Returns for all card types at a glance. The Non-Funded section features the net amount of all cards authorized by your Point of Sale (POS) solution but not deposited by Global Payments. The Net Deposit section summarizes your daily net totals for card types deposited by Global Payments on your behalf and into your bank account.

4. **Deposit Item Summary** (DB (debit) and CR (credit)) Adjustment sections apply solely to merchants who are still processing card transactions manually.

5. **Card Summary** To help you keep track of the types of cards your customers are using, we’ve added an easy-to-read section that summarizes your daily sales by major card type, including VISA®, Interac® Direct Payment (debit), MasterCard®, American Express®, Diners Club® and other cards.

6. **Chargebacks** This section lets you quickly identify VISA and MasterCard chargebacks and rejects processed through your account. Chargebacks are itemized by day with an item count and total daily dollar amount. This section will appear only if you’ve had chargeback activity.

7. **Discount** This section not only shows you what consumers spend by major card type, it also indicates the average amount that they are spending. At the same time, you can also see the Discount Rate and Item Rate for cards processed through Global Payments.

---

**How to read your statement**

1. **Mailing Information** Always check your business mailing and contact information on your statement to ensure that it is accurate. If there are any changes to your business, please contact Customer Care or your Account Representative.

2. **Merchant Profile Information** Once you become a Global Payments’ merchant, a business profile is created for you which contains your merchant number, all of your pertinent business information and mailing information.

3. **Deposits** See your daily Sales and Returns for all card types at a glance. The Non-Funded section features the net amount of all cards authorized by your Point of Sale (POS) solution but not deposited by Global Payments. The Net Deposit section summarizes your daily net totals for card types deposited by Global Payments on your behalf and into your bank account.

4. **Deposit Item Summary** (DB (debit) and CR (credit)) Adjustment sections apply solely to merchants who are still processing card transactions manually.

5. **Card Summary** To help you keep track of the types of cards your customers are using, we’ve added an easy-to-read section that summarizes your daily sales by major card type, including VISA®, Interac® Direct Payment (debit), MasterCard®, American Express®, Diners Club® and other cards.

6. **Chargebacks** This section lets you quickly identify VISA and MasterCard chargebacks and rejects processed through your account. Chargebacks are itemized by day with an item count and total daily dollar amount. This section will appear only if you’ve had chargeback activity.

7. **Discount** This section not only shows you what consumers spend by major card type, it also indicates the average amount that they are spending. At the same time, you can also see the Discount Rate and Item Rate for cards processed through Global Payments.
GLOBAL PAYMENTS’ STATEMENT @DVANTAGE
LEADING-EDGE SERVICES AND SOLUTIONS, ALL IN ONE MONTHLY STATEMENT

How to read your statement (cont.)

8. Other Fees
   This section shows the Interchange Downgrade Fees (IDF).

9. Other Fees
   This section shows a breakdown of miscellaneous fees, such as settlement, dial authorization and set-up fees.

10. Effective Rate
    This section provides your Effective Merchant Discount Rate, which is calculated as your total fees paid, divided by the total sales volume, for each type of payment card.

11. Billing Summary
    This section summarizes the total amount owed for all Global Payments Direct, Inc. related services including transaction processing, set-up and service costs.

12. Total
    This figure represents the total amount owing to Global Payments for all of your merchant services during the monthly statement period from the first business day of the month to the last business day of the month. This amount will be debited from your business bank account on the first business day of the following month.

13. Notices
    This section describes commonly used acronyms used throughout your Merchant Statement.

Please Note: As part of your customized Merchant Statement, only those statement sections reflecting monthly activity will appear.

Glossary

The following glossary provides definitions for key acronyms that may appear on your Merchant Statement:

- **IDP** – Interac Direct Payment
- **AMEX** – American Express
- **DISC** – Discover Network
- **VISA** – Visa Consumer
- **VBI** – Visa Business
- **VODT** – Visa Debit
- **VISP** – Visa Signature Preferred
- **VINN** – Visa Infinite
- **VIP** – Visa Prepaid
- **MC – MasterCard Consumer
- **MCBS – MasterCard Business
- **MCCEC – MasterCard High-Spend
- **MBWE – MasterCard Business World Elite – Premium High Spend
- **MCVH – MasterCard Premium High-Spend
- **PLR – Private Label
- **Rtn – Return
- **AMEX ASMTS – American Express Assessment Fee
- **MC ASMTS – MasterCard Assessment Fee
- **STD – Standard Transactions
- **ELC – Electronic Transactions
- **REC – Reversing Transactions
- **PREM – Premium Cards Transactions
- **EMER – Emerging Market Transactions
- **EMV – Chip Transactions
- **NON-EMV – Non-EMV Transactions
- **CDN – Canadian
- **FON – Foreign/International
- **MC XRCB – MasterCard Cross Border Assessment Fee (Canadian $ merchants only)
- **MC XB INTL – MasterCard Cross Border Assessment Fee (US$ merchants only)

Global Payments and the Global Payments logo are trademarks of Global Payments Inc. and may not be copied, imitated, or used, in whole or in part, without prior written consent. All other trademarks, registered trademarks, product names, and logos identified or mentioned herein are the property of their respective owners. Payment processing and pricing approvals provided by Global Payments Direct, Inc. Terminals and terminal services provided by Global Payments.

© 2015 Global Payments Inc.
ALL RIGHTS RESERVED
Global Payments Canada GP
P.O. Box 4001, Station B
Etobicoke, ON, M9W 7H

DM-70611-v1-EN

Understanding Your Statement

GLOBAL PAYMENTS CANADA GP
Customer Service

Toll-free, 24-hour customer support and voice authorization is available through Global Payments. Refer to your merchant authorization stickers for a listing of customer service phone numbers. Forward your merchant account inquiries regarding policies to:

Global Payments Direct, Inc.
Attention: Customer Care Centre
c/o P.O. Box 4010, Station B
Etobicoke, ON
M9W 7H8
1.800.263.2970

Please include your merchant number and daytime telephone number with all inquiries.

Dispute Resolution

Arbitration Agreement (as to claims involving American Express)

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

a) Asserting a Claim. The parties agree to use commercially reasonable efforts to settle any Claim within 30 days following the time that a Claim is raised or shorter time period as either party may determine. All Claims will be resolved exclusively by arbitration pursuant to this Section, except as otherwise provided for herein. Solely in this section, Claim means any claim (including initial claims, counterclaims, cross-claims, and third party claims), dispute, or controversy between Merchant and Amex Bank of Canada whether based on contract, tort (including negligence, strict liability, fraud, or otherwise), or statutes, regulations, or any other theory, arising from or relating to this Agreement, or the relationship resulting from this Agreement, including the validity or enforceability or scope of this Arbitration provision. Claim also includes any claim, dispute, or controversy that may arise from or relates to: (i) the ordinary business practices of Global Payments or American Express, policies and procedures including Global Payments’ right to Chargeback, create reserves and debit Merchant’s Bank Account.

b) Arbitration. A Claim that is not resolved directly between the parties will be resolved pursuant to this Section and the National Arbitration Rules (Rules) of ADR Institute of Canada, Inc. (Administrator) or its successors or replacement Administrator. For a copy of the Rules, to file a Claim or for other information about the Administrator contact: ADR Institute, 234 Eglinton Avenue East, Suite 405, Toronto, Ontario M4P 1K5; email admin@adrcanada.ca. Prior to the initiation of
any Claim, Amex Bank of Canada have the right to change or replace the Administrator of the Rules in its sole discretion.

c) Small Claims Court Proceedings and Complaint Procedures. Notwithstanding anything to the contrary in this Section, Merchant may pursue any Claim without resort to arbitration in a small claims court of the province or territory of Merchant's main business office in Canada, so long as the Claim is individual, within the jurisdiction of and pending only in that court. Merchant may also access our complaint escalation procedures set forth in the Merchant Agreement between Global Payments and Merchant.

d) Consolidation. The parties agree that individual arbitration provides a more efficient and cost effective method of resolving Claims than court litigation. All Claims will be arbitrated on an individual basis. Claims brought by Merchant against Amex Bank of Canada against Merchant may be joined, heard one after the other or consolidated as the arbitrator may direct in arbitration with Claims brought by or against someone other than Merchant, if agreed to in writing by all parties. The parties further agree that the arbitrator will have no jurisdiction or authority to consider any Claim brought on a class action or representative party basis.

e) Arbitration Procedures and Appeal. The arbitrator will take reasonable steps to preserve the privacy of individuals and of business matters and the Confidentiality provisions of the Rules. Where the Claim being arbitrated is for an amount less than $50,000, there will be no oral discoveries or oral hearing subject to the direction of the arbitrator to direct otherwise. The arbitrator's decision will be final and binding. However, where an appeal is not prohibited by statute, any party can appeal the award to an appeal panel administered by the Administrator, which will consider anew any aspect of the initial award objected to by the appealing party. Where the award under appeal is for more than $50,000, the appeal will be to a three-member appeal panel. The appealing party will have 30 days from the date of entry of the written arbitration award to notify the other party that the award has been appealed. The Administrator will appoint the appeal panel that will conduct arbitration pursuant to the Rules and issue its decision within 120 days of the date of the appealing party's written notice. The decision of the three-member appeal panel will be by majority vote. The appeal decision will be final and binding and there will be no further appeal. The appeal decision will be considered as a final award.

f) Location of Arbitrations/Payment of Fees. Any arbitration hearing that Merchant attends will take place in the province or territory of Merchant's main business office in Canada. If Merchant does not have a business office in Canada, then the arbitration hearing will take place in Toronto, Ontario. The arbitrator and, where applicable, the appeal panel shall be entitled to fix the costs and expenses of the arbitration, including reasonable legal fees, the costs and expenses of the arbitration and appeal, and the fees of the arbitrator, appeal panel and Administrator.
g) Definition. For purposes of this Section, (i) Amex Bank of Canada includes any of Amex Bank of Canada’s Affiliates, licensees, predecessors, successors, or assigns, any purchasers of any receivables, and all agents, directors, and representatives of any of the foregoing, (ii) Merchant includes any of Merchant’s Affiliates, licensees, predecessors, successors, or assigns, any purchasers of any receivables and all agents, directors, and representatives of any of the foregoing; and Claim shall have the meaning set out herein.

h) Continuation. This Section will survive termination of this Agreement, any legal proceeding to collect a debt, any bankruptcy and any sale of Merchant, or their respective assets (in the case of a sale, its terms will apply to the buyer). If any portion of this Section of this Agreement is deemed invalid or unenforceable, it will not invalidate the remaining portions of this Section, this Agreement or any predecessor agreement, each of which shall be enforceable regardless of such invalidity.
When you follow best practices in accepting credit and debit cards, it will help to assist you in treating all customers fairly and honouring cards without discrimination. It will also help you to be vigilant about security and avoid possible cardholder disputes or chargebacks.

<table>
<thead>
<tr>
<th>To Follow Best Practices, DO:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅ Validate your compliance to the Payment Card Industry Data Security Standards Program (PCI DSS).</td>
</tr>
<tr>
<td>✅ Use a terminal or third party terminal provider service that is PCI DSS compliant and truncates the card expiration date and all but the last 4 digits of the card number on the cardholder copy of the receipt. (Note: Until notified, merchant copy of receipt bearing signature may display full account number and expiration date.)</td>
</tr>
<tr>
<td>✅ If using a Data Storage Entity (DSE), comply with all applicable DSE identification and registration requirements as set forth in the regulations of the Visa and MasterCard Associations.</td>
</tr>
<tr>
<td>✅ Store all materials containing cardholder account and transaction information, or cause a DSE to store all materials containing cardholder account and transaction information, in a restricted/secure area.</td>
</tr>
<tr>
<td>✅ Limit stored cardholder account and transaction information to cardholder name, card account number, expiration date, and service code to the extent required.</td>
</tr>
<tr>
<td>✅ Prevent storage of any system card-read data, CVC 2 data, PIN data or AVS data.</td>
</tr>
<tr>
<td>✅ Limit access to sales drafts, reports, or other sources of cardholder data to your employees on a need to know basis.</td>
</tr>
<tr>
<td>✅ Render materials containing cardholder account information unreadable prior to discarding.</td>
</tr>
<tr>
<td>✅ Retain legal control over cardholder transaction data and personal cardholder information if you use a third-party terminal provider or payment application solution vendor.</td>
</tr>
<tr>
<td>✅ Prevent use of cardholder transaction data for any fraudulent purpose or use in violation of the regulations of the payment networks.</td>
</tr>
<tr>
<td>✅ Prevent unauthorized access to your POS terminal by changing your POS terminal password frequently and immediately after an employee has been terminated or has quit.</td>
</tr>
<tr>
<td>✅ Immediately notify Global Risk Management at 1-800-846-0626 of any suspected or confirmed loss or theft of materials or records that contain account information retained by merchant or its third party terminal provider or payment application solution vendor.</td>
</tr>
<tr>
<td>✅ Immediately notify Global Payments in writing of the use of an agent, third party terminal provider or payment application provider not previously identified to Global.</td>
</tr>
<tr>
<td>✅ Communicate all of the above requirements to your third party terminal provider and payment application(s) solution vendor(s), and direct them to payment network information, publications, and/or websites regarding safeguarding cardholder account data.</td>
</tr>
<tr>
<td>✅ Require your third party terminal provider and payment application solution vendor(s) to adhere to payment network data security requirements (PCI DSS).</td>
</tr>
<tr>
<td>✅ Retain sales drafts for 18 months or such longer period of time required by local law.</td>
</tr>
<tr>
<td>✅ Display proper signage.</td>
</tr>
<tr>
<td>✅ Ensure your company posts and adheres to a privacy policy that complies with all applicable privacy legislation.</td>
</tr>
</tbody>
</table>
To Follow Best Practices, DON’T:

- Assign a minimum or maximum purchase amount.
- Add a surcharge or fee (unless approved by Global Payments in writing).
- Restrict bankcard use (for a sale or discounted item).
- Use a bankcard to guarantee a cheque.
- List a cardholder’s personal information on a bankcard sales slip (unless the Authorization operator requests it).
- Retain sensitive cardholder data subsequent to the authorization if prohibited, including complete contents of a card’s magnetic stripe.
- Sell, transfer or disclose cardholder account information or personal information. (Such information must be released only to Global or Member, or as specifically required by law.) If you want to participate in a loyalty program, the loyalty vendor must be certified by the payment networks and implemented in accordance with Global Payments processes and procedures.
- Render materials containing cardholder account information unreadable prior to discarding.
- Give cash or cheques refund when a purchase made with a credit card is returned.
- Provide “cash back” services on credit card purchases.
- Provide “cash back” services on an Interac debit card purchase except as part of a transaction that includes a purchase by the cardholder.
- Provide cash advances from a credit card unless you are a financial institution approved to do so through your merchant account.
- Use another acquirer or third party telephone number for authorization of a transaction other than the authorization number provided to you by Global Payments.

Do Not Ask for Personal Information Unless…

- You require this information to deliver an order – you may not refuse a transaction if the cardholder refuses to provide additional information unless this information is necessary to deliver an order;
- The Authorization operator specifically requests you to obtain the information;
- The card is not signed, and you must have the cardholder sign it and you must check the signature against another piece of valid photo identification. You must not complete the transaction if the cardholder refuses to sign the back of their card;

Be aware of your obligations under all applicable privacy laws.
Never Honour a Bankcard When…

- The customer does not have the actual bankcard;
- The card appears to have been altered or tampered with;
- Authorization is declined or you’re told to pick up the card;
- The card is not signed and/or signatures do not match;
- The cardholder refuses to sign the back of their card;
- The transaction involves illegal goods or services or is otherwise in violation of applicable law.

Working Together to Prevent Fraud

While it is not always possible to prevent fraud from happening, education and awareness are the best ways to avoid it. This information is provided to make you aware of the many ways that fraudulent activity occurs, what you should watch for and the things that you and your employees can do to protect your business.

Global Payments’ commitment to providing security for payment transactions helps both you and your customers feel safe about using payment cards; however, there are some precautions you can take that can significantly decrease the probability of fraud and/or other unauthorized payment card-related occurrences.

Prohibited Transactions

Merchants who accept credit cards must be aware of prohibited transactions and the penalties that can be imposed if a prohibited transaction is completed. A prohibited transaction is one that is not in compliance with the operating regulations of the payment networks and/or policies and procedures as defined in the Global Payments Merchant Agreement. If deposited, sales drafts involving prohibited transactions will be subject to chargebacks and may lead to the termination of your Global Payments Merchant Agreement – perhaps immediately!

The following are examples of prohibited transactions:

- Processing transactions to cover previously incurred debts, or bad debt such as bounced cheques, or payment for returned merchandise
- Processing a sale on a previously charged back transaction
- Accepting transactions that are declined by the Authorization Centre
- Attempting multiple authorization requests following a decline
- Accepting cards with an invalid effective date
- Accepting expired cards
- Using a split sale to avoid authorization requirements
- Giving cash to the cardholder
- Delivering goods or performing services after notice of a cancellation by the cardholder of a pre-authorized order
- Continuing to bill a card after the cancellation of a recurring payment arrangement
- Accepting transactions where the signature on the credit card is not the same as the one on the sales draft
- Engaging in factoring (draft laundering) or accepting or depositing drafts from other banks, merchants or businesses that you may own or purchase, but are not explicitly listed in your
current application or Merchant Agreement (or supplements to it) currently on file with Global Payments. Laundering of deposit drafts will likely result in the immediate termination of your merchant payment card privileges with us!

- Depositing a sales draft twice
- Depositing a sales draft in one or more financial institutions for payment before or after you deposit it with Global Payments

In the case of stolen cards, fraud normally occurs within hours of the loss or theft – before most victims have called to report the loss. Checking the signature becomes very important in these first few hours of loss. Also keep in mind that the thief may have altered the signature panel, or re-embossed the card, to change the account number slightly.

**American Express: Prohibited Uses of the Card**

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

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

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

**Note**
Educate your staff about prohibited transactions to reduce the risk of accepting counterfeit or fraudulent card transactions. A fraudulent transaction could involve an invalid account number, or a valid number with unauthorized use. Unauthorized use of a lost or stolen card is one of the greatest contributors to fraud losses.

**Take Charge of Chargebacks**
Chargebacks are one of the most common - and costly - ways that fraudsters take advantage of merchants. For example, some fraudsters, appearing to be legitimate customers, will take both the “merchant copy” and “customer copy” of the sales slip after they have signed it. When they receive their credit card statement, they dispute the charge. And, since your company has no record of the transaction, the full amount is credited back to the consumer, and you face a loss.

There are steps you can take to prevent chargebacks and fraud from occurring. The following examples are based on the card processing method used.

**Processing Transactions Manually with an Imprinter**
• If you process transactions manually, be sure to take an imprint of the card every time a purchase is made and complete the manual sales draft.
• Be sure to call in for authorization for every credit card transaction.
• Make sure you clearly print the sales draft so that it is legible and easy to read.
• Don’t forget to write your merchant number on the draft.
• Have the customer sign the receipt while you watch, and verify that this signature matches the one on the back of the card.
• Don’t divide/split one purchase among more than one sales draft.
• Do not change or alter the sales draft after the customer has signed it. If there is a dispute, the customer’s copy is treated as correct.
Card Acceptance Best Practices

• If a transaction is cancelled by the customer, take the required steps to stop or reverse the billing immediately.
• Be sure to display your return policy at the point of sale. Remember – it is your responsibility to inform customers of your policy.
• Maintain a well-trained staff, and ensure that they follow checkout procedures correctly.
• Save all copies of your sales drafts in case of future disputes.

Processing Transactions through an Electronic Point-of-Sale Terminal
• Be sure to always swipe/insert the card through your electronic point-of-sale device. Keying in transactions increases your exposure to chargebacks.
• Be certain your return policy is displayed and clearly stated on all of your materials and/or sales receipts.
• Keep your point-of-sale equipment clean and operating efficiently.

Mail and Telephone Orders
• If possible, establish the customer’s identity by writing his/her name, billing and ship to address, credit card number and expiry date on the sales draft (also include name of issuing institution).
• Be sure to call in for authorization for every credit card transaction.
• If you are taking an order over the phone, fax, Internet, or by mail, we recommend that goods be shipped to the billing or permanent addresses where possible – steer clear of post office boxes, hotel lobbies or freight forwarders. Remember all cardholder or Issuer disputes may be charged back and are your responsibility.
• Always send a copy of the sales draft and order form to the customer, either when the product is ordered or when it is shipped.

Protecting your Internet Business

Internet merchants should be just as aware of the risks of fraud as traditional merchants and should consider ways to prevent fraud.

If you are creating or operating an online store, be sure to learn about security risks by assessing your shopping cart procedures, securing your online transactions and letting your customers know that your website transactions are safe.

In addition, here are some key ways you can prevent Internet fraud:

• Post your purchase/return policies on your website where your customers can see them clearly.
• Start by taking a few extra steps to confirm each order, and reject orders that leave out important information.
• Be careful when dealing with orders that have different “ship to” and “bill to” addresses.
• Avoid shipping to post office boxes, hotel lobbies or other addresses that are not permanent, as these addresses can be harder to trace later.
• Pay extra attention to orders that are larger than your usual orders, as well as international orders, especially if express shipping is requested.
• Note the customer’s email address, and make sure it is valid and matches the cardholder’s name.
• Be sure that each transaction is authorized correctly and that proper procedures are followed.
• Do not accept other merchants’ requests to deposit their receipts through your account – If any items are charged back, you will be responsible for them.
• If you are suspicious about an order, pend the order and call the Issuer to request a cardholder validation of your order.

Factoring or Credit Card Draft Laundering

Beware of credit card draft laundering.

In order to commit a credit card fraud, unscrupulous individuals rely on merchants with good reputations who are authorized for card acceptance. They typically approach the honest merchants with a proposition to process third party credit card sales drafts in return for a commission or fee.

Beware of this scheme: Depositing sales drafts other than your own is a violation of your Merchant Agreement. Also known as factoring or laundering, processing such sales drafts can be a criminal offence.

When sales drafts turn out to be fraudulent and result in chargebacks you, the honest merchant, may suffer the financial losses which can be significant. Your Merchant Agreement may also be terminated. If fraud is involved, criminal prosecution may be initiated.

Entering into an agreement with other parties before depositing sales drafts will not protect you from these consequences. Any change in corporate status must be reported to Global Payments and your agreement amended, subject to re-approval.

Help us put a stop to this type of fraudulent activity: If you are approached by someone to deposit their sales drafts, report it to Global Payments immediately.

Spotting Counterfeit/Altered Cards

Knowing the card security features of VISA, MasterCard, American Express and Discover credit cards can help you and your employees detect counterfeit or altered cards and protect you from potential losses.
MasterCard Formats

MasterCard Worldwide has introduced new card design format options and modified several card security features. New card design options offer flexible placement of the MasterCard Hologram (card front or back) and introduce the option to use a new holographic magnetic tape, HoloMag™ (card back only). In addition, cards may be any colour or even feature a background pattern or a photograph. Regardless of the card design presented, check the signature and other card features for validity, and don’t hesitate to call for a Code 10 authorization if you are suspicious.

MasterCard Card Identification Features

MasterCard card front requirements:

- Must include full-color MasterCard Brand Mark.
- MasterCard account numbers must start with the number 5.
- First four digits of the account number must be the same digits as those printed directly below (pre-printed BIN).
- 16-digit account number must be clear and uniform in size and spacing and must appear on one line.
- Must include valid expiration date.
- Must include MasterCard Hologram unless hologram or MasterCard HoloMag tape appears on card back.

MasterCard card front option:

- MasterCard Hologram may be removed from the card front if the hologram MasterCard HoloMag tape appears on card back.
- “MC” Security Character is no longer permitted on newly issued cards (effective June 1, 2006), but may continue to appear on cards through June 2010.
- Card design and MasterCard Brand Mark may be oriented vertically.
- Chip may be present on card.
- MasterCard Brand Mark may be below or above globe Hologram.
Card Front Security Features Overview

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Current Requirement/Placement</th>
<th>New Requirement/Placement</th>
</tr>
</thead>
<tbody>
<tr>
<td>MasterCard Brand Mark</td>
<td>Card front</td>
<td>No change</td>
</tr>
<tr>
<td>Hologram (Global and Debit)</td>
<td>Card front</td>
<td>Card front or back based on design/type unless HoloMag tape is used</td>
</tr>
<tr>
<td>Account Number</td>
<td>Card front</td>
<td>No change</td>
</tr>
<tr>
<td>Pre-printed Bank Identification Number (BIN)</td>
<td>Card front – first four digits of the account number must be the same digits as those printed directly below (pre-printed BIN)</td>
<td>No change</td>
</tr>
<tr>
<td>“MC” Security Character</td>
<td>Card front</td>
<td>No longer permitted on newly issued cards (effective June 1, 2006), but may continue to appear on cards through June 2010</td>
</tr>
</tbody>
</table>
MasterCard® Card Identification Features

MasterCard International has introduced new card design format options and modified several card security features. New card design options offer flexible placement of the MasterCard Hologram (card front or back) and introduce the option to use a new holographic magnetic tape, HoloMag™ (card back only). This quick reference guide will highlight valid card formats, as well as mandated card security features.

Card Front Requirements
- Must include full-color MasterCard Brand Mark
- Must include valid expiration date
- Must include valid account number
- First four digits of the account number must be the same digits as those printed directly below (pre-printed BIN)
- 16-digit account number must be clear and uniform in size and spacing and must appear on one line
- Must include valid expiration date
- Must include valid account number
- First four digits of the account number must be the same digits as those printed directly below (pre-printed BIN)

Card Front Options
- MasterCard Hologram may be removed from the card front if the hologram or MasterCard HoloMag tape appears on card back
- “MC” Security Character is no longer permitted on newly issued cards (effective June 1, 2006), but may continue to appear on cards through June 2010
- Card design and MasterCard Brand Mark may be oriented vertically.

Card Front Security Features Overview

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Current Requirement/Placement</th>
<th>New Requirement/Placement</th>
</tr>
</thead>
<tbody>
<tr>
<td>MasterCard Brand Mark</td>
<td>Card front</td>
<td>No change</td>
</tr>
<tr>
<td>Hologram (Global and Debit)</td>
<td>Card front</td>
<td>No change</td>
</tr>
<tr>
<td>Account Number</td>
<td>Card front</td>
<td>No change</td>
</tr>
<tr>
<td>Pre-printed Bank Identification Number (BIN)</td>
<td>Card front—first four digits of the account number must be the same digits as those printed directly below (pre-printed BIN)</td>
<td>No change</td>
</tr>
<tr>
<td>“MC” Security Character</td>
<td>Card front</td>
<td>No longer permitted on newly issued cards (effective June 1, 2006), but may continue to appear on cards through June 2010</td>
</tr>
</tbody>
</table>
MasterCard card back requirements:

- Must include signature panel with the word “MasterCard” printed in multicolors at a 45° angle.
- Last four digits of the account number must be printed in reverse italics on the signature panel.
- CVC 2 number (three-digit validation code) must be printed in reverse italics to the right of the last four digits of the account number.
- Magnetic tape must be present and appear smooth and straight with no signs of tampering.
- Must include MasterCard Hologram or HoloMag tape unless hologram appears on card front.

MasterCard card back options:

- HoloMag tape may be used in place of the traditional magnetic tape.
- MasterCard Hologram may be placed on the card back if not appearing on the card front.

Card Back Security Features Overview

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Current Requirement/Placement</th>
<th>New Requirement/Placement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hologram (Global and Debit)</td>
<td>Card front</td>
<td>Card front of back based on design/type unless HoloMag tape is used</td>
</tr>
<tr>
<td>HoloMag Tape</td>
<td>N/A – new security feature</td>
<td>Card back unless MasterCard Hologram is used</td>
</tr>
<tr>
<td>Last Four Digits of Account Number</td>
<td>Card back – printed in reverse italics in the upper center of the signature panel</td>
<td>Card back – printed in reverse italics in the upper right corner of the signature panel</td>
</tr>
<tr>
<td>CVC 2 Number</td>
<td>Card back – printed in reverse italics in the upper center of the signature panel to the right of the last four digits of the account number</td>
<td>Card back – printed in reverse italics in an adjacent white box to the right of the signature panel</td>
</tr>
</tbody>
</table>
Card Acceptance Best Practices

MasterCard® Card Back Features and Designs

Card Back Requirements
- Must include signature panel with the word “MasterCard” printed in multicolors at a 45° angle
- Last four digits of the account number must be printed in reverse italics on the signature panel
- CVC 2 number (three-digit validation code) must be printed in reverse italics to the right of the last four digits of the account number
- Magnetic tape must be present and appear smooth and straight with no signs of tampering
- Must include MasterCard Hologram or HoloMag tape unless hologram appears on card front

Card Back Options
- HoloMag tape may be used in place of the traditional magnetic tape
- MasterCard Hologram may be placed on the card back if not appearing on card front

Card Back Security Features Overview

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Current Requirement/Placement</th>
<th>New Requirement/Placement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hologram (Global and Debit)</td>
<td>Card front</td>
<td>Card front or back based on design type unless HoloMag tape is used</td>
</tr>
<tr>
<td>HoloMag Tape</td>
<td>N/A—new security feature</td>
<td>Card back—printed in reverse italics in the upper right corner of the signature panel (permitted now, required after June 1, 2006)</td>
</tr>
<tr>
<td>Last Four Digits of Account Number</td>
<td>Card back—printed in reverse italics in the upper center of the signature panel</td>
<td>Card back—printed in reverse italics in an adjacent white box to the right of the signature panel (permitted now, required after June 1, 2006)</td>
</tr>
<tr>
<td>CVC 2 Number</td>
<td>Card back—printed in reverse italics in the upper center of the signature panel to the right of the last four digits of the account number</td>
<td>Card back—printed in reverse italics in the upper center of the signature panel to the right of the last four digits of the account number</td>
</tr>
</tbody>
</table>

If you are ever suspicious about a MasterCard card, call your Voice Authorization Center and request a Code 10.

© 2005 MasterCard International Incorporated
5-11473

HoloMag™ is a trademark of ABNH
Visa Card Formats
Every VISA card is designed with special security elements to deter counterfeiting and alteration. When you are presented with a VISA Classic, VISA Gold (Premier), or VISA Business Card, look for the following security elements:

Security Features
The following security features are required for all VISA cards

- The account number must appear clear, clean and uniform. All VISA account numbers begin with 4. If a card has been re-embossed, the original embossed numbers have been flattened and new numbers embossed, the numbers may appear fuzzy, like “ghost images.” All or part of the account number on the front of the card must match the printed account number on the sales receipt. Some unembossed VISA cards may have only partial account numbers printed on the card.
- The first four numbers of the account number must appear below the account number. These four numbers are the Bank Identification Number (BIN). If the two numbers do not match, the card has been altered or is counterfeit. The magnetic stripe should be smooth and straight, with no signs of tampering.
- Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel or writing over another name with a felt-tip pen. The repeated word “VOID” appears if the panel has been erased or compromised.
- The VISA Brand Mark must appear in either the bottom or upper right corner.
- The Dove Hologram appears on most cards, however its location on the card may vary. It can be in its traditional location on the front of the card, or a smaller hologram may be on the card back.
- Make sure that the repetitive VISA name, printed in blue and gold at a 45-degree angle, is clearly visible on the signature panel.
- The card account number, plus a 3 digit Card Verification Value 2 (CVV 2) is reverse indent-printed on the signature panel. Some cards will have only the last four digits of the account number plus the 3 digit CVV2, on the signature panel.
- The Visa Brand Mark appears in the lower right corner. Visa Debit cards have the word “DEBIT” printed above the Visa Brand Mark.
Security Features - Visa Flag Design with hologram

The Account Number
The account number must appear clear, clean and uniform. All Visa account numbers begin with 4. If a card has been re-embossed, the original embossed numbers have been flattened and new numbers embossed, the numbers may appear fuzzy, like “ghost images.”

All or part of the account number on the front of the card must match the printed account number on the sales receipt. Some unembossed Visa cards may have only partial account numbers printed on the card.

Magnetic Stripe
The magnetic stripe should be smooth and straight, with no signs of tampering.

Bank Identification Number
The first four numbers of the account number must appear below the account number. These four numbers are the Bank Identification Number (BIN). If the two numbers do not match, the card has been altered or is counterfeit.

Security Character
Visa cards may have a stylized “V” security character embossed to the right of the expiration date.

The Dove Hologram
The three-dimensional dove hologram should reflect light and seem to change as you rotate the card. Most counterfeit cards contain a one-dimensional printed image on a foil sticker.

The Signature Panel
Make sure that the repetitive Visa name printed in blue and gold at 45-degree angle, is clearly visible on the signature panel.

The card account number, plus a 3 digit Card Verification Value 2 (CVV2) is reverse indent-pressed on the signature panel. Some cards will have only the last 4 digits of the account number plus the 3 digit CVV2, on the signature panel.

Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel, or writing over another name with a felt-tip pen. The repeated word “void” appears if the panel has been erased or compromised.

VISA Brand Mark
The VISA Brand Mark must appear in the bottom or upper right corner. There is a microtext border.

Security Features — Mini Hologram on Card Back

The Signature Panel
The signature panel must appear on the back of the card. It may look like this or be custom designed. The word “VISA” is repeated and visible on the panel when placed under an ultraviolet light. Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel, or writing over another name with a felt-tip pen. The repeated word “void” appears if the panel has been erased or compromised. The manufacturer’s ID is printed underneath the signature panel.

The Mini Dove Hologram
When the Mini Dove Design Hologram is used, it must appear on the back of the card. For non-Chip cards, it may be placed either below or to the left or right of the signature panel. For Chip cards, it is placed below the signature panel.

The Account Number
The 16-digit account number must appear clear, clean and uniform in size and spacing. All Visa account numbers begin with 4.

VISA Brand Mark
The VISA Brand Mark must appear in the bottom right, top left or top right corner. Most cards will be horizontal in orientation. Visa cards with a chip may have a vertical orientation. A “V” is visible over the VISA Brand Mark when placed under an ultraviolet light.
Card Acceptance Best Practices

Security Features

The Account Number
The account number must appear clear, clean and uniform. All Visa account numbers begin with 4. If a card has been re-embossed, the original embossed numbers have been flattened and new numbers embossed, the numbers may appear fuzzy, like “ghost images.”

All or part of the account number on the front of the card must match the printed account number on the sales receipt. Some unembossed Visa cards may have only partial account numbers printed on the card.

Bank Identification Number
The first four numbers of the account number must appear below the account number. These four numbers are the Bank Identification Number (BIN). If the two numbers do not match, the card has been altered or is counterfeit.

Hologram on Card Front

Magnetic Stripe
The magnetic stripe should be smooth and straight, with no signs of tampering.

The Signature Panel
The signature panel must appear on the back of the card. It may look like this or be custom designed. The word “VISA” is repeated and visible on the panel when placed under ultraviolet light.

Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel, or writing over another name with a felt-tip pen. The repeated word “void” appears if the panel has been erased or compromised.

CVV2
The three-digit code (CVV2) may appear in the white box to the right of the signature panel or be reverse indent printed onto the signature panel.

The Dome Hologram
The three-dimensional dome hologram should reflect light and seem to change as you look at the card. Most counterfeit cards contain one-dimensional printed image on a flat sticker.

Security Features

HoloMag on Card Back

Holographic Magnetic Stripe
When the hologram is present on the card it must always be on the card back, and no other hologram appears on the card.

The Signature Panel
The signature panel must appear on the back of the card. It may look like this or be custom designed. The word “VISA” is repeated and visible on the panel when placed under ultraviolet light.

Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel, or writing over another name with a felt-tip pen. The repeated word “void” appears if the panel has been erased or compromised.

CVV2
The three-digit code (CVV2) may appear in the white box to the right of the signature panel or be reverse indent printed onto the signature panel.

Visa Brand Mark
The Visa Brand Mark must appear in either the bottom right top left or top right corner. A “V” is visible over the Visa Brand Mark when placed under an ultraviolet light.
Discover Formats

The following security features appear on Discover cards:

- The words “DISCOVER NETWORK” will appear under an ultraviolet light.
- Card numbers will appear on either the front or back of the card. Card numbers start with “6” and are composed of 16 digits that should be clear and uniform in size and spacing.
- A security character, displayed as an embossed stylized “D,” appears on the front of embossed cards.
- The Cardholder name and, if applicable, business name will appear on either the front or back of the card.
- The “Valid Thru” date may appear on either the front or back of the card in an mm/yy format that indicates the last month in which the card is valid.
- Cards must contain either the security hologram on the front or back of the card OR holographic magnetic stripe on the card back.
- The words “DISCOVER” or “DISCOVER NETWORK” appear on the signature panel on the back of the card. An underprint of “void” becomes visible if erasure of the signature is attempted.
- A minimum of the last four digits of the card number are displayed on the back of the card, printed in reverse indent printing on the signature panel.
- A 3- or 4-digit CID is printed in the same style in a white box to the right of the signature panel.
- The Discover Acceptance Mark will appear on the front of most cards, and may also appear on the back of the card, along with other affiliated logos.

Discover®

The word “DISCOVER” appears on the front of the card under an ultraviolet light.

Card numbers will appear on either the front or back of the card. Card numbers begin with the number “6” and are composed of 16 digits that should be clear and uniform in size and spacing.

A security character, displayed as an embossed stylized “D,” appears on the front of embossed cards.

The cardholder name and, if applicable, business name will appear on either the front or back of the card.

The “Valid Thru” date may appear on either the front or back of the card in an mm/yy format that indicates the last month in which the card is valid.

This example shows features that may appear on cards when appropriate. Chip-enabled cards will have an embedded smart chip. Contactless cards must display the Discover Zip indicator and the EMVCo contactless indicator. The cardholder name, card number, member since and expiration date are thermal printed on unembossed cards and therefore are flat. The stylized “D” does not appear on unembossed cards. The phrase “Electronic Use Only” must appear on unembossed cards.
American Express Card Security Features

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

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

Merchants must look for the following:

- Pre-printed (non-embossed) Card Identification Numbers (CID) usually appear above the Card Number, on either the right or the left edge of the card.
- Only the person whose name is embossed on an American Express card is entitled to use it. Cards are not transferable.
- All American Express account numbers start with “37” or “34.” The Card Number appears embossed on the front of the Card. Embossing must be clear, and uniform in sizing and spacing. Some Cards also have the Card Number printed on the back of the Card in the signature panel. These numbers, plus the last four digits printed on the Charge Record, must all match.
- Some cards contain a holographic image on the front or back of the plastic to determine authenticity. Not all American Express Cards have a holographic image.
- The signature on the back of the card should match the customer’s signature on the Charge Record, and must be the same name that appears on the front of the Card. The signature panel must not be taped over, mutilated, erased or painted over. Some Cards also have a three-digit Card Security Code (CSC) number printed on the signature panel.

Treatment of the American Express Brand

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

- indicate or imply that it prefers, directly or indirectly, any Other Payment Products over the Card,
- try to dissuade Cardmembers from using the Card,
- criticize or mischaracterize the Card or any of American Express’ services or programs,
- try to persuade or prompt Cardmembers to use any Other Payment Products or any other method of payment (e.g., payment by cheque),
- impose any restriction, conditions, disadvantages or fees when the Card is accepted that are not imposed equally on all Other Payment Products, except for electronic funds transfer, or cash and cheque,
- suggest or require Cardmembers to waive their right to dispute any Transaction,
• engage in activities that harm the American Express business or the American Express Brand (or both),
• promote any Other Payment Products (except Merchant’s own private label card that Merchant issues for use solely at Merchant’s Establishments) more actively than Merchant promotes the Card, or,
• convert the currency of the original sale Transaction to another currency when requesting Authorization or submitting Transactions (or both).

The prohibitions stated in the previous section apply unless allowable under Applicable Law or industry codes of conduct to which American Express subscribes.

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

Note
Merchant Code 10: If you are suspicious of a card transaction, call 1-800-528-2121.
Fraud artists are constantly coming up with new ways to exploit unsuspecting merchants – from accessing cardholder information, terminal data or your terminal functions to attempting to replace your point-of-sale (POS) unit with dummy terminals and card-skimming equipment. Gaining access to just one terminal can be highly profitable for these criminals.

Impersonation Fraud

The most effective way for merchants to protect themselves from impersonation fraud is to recognize the tactics involved and know how to respond.

1. When you request technical support from Global Payments our Customer Care Centre representative will:
   - Record the technical issue
   - Confirm that a technician has been dispatched and
   - Provide you with a unique reference number identification code

2. When the technician presents himself at your place of business, you should:
   - Request the reference number identification code from the technician
   - Request his employee identification to ensure he is an authorized Global Payments technician

Without confirming these two forms of identification, never allow the technician to access your POS equipment. If you are the least bit uncertain, contact Global Payments Customer Care Centre to validate and confirm that the call for technical support was initiated and a reference number identification code assigned.

Note

Global Payments will NEVER ask you to confirm or divulge your point-of-sale terminal password. Global Payments will NEVER send technical personnel to your business unless you request a service call.

If you suspect an impersonator, immediately:
- Report the incident to your security personnel, owner, manager or supervisor.
- Report the incident to the police. (You can help the authorities by noting the individual’s physical appearance and license plate number.)
- Report the incident to Global Payments Customer Care Centre.

POS Password Protection:
- Remember to immediately change your password when you receive your POS terminal(s) and then on a regular basis thereafter.
- Never divulge your POS terminal password to non-authorized individuals.
- Never display the POS terminal password for others to find.
- Always change your password when an employee or authorized user has been dismissed or has left your place of employment.
POS Terminal Protection

- Remember to always complete an end-of-day settlement on a daily basis.
- Remember to turn off your POS terminal at the end of every business day.
- Remember to protect your POS terminal against theft by placing the device where criminals cannot reach it or have access to it.
- Inspect your POS terminal and PIN pad daily to confirm your equipment is the original provided to you by Global Canada for any signs of tampering.
- Report any suspicious activity immediately to Global Payments Customer Care Centre.

When the Card Is Not Present, Caution Should Be!

You and your staff are the most effective weapons your business has against fraud. The risk of fraud increases greatly if your customer and the customer’s credit card are not present at the time a purchase is made because you don’t have the opportunity to inspect the card. “Card not present” transactions include catalogue purchases, telephone or fax orders, and Internet sales. They can also include recurring payments, such as automatic donations and subscriptions.

Without the card in hand, you are unable to inspect the card, check for suspicious markings or verify the customer’s signature.

If you are processing card transactions by telephone, mail, fax or Internet, make sure that your Merchant Agreement authorizes you to perform these transactions where the card is not present. Even after you have the proper agreement in place, it is crucial that you take the precautionary steps to prevent potential chargebacks:

- Start by getting authorization for every transaction. This reduces the likelihood processing an expired or invalid card.
- Never ship items to hotels, office lobbies, or post office boxes. Without a permanent address, there’s no way to verify whether the shipment has been received or follow up with the customer.
- If a customer contacts you to cancel a recurring transaction, stop billing immediately.
- Protect yourself by making sure your return policy is clearly stated on your order forms, website, advertising, and catalogue materials.
- Remember all cardholder or Issuer disputes/chargebacks resulting from card-not-present sales are your responsibility and may be debited from your merchant account.

Skimming

Merchant Best Practice to Deter Skimming

What is Debit/Credit Card Skimming?
Card skimming is the transfer of electronic data from a customer’s debit/credit card to another source for fraudulent purposes.

Best Practices – Why bother?
Debit/Credit card skimming affects everyone, from merchants to customers. It is in everyone’s best interest to prevent debit/credit card skimming to avoid putting your reputation and your customers at risk.
Best Practice Activities

- Always obtain all information for each staff member, including full name, date of birth, current resident address/telephone number and SIN.
- Every new hire must complete a detailed application including previous employment, home address and references. Hiring managers should ensure that the information provided by new hires is true and accurate.
- Government-issued photo identification must be presented to the manager for each new hire. Keep a photocopy of the identification or take a picture of each new employee at the time of hiring them and maintain a copy of all new hires.
- Conduct thorough in-person interview with each new applicant. Your organization may utilize new employee testing or screening to help identify the best candidates.
- Inform each new hire that skimming is a criminal offence and will not be tolerated.

Red Flags – Be cautious if:

- the only phone number a new hire provides is a cell phone
- new hires cannot present photo ID
- new hires only want to work midnight shifts

Employee Monitoring

- Maintain accurate shift schedules, including last minute changes, for at least 12 months.
- Make employees accountable by requiring them to write their name or employee number on the back of each legitimate transaction draft.
- Make random visits during evening or weekend hours when managers are not usually present, as these are the times most card skimming occurs.
- Review surveillance films on a regular basis, especially when new hires begin work on off-peak-hours shifts.

Red Flags – Be cautious if:

- employees seem afraid to allow device inspections or to answer questions about suspicious customers or transactions.
- employee quits suddenly and leaves pay cheque behind. Alert your supervisor and/or Global Payments immediately.

Equipment and Site Inspection

- Conduct inspections daily on your POS terminals for tampering, punctured/torn security stickers.

Red Flags – Be cautious if:

- anything on the ceiling appears different (Pinhole cameras for capturing customers’ PINs can be installed in ceiling tiles.)
- ceiling tiles have been moved or if new wires appear behind the ceiling tiles
- cash registers or POS device has been removed and/or fixed in a stationary location
Fraud Protection

Equipment

• Install security seals (also called tamper proof labels) on all sides of any keyboard or POS terminal.
• Maintain an accurate and up-to-date list of serial numbers for all devices and check devices daily to ensure numbers are the same.

Communication

• Stay current on trends in card fraud by reviewing acquirer communications.
• Make sure you and your employees know the appropriate procedure to report suspicious activity and/or damaged or compromised devices.

Commitment to Best Practices

Using these principals will help protect your business and your customers. For more information please contact Global Customer Care Centre.

Don’t Be Bullied

Here, the customer attempts to intimidate the cashier by causing a fuss at the register so that the purchase is rushed, which may lead to improper check out. They may tell you that the card won’t read and not to bother running it through – that you’ll have to key it in manually. In such instances, customers have also been known to complain about the service or length of the line. They may even demand to see a manager – anything to keep the cashier’s attention off the authorization of the credit card.

By creating a tense atmosphere, the cashier is often prone to rush the person through the process just to get the customer out of the store. This is when criminal activity takes place. The result is usually a costly chargeback for the merchant.

Use only the authorization numbers provided by Global Payments. Never call a telephone number given by the cardholder for authorization.

Don’t be intimidated by these bullies; always take your time, and make sure the correct procedure is followed when authorizing the card. You may not be losing a sale by making the impatient customer wait – you may be saving your company the cost of a chargeback later.

Deceptive Deliveries

An easy way to spot a situation that may be fraudulent is to look at the delivery address. Often thieves will have a package delivered to an address that is not permanent or requires the package to be left at a front desk. Look carefully at orders that require deliveries to office complexes, hotel lobbies or post office boxes, as they are almost impossible to trace if the transaction is questioned. In this situation, it is best to call the customer and ask for a permanent address.
The Manual Key-In

Often fraud occurs when the thief damages the magnetic stripe on the card so that you are forced to manually enter the number on your point-of-sale terminal. Fraudulent cards are often damaged in order to bypass the antifraud features that are placed on them – the magnetic strip cannot be swiped and transmitted to the verification centre for authorization in the case of a manual key-in.

If you have a point-of-sale terminal, always swipe/insert every card that is presented for payment no matter how damaged or worn. Be wary of customers who let you know right away that their card won’t work or the magnetic stripe is damaged. If the card doesn’t swipe and you have to manually key in the number, ensure that you take a manual imprint of the card. If the card is severely damaged, simply ask for another form of payment.

Borrowed Cards

Beware of people presenting letters of authorization for use of a credit card that doesn’t belong to them. Under no circumstances are these letters an acceptable form of verification or authorization and should not be accepted. Friends, coworkers, spouses, and children are not permitted to borrow each other’s cards. The only person who should be presenting the card to you is the authorized user whose name is on the front of the card and signature on the back of the card. Processing transactions using these cards may result in cardholder disputes and chargebacks to you.

One Person’s Trash Is Another’s Gold Mine

The garbage is probably the last place you would think to protect. Thieves look in your trash for credit card slips, banking information, warranty information, credit applications or returned slips – anything that has personal information such as a name, address or phone number.

Your trash could be a thief’s “treasure,” with all of the information a criminal needs to make a false card, as well as information about your company that could hurt you later if it fell into the wrong hands. Recognize materials that may contain private information and dispose of them properly. Use a paper shredder to destroy any documents that have any personal information on them before declaring them trash. Protecting your customers and your business is worth a few extra seconds.

The Terminal Repair Scam

This is one of the oldest scams in the book, but also one of the most popular and most effective ways for thieves to lift confidential information. They come into your business and tell you that your POS terminal needs to be repaired – offsite. But don’t worry; they’ll replace your broken one with a loaner. Once the loaner is in place, all of the information you scan through is recorded, and now the information is theirs.

You may not even see it coming, as these criminals often pretend to work for POS companies or say that they are attending to other official business. Any attempt to repair your terminal should be reported to the police, and no replacement terminals should be accepted. The safest thing you can do is to be cautious and report any suspicious activity immediately by calling Global Payments Customer Care Centre. They will check to see if there is a service call or replacement request noted for your location.
Fraud Protection

Fraudulent Returns

Fraudulent returns are a major problem associated with fraud and theft. Staff members have been caught returning items that were never purchased and pocketing the money. In some cases, merchants don’t even realize they have been victimized until it is too late. Make sure you and your employees take the necessary steps to ensure this doesn’t happen in your business. Global Canada’s terminals can also limit access to returns by requiring the use of passwords. (See the terminal documentation.)

- Change your point-of-sale terminal password immediately after you have received the equipment.
- Keep your point-of-sale terminal passwords confidential and stored in a safe place.
- Change your password often to protect yourself in case someone does get into your system.
- Don’t share your terminal.
- Make sure to follow the proper end of day procedures to shut down your POS terminal at the end of every business day.
- Keep a record of your payment card balances and review your sales transaction activity daily to identify any problems.

International Credit Cards

Take extra care when accepting international credit cards. Thieves use foreign cards because cashiers are not as familiar with them. The criminal searches for a busy merchant who may overlook irregularities in a card issued by a foreign bank rather than become suspicious.

Inspect the card thoroughly, checking to make sure the card is valid, and always swipe/insert it. The main elements of the card – logo, hologram, chip, clear embossing and so on – should be the same despite where the card originated. Check to make sure the signature matches the name on the card, and that once swiped/inserted, the number on the terminal matches the number on the card. Also, watch out for customers who check out the cashiers first before getting in line – criminals often look for an inexperienced clerk or someone who may be easily intimidated. If anything seems suspicious during the transaction, call in a Code 10.

Office Products Scams

Watch out for companies trying to sell office products such as point-of-sale supplies, copy paper, ink cartridges, stationery and other supplies to your business. They may try to appear as if they are working for a reputable company. In reality, they will overcharge you for inferior merchandise. Deceptive telemarketing is a violation of the law – Report any suspicious persons immediately. If you have any questions about authorized suppliers for Global Payments, just call our Customer Care Centre.
Phone Fraud

Like the paper scammers, you may not see the phone fraud coming until it is too late. Of course, there are the telemarketers who use the phone to further their illegitimate businesses and scam money. But what about the criminals that aren't selling anything at all?

These crooks still use the phone to swindle merchandise from the retailer. Most of the time the criminal will phone a store, telling the clerk he has picked out the items he wants but cannot come to pick them up for some reason or another. He will ask the clerk to run his credit card through and assure the clerk that a courier will be by to pick up the merchandise. Once the merchandise has left the store, there is no way of knowing to whom it actually went or where it was going.

Often these phone fraudsters pose as respected individuals with high profile jobs and qualifications. It is not uncommon; however, to find out the person has stolen a credit card and is using someone else’s identity to receive the desired merchandise. There is no real way of knowing if the card is legitimate in a situation where the cardholder is not able to show up. It is safest to stick to the rules in these situations – Don’t take credit card numbers over the phone, and reject a credit card that is not being handed to you by its lawful owner.

Point-of-Sale Protection

Research shows that some businesses repeatedly expose their customers to fraud by asking them to provide a phone number with a credit card transaction or a credit card number as a voucher for a personal check. Remember, under the privacy legislation of some jurisdictions, your business may be liable under law for not handling your customer’s confidential information appropriately. Shield your customers from card thieves by not recording private information. If you must list the identifying information, write it elsewhere (such as your copy of the sales receipt or on a store invoice. Keep these pieces of information somewhere that is inaccessible to unauthorized personnel. Your customers will appreciate the fact that you are looking after their best interests. Thermal printers can further safeguard your customers since only the merchant copy of the sales draft will have the cardholder signature.

The Last Minute Shopper

Be on the lookout for the shopper who is purchasing expensive items just before closing time, or someone who is hurriedly filling a shopping cart with this type of item, without paying much attention to price, size or quality. These are the shoppers whose transactions need to be handled with your utmost attention.
Don’t Hesitate! Call In a Code 10

Any time you have doubts about something – a fraudulent card, a signature or even a customer’s behaviour – call in a Code 10. A Code 10 allows you to call for an authorization without the customer becoming suspicious.

After dialling the Authorization Centre, inform the operator that you have a Code 10. The operator will put you through to the correct person, who will ask you a series of “yes” or “no” questions. Hold the card in your hand if possible while making the call. If the operator decides something is amiss, he or she will deny authorization. The operator may even request to speak with the cardholder to ask account information questions that only the true owner of the card would know. A Code 10 can be used any time you feel a transaction may not be legitimate, even if you have already obtained approval on a transaction or if the customer has already left the premises.
Merchant Requirements for Securing Cardholder Information

Global Payments continues to work on your behalf to reduce payment card fraud, and offer this communication to enhance your awareness, minimize risk, and protect your customers.

The rising incidence of stolen cardholder account data is a major concern for all participants in the payment industry. As a result of these thefts, merchants and financial institutions suffer fraud losses and unanticipated operational expenses, and consumers are inconvenienced significantly. To protect your business, your customers (cardholders), and the integrity of the payment system, each of the payment networks has in place a set of requirements governing the safekeeping of account information. This document gives a brief overview of the most critical aspects of those requirements.

<table>
<thead>
<tr>
<th>Critical Aspects of Securing Cardholder Information</th>
</tr>
</thead>
</table>
| **Storage of Cardholder Information** | Store only the portion of the customer's account information that is essential to your business – i.e., name, account number or expiration date. Store all material containing this information (e.g., authorization logs, transaction reports, transaction receipts, car rental agreements, and carbons) in a secure area limited to authorized personnel. **Do not** store the following under any circumstance:  
  • Full contents of any track from the magnetic stripe on the back of the card.  
  • Card-validation code – the three-digit value printed on the signature panel of a VISA, MasterCard, American Express, Discover, JCB, or Diners Club card, and four-digit code printed on the front of an American Express card. |
| **Destruction of cardholder information** | Destroy or purge all media containing obsolete transaction data with cardholder information. |
| **Use of Agents or Third Parties (Vendors, Processors, Software Providers, Payment Gateways, or Other Service Providers) requests it).** | Advise each merchant bank or processing contact (representing each of your card brands) of any agents that engage in, or propose to engage in, the processing or storage of transaction data on your behalf – regardless of the manner or duration of such activities. Make sure these agents adhere to all rules and regulations governing cardholder information security. Any violation by your agent may result in unnecessary financial exposure and inconvenience to your business. |
| **Reporting a Security Incident** | In the event that transaction data is accessed or retrieved by any unauthorized entity, notify the merchant bank or processing contact for each card brand immediately. This report will not only minimize risk to the payment system, but protect your customers in the most responsible manner. Systems and procedures are in place to immediately stop the unauthorized use of compromised data, but are effective only when you do your part to promptly report a security incident. |
Defeating Fraud Helps You and Your Customers
Losing any amount of money to fraud is too much! From merchant chargebacks to higher operating costs, fraud affects us all. The most efficient place to prevent fraud is at the point-of-sale by making sure your employees follow these simple guidelines for every credit card transaction:

Follow procedures:

- If you are suspicious for any reason, call for a Code 10 authorization
- If you have an electronic POS terminal, always swipe/insert every card in the terminal, even if the customer says the magnetic stripe or chip is damaged. If there is no response, call for an authorization and take a manual imprint of the card. If the card looks deliberately damaged, call for a Code 10 authorization.
- If the magnetic stripe or chip is not reading, key in the number manually, take an imprint and complete the sales draft as directed.
- Always obtain an authorization at the time of sale. If suspicious, call for a Code 10 authorization.
- Ensure there’s a paper trail. With signed receipts and credit card slips, there's a good chance you can prove that the merchandise was delivered to the cardholder.

Check the card:

- Check the signature on the draft against the signature on the back of the card. If the signatures don’t match up, have the customer sign again or ask for a piece of photo I.D. If you are still not satisfied, call for authorization to confirm the validity of the card.
- Check the expiration date. Cards are often mistakenly used before their initiation date or after their expiration date.
- Always check the card to ensure it is valid by checking for card security features. Make sure the customer’s address and phone number match up. Be particularly cautious with orders when cardholders live out of the country and/or merchandise is being shipped out of the country.

Learn Fraud Signals:

- Train your staff to recognize suspicious transactions, such as orders that are much higher than usual and multiple orders on the same card in a short period of time.
- Be wary of customers who buy many items without regard for the price, size or color. They are often using a counterfeit card to load up on merchandise before it is detected.
- Watch out for “the check-out bully.” The bully’s objective is to make such a commotion that the cashier becomes intimidated and rushes the purchases through without following proper authorization procedures.
- Be suspicious of phone order requests for delivery to hotels, office complexes, and post office boxes. Items delivered to a non-residential address may be impossible to trace and could be charged back to you if the transaction is questioned.
• Thieves often purchase big-ticket items shortly before closing in an attempt to rush the sale and avoid authorization procedures.

Good Practices:

• Keep the transaction slip and the merchandise behind the counter until the sale has been completed. This prevents anyone from stealing your copy of the sales draft or from running out of the store with your merchandise if the authorization is declined.
• Never accept a letter that claims to give the customer permission to use someone else’s card. Only the authorized signatory can use the card.
• Don’t accept credit card payments over the phone, by mail, fax or on the Internet unless you have signed the applicable Merchant Agreement, which can be obtained by contacting Global Payments.

Business Owner, Beware:

• Seasonal fraud specialists who don’t have their own merchant accounts often approach legitimate merchants. They will typically offer you a kickback in exchange for depositing transactions through your account. It is important that you only process your own transactions.
• Be wary of high-pressure telemarketers who want to sell you printer paper, toner or other supplies for your Global Payments transaction solution. Purchase supplies only through an authorized Global Payments vendor.
• Make sure your staff know the proper procedures for credit card transactions and follow card acceptance procedures.
• Efficient accounting and reconciliation of your receipts can help pinpoint potential account problems quickly.
• Encourage your staff to report anyone who tries to coerce them to use or install skimming equipment and/or devices to commit payment card fraud.

Take Charge - Protection from Credit Card Fraud

Whether it’s a different twist on an old scam or a new scam altogether, there will always be someone who tries to pull the wool over your eyes. If you and your staff are well prepared with the skills to recognize suspicious transactions, and know how to correct the situation, then, you’re beating fraudsters at their own game.

Take the extra steps to stop fraud before it starts. After all, it is the merchant – not the consumer – that stands to lose the most from credit card fraud. The most important thing you can do is stay educated on the ways fraud occurs, and follow your instincts when you find yourself in a suspicious situation. The majority of the time, plain old common sense can prevent losses.

By following the information in this Guide and working together, we increase the chances of successfully protecting your business against fraud!
In the event you wish to terminate your services, please follow these steps:

1. Phone the Customer Care Centre and advise them immediately.
2. The Customer Care Centre analyst will advise you if any further action is necessary or for further instructions on returning your terminal.

Please note that early termination fees apply, depending upon the terms of your Merchant Agreement and/or your POS Equipment Agreement. In addition, it is your responsibility to return any and all point of sale (POS) equipment in good working order and to maintain the confidentiality of all related information.
Exhibit A. Visa Debit Services

1. If you accept VISA credit cards you may choose whether or not to also accept Visa Debit cards issued by Canadian issuers.
2. If you accept VISA Debit cards, you may choose whether or not to also accept Visa credit cards issued by Canadian issuers.
3. Unless you have elected not to be a Visa Debit acceptor, if you accept VISA credit cards you must accept any valid VISA credit card that a cardholder properly presents for payment, including foreign VISA Debit cards. This means that you must permit the cardholder to choose whether he or she pays for a transaction with that VISA card or with some other means of payment accepted by you.
4. If a cardholder presents a VISA card that bears a mark or logo representing another payment service:
   • You must honour the cardholder’s request if the cardholder indicated that the transaction is to be processed as a VISA transaction.
   • You may not mislead the cardholder concerning what payment service or system will be used. If you provide any information regarding the customer’s rights related to various transaction choices, that information must be accurate.
5. Where a transaction initiated with a Visa Debit card is conducted at a merchant that is not a Visa Debit acceptor, it shall not be a Visa Debit transaction. Where a transaction initiated with a Visa Debit card is conducted at a merchant where the cardholder selects another payment service, other than Visa Debit, it shall not be a Visa Debit transaction.
6. Visa Debit operates solely on the chip platform of cards issued by Canadian issuers, so you must be chip-enabled to accept such Visa Debit transactions.
7. A foreign Visa Debit card containing a chip is handled as a regular “Chip and PIN” transaction. The card is inserted into the chip-reading terminal, and the cardholder enters their PIN to complete the transaction. If the foreign Visa Debit card does not contain a chip, it is handled as a regular magnetic stripe transaction; the card must be swiped, and the cardholder must sign the transaction record.
8. Notwithstanding any authorization or approval of a transaction, Global or Member may charge back to you any Visa Debit transaction if the card issuer determines that the transaction was presented in violation of the Visa Debit rules or if such transaction is disputed by the cardholder pursuant to an applicable Visa Debit rule.
Exhibit B. UnionPay (UP) Card Services

1. You and Global Payments will mutually agree upon the schedule for the implementation of UP card processing. Global Payments will advise you of any processes to be followed regarding UP payment card processing that are in addition to or different from those processes set forth in the Merchant Agreement governing your acceptance of other credit cards and debit cards, and you agree to comply therewith. You acknowledge that the terms of the Merchant Agreement governing credit card processing and the terms of the Merchant Agreement governing debit card processing apply to the processing of UP credit cards and debit cards, respectively, except to the extent that Global Payments otherwise advises you.

2. You agree to obtain the necessary point-of-sale equipment to submit UP card transactions to Global Payments. You will use such equipment to process credit and debit cards bearing the UP logo.

3. A merchant must post a notice in an easily visible place if the merchant does not provide refund service, or the merchant uses goods of equivalent value for replacement instead of refund.

4. Global Payments is required to terminate your acceptance of UP card transactions if you unreasonably delay your response to retrieval requests.

5. In the event that you are requested to recover a cardholder’s UP card, you will use the transaction receipt as the receipt of the recovered card to the cardholder. The receipt should be in triplicate and record card number as well as reason for card capture. The three copies of the receipt are kept by the merchant, the cardholder and Global Payments. A recovered card must be immediately cut in the corner as follows: Cut in the top left corner of the back along a direction which meets the bottom edge of the magnetic strip, and forming an angle of no more than degrees. You shall notify Global Payments within three business days after the date of card recovery.
Exhibit C. Mail and Telephone Orders  (Credit and VISA Debit Card Only)

You shall provide telephone, fax or mail order services only with the express consent of Global Payments. If you intend to convert all or part of your business to telephone or mail order services, or to other services where the card is not physically present, you will provide Global Payments with days prior written notice of your intention and will wait until you receive Global Payments’ consent to the conversion before offering any of these services.

If you are providing telephone and mail order services at any time during the term of the Merchant Agreement, you shall comply with the terms and conditions relating to telephone and mail order services set forth below and any written directions issued by Global Payments relating to telephone or mail order services.

1. **Prohibitions.** You will not accept telephone and mail order payments:
   (a) without a mail order form signed by the customer or without verbal authorization from the customer (for telephone orders) that authorizes the charge to a specific card;
   (b) if you have received notification that the card has been voided or revoked; or
   (c) if the goods or services for sale are offered in violation of applicable laws, in a fraudulent manner, are contrary to public policy or have not otherwise been authorized under the Merchant Agreement.

2. **Processing.** You will not process any telephone or mail order charges or submit any telephone or mail order sale for purchase until the goods or services purchased are shipped or performed, as applicable.

3. **Procedure.** You will complete a sales draft for each mail order or telephone order, including the date of the transaction, in a form supplied or approved by Global Payments, by following the procedures described in this Guide and the Merchant Agreement, and by indicating on the signature panel of the sales draft “mail order/MO” or “telephone order/TO”

4. **Risk Allocation.** You acknowledge and understand that all sales processed where the card is not physically present are subject to an increased risk of chargeback and that obtaining an authorization is not a guarantee against a chargeback. You hereby assume responsibility and agree to pay Global for all chargebacks relating to telephone order/mail order sales and hereby agree to indemnify Global Payments and Member for all costs, fees and expenses in connection therewith.

5. **Liability.** You acknowledge and understand that you accept full liability for the identification of the cardholder on any telephone or mail order transactions.
Exhibit D. Ecommerce/Internet Services (Credit and VISA Debit Card Only)

You shall provide Internet services only with the express consent of Global Payments. If you intend to convert all or part of your business to Internet services, you will provide Global Payments with 60 days prior written notice of your intention and will wait until you receive Global Payments’ consent to the conversion before offering any of these services. If you are providing Internet services at any time during the term of the Merchant Agreement, you shall comply with the terms and conditions relating to Internet services set forth below and any written directions issued by Global Payments relating to Internet services.

1. You agree that all ecommerce/Internet transactions will be treated as telephone and mail order transactions as described in the Merchant Agreement and that, as the customer’s card is not physically present for ecommerce/Internet transactions, you may incur a chargeback on all ecommerce/Internet transactions, in accordance with the appropriate VISA, MasterCard, American Express and Discover operating rules. You also agree to abide by the terms and conditions relating to telephone and mail order services set forth in these Exhibits or as otherwise directed by Global Payments.

2. You agree that your website will display the card acceptance brand marks in full color.

3. You agree that your website will contain all the following information presented in a clear manner:
   • a complete and accurate description of the goods or services offered
   • your return/refund policy
   • your consumer data privacy policy
   • the method of transaction security used to secure cardholder account data during the payment process
   • security capabilities and policy for transmission of payment card details
   • a customer service contact, including electronic mail address or telephone number
   • transaction currency (e.g., US dollars, Canadian dollars)
   • export restrictions (if known)
   • your delivery/fulfilment policy
   • merchant’s physical address (not a post office box or mail forwarding service) for correspondence and judicial process, or in the case of a merchant that sells digital goods only, the physical address where one of the principals resides
   • merchant outlet country (must be presented at time of presenting payment options to customer)
   • your country of domicile

4. You agree to only use an electronic commerce solution for processing ecommerce/Internet transactions that is capable of providing the required information set out by Global Payments from time to time in accordance with VISA, MasterCard, American Express and Discover regulations.
   • An electronic commerce transaction must be identified in both the authorization request and the clearing record.
   • An electronic commerce merchant must provide cardholders a data protection method approved by the payment networks, such as Secure Socket Layer (SSL)
or secure cardholder authentication such as 3-D Secure (Verified by VISA) and MasterCard SecureCode.

5. You agree to include the following data on a transaction receipt completed for an ecommerce/Internet transaction:
   (a) Merchant name most recognizable to the cardholder, such as:
       - Merchant “doing business as” name (DBA, as used on your website)
       - Merchant “universal resource locator” (URL), if possible
       - Merchant name used in the VisaNet Clearing Record
   (b) Customer Service contact information including telephone country code and area code. If you deliver goods or services internationally, you must list both local and internationally accessible telephone numbers.
   (c) Merchant online address
   (d) Description of merchandise/services
   (e) Transaction amount
   (f) Transaction Date
   (g) Transaction Type (Purchase or Credit)
   (h) Purchaser Name
   (i) Authorization Code
   (j) Unique transaction identification number
   (k) Terms and conditions of sale, if restricted
   (l) Exact date free trial period ends, if offered
   (m) Cancellation policies
   (n) Return/refund policy (if restricted)

6. You agree to provide a completed copy of the transaction record to the cardholder at the time the purchased goods are delivered or services performed. You may deliver the transaction receipt in either of the following formats:
   • Electronic (e.g., email or fax)
   • Paper (e.g., hand-written or terminal-generated)

7. You agree to not return the account number to the cardholder either online or on the transaction receipt.

8. You agree not to engage in the sale of prohibited products and services or conduct business in the following areas without the specific written consent of Global Payments:
   • Online gambling and online gambling transactions (including, but not limited to, any of the following: pyramid schemes, betting, lotteries, casino-style games, funding an account established by the merchant on behalf of the cardholder, purchase of value for proprietary payment mechanisms, such as electronic gaming chips).
   • Sale of pornographic or illicit material of any type.
   • Escort services.
   • Goods and/or services prohibited by applicable law or under the rules, regulations or directives of any payment network.
9. You agree that any cardholder information, stored or otherwise, must be appropriately managed, controlled and protected and held in a secure manner to prevent access by unauthorized parties and prevent unauthorized use. This includes, but is not limited to the following:
   (a) You will provide multiple security measures to protect cardholder databases, so that if any one security control fails, it will not result in unauthorized disclosure of account and transaction information.
   (b) You must implement controls so that the cardholder Internet sessions cannot be redirected to an unauthorized website. If a cardholder is redirected to an unauthorized website, the cardholder may unknowingly disclose confidential information, account, or transaction information using strong cryptography.
   (c) You must secure all communication between the cardholder and yourself including, but not limited to, cardholder identification, authentication information, account, or transaction information, using strong cryptography.
   (d) You must ensure that databases containing cardholder information are only accessible through tested web interfaces designated for authorized users. Static passwords do not provide adequate security for system, database or application administrative access over the Internet to cardholder databases.
   (e) Your application process must never allow the user to enter unrestricted system or database commands. Application programs must never cause the application to fail in a way that allows users to enter unrestricted system or database commands.
   (f) Your customer support functions must only originate from approved networks and computers.

10. You agree that you also have in place, or will implement before commencing accepting transactions, the following additional measures to protect a cardholder database:
   (a) You will implement network access controls that prevent the system that hosts the cardholder database from being directly addressed from the Internet;
   (b) You will not open or run email attachments or other unknown files on the web or database servers from unknown sources. You will not use the web or database servers as browsers to view other website;
   (c) You will secure the account number by doing the following:
       - Using strong cryptography (preferably hardware which secures the cryptographic keys) if the account number must be decrypted on a computer system that can be addressed from the Internet; or
       - Using strong cryptography hardware or software if the account number can only be decrypted on devices not accessible from the Internet; or
       - Not storing the account and transaction information on a computer accessible from the Internet.

11. You agree that before implementing any changes on a computer system that contains account and transaction information accessible from the Internet, you will validate that the changes do not adversely effect the following:
   - Hardware that implements security controls.
• Software that implements security controls for account and transaction information. You also agree that, after implementation, you will validate that the appropriate security controls remain in effect.

12. You agree that VISA, MasterCard, American Express and/or Discover may permanently prohibit you or one of your owners, officers, partners, proprietors, or employees from participating in the VISA, MasterCard, American Express or Discover, as applicable, for any reasons it deems appropriate, such as:
   • Fraudulent activity;
   • Presenting transaction receipts that do not result from an act between you and the cardholder (laundering);
   • Activity that causes Global Payments or Member to repeatedly violate the VISA International Operating Regulations, MasterCard International Operating Regulations, American Express OptBlue Program Merchant Guide or the Discover Operating Regulations;
   • Activity that has resulted in a VISA, MasterCard, American Express or Discover Regional office prohibiting you from participating in the VISA, VISA Electron, MasterCard, American Express or Discover Program; or
   • Any other activity that may result in undue economic hardship or damage to the goodwill of the MasterCard or VISA system.

13. You agree that Global Payments, Member, VISA, MasterCard, American Express and/or Discover have the right to perform periodic audits of your website to confirm that you are adhering to the policies and procedures laid out in this agreement and any written directions issued by Global Payments.

14. You agree to perform periodic self-assessments regarding website security and data security as may be recommended or required by VISA, MasterCard, American Express and/or Discover, including but not limited to participating in the Payment Card Industry Data Security Standard (PCI DSS) program.

15. You agree to pay any fees or charges relating to ecommerce/Internet services set by Global Payments from time to time.

16. In the event of an inconsistency between the terms and conditions of this service description and any other terms and conditions of the Merchant Agreement, the provisions of this Exhibit shall prevail.

17. Risk Allocation. You acknowledge and understand that all sales processed where the card is not physically present are subject to an increased risk of chargeback and that obtaining an authorization is not a guarantee against a chargeback. You hereby assume responsibility and agree to pay Global for all chargebacks relating to ecommerce/Internet sales and hereby agree to indemnify Global Payments and Member for all costs, fees and expenses in connection therewith.
Exhibit E. Tele-Deposit Service

Tele-Deposit is a service that allows you to request authorization for transactions through a specifically designated telephone line and interactive voice response technology to deposit sales drafts electronically. If you subscribe for the Tele-Deposit service, you shall comply with the terms and conditions set forth below and follow the written directions for the proper functioning of the Tele-Deposit services given to you by Global Payments from time to time pursuant to the terms of the Merchant Agreement.

You agree to keep confidential any access codes provided to you by Global Payments in connection with the Tele-Deposit services.

If you terminate the Tele-Deposit service during the initial term of the Merchant Agreement, you agree to immediately pay the balance of the fees or charges that would have applied for that service during the remaining months of the initial term.

Risk Allocation. You acknowledge and understand that all sales processed where the card is not physically present are subject to an increased risk of chargeback and that obtaining an authorization is not a guarantee against a chargeback. You hereby assume responsibility and agree to pay Global for all chargebacks relating to telephone order/mail order sales and hereby agree to indemnify Global Payments and Member for all costs, fees and expenses in connection therewith.

Exhibit F. Pay@Pump Service (Credit and Debit Cards)

Pay@Pump is a service that permits you to accept credit cards and *Interac* Direct Payment cards for pre-authorized purchases at oil & gas retailing fuel dispensing pumps.

If you subscribe for the Pay@Pump service, you shall comply with the terms and conditions set forth below.

1. You acknowledge that each transaction in the Pay@Pump service has two parts, an authorization request and a completion. You agree that each completion shall be made within two hours of the authorization request applicable to it. If the completion is not generated within this time period, or if the completion is not received by the card issuer within hours after the applicable authorization for any reason other than Global Payments’ gross negligence, Global Payments shall not be obligated to reimburse you for the transaction. In such cases, Global Payments shall make the request for such payment from the card issuer on your behalf, and shall forward to you any amount recovered in that respect.
2. Each transaction using the Pay@Pump service will be deemed to have taken place at the time of PIN entry and selection by the cardholder of an amount.
3. You must make appropriate provision to permit cancellation by the cardholder of transactions for which an authorization request has been made. Cancellation may occur before or after the authorization response arrives at the terminal. Fees per transaction are payable to Global Payments whether or not a transaction is completed or cancelled.

4. Provision of the Pay@Pump service depends on the normal functioning of telephone and computer services used by Global Payments, Member and other persons. Neither Global Payments nor Member is responsible for the timeliness with which the financial institution may credit your account. This clause survives termination of the Merchant Agreement.

5. You acknowledge and accept the Interac security requirements for automatic fuel dispensers (AFDs) and your indemnification obligations associated therewith.

6. In the event of any inconsistency between the terms and conditions set out in this service description and any other terms or conditions of the Merchant Agreement, the provisions of this Exhibit shall prevail.

Exhibit G. Push Funds Service (Credit and Debit Cards)

The Push Funds Service is a service which allows you to have your VISA, MasterCard, American Express, Discover and/or debit sales vouchers transferred by Global Payments and Member at the end of each banking day to an account specified by you at another financial institution. If you choose to subscribe to the Push Funds Service, you must indicate such choice on the Merchant Agreement. If you subscribe to this service at any time during the term of the Merchant Agreement, you shall comply with the terms and conditions set forth below and any other written directions issued by Global Payments pertaining to the Push Funds service.

1. You authorize and direct Global Payments and Member to transfer at the end of each banking day to your account at the financial institution indicated by you on the signature page (called in this service description the “Account” and the “FI,” respectively) the value of all credit card and debit card sales drafts processed by Global Payments, less any adjustments, credit vouchers and transactions charged back to you. The parties agree that all references in the Merchant Agreement to your merchant bank account or your merchant bank account at Member shall be read as references to the account described in this Section 1.

2. You agree to execute and deliver to Global Payments and Member the “Push Funds Service Authorization and Direction” provided to you by Global Payments to authorize and direct the FI, on receipt of request from Global Payments or Member, to debit the Account at any time and from time to time for any amounts specified by Global Payments or Member representing any adjustments, items charged back, and credit vouchers and any fees or charges you owe Global Payments or Member. You agree that Global Payments or Member may provide a copy of such form to the FI on request, and your delivery to Global Payments or Member shall constitute delivery to the FI.
3. You acknowledge that, due to the nature of the Push Funds Service, Global Payments and Member cannot make any representation regarding the time frames in which your merchant bank account will be credited or debited for the net amount of your credit and debit transactions relative to the settlement window established by Global Payments for you from time to time.

4. Provision of the Push Funds service depends on the normal functioning of telephone and computer services used by Global Payments, Member and other persons. Global Payments and Member are not responsible for the timelines with which the FI may credit your account with such financial institution. This clause survives termination of the Merchant Agreement.

5. You warrant the accuracy and completeness of the above information regarding FI, transit and Account, and agree to advise Global Payments and Member in writing of any change to that information.

6. You agree to pay any fees or charges relating to the Push Funds service set by Global Payments from time to time, in addition to any other fees or charges payable under the terms and conditions of the Merchant Agreement.

7. In the event of an inconsistency between the terms and conditions of this Push Funds service description and any other terms and conditions of the Agreement, the provisions of this Exhibit shall prevail.

Exhibit H. Lodging Merchants

This Exhibit supplements the Merchant Agreement, and merchants in the lodging industry are to comply with the four sections of this Exhibit.

1. Special Authorization Procedures for Lodging Merchants

This Section 1 provides the special procedures that may be used in certain circumstances to obtain an authorization for a VISA, MasterCard or Discover transaction based on Merchant’s estimate of the total transaction amount and the additional procedures to be followed if the actual amount of the transaction exceeds, or is likely to exceed, the initial estimate by more than a specified amount. When applicable, the procedures in this Section 1 override any conflicting terms set forth in the Merchant Agreement. To use these special authorization procedures, Merchant must be engaged in providing lodging accommodations.

If Merchant is engaged in providing lodging accommodations, Merchant must estimate the amount of the transaction based on the Cardholder’s intended length of stay at check-in, the room rate, applicable tax and/or service charge rates and Merchant’s procedure for estimating additional ancillary charges.

In all other circumstances, Merchant must obtain an authorization approval code for the estimated transaction amount. Merchant must record on the guest folio and/or Sales Draft the date, amount and authorization approval code(s) obtained.
If necessary, Merchant may obtain additional authorizations for additional amounts (not cumulative of previous amounts) at any time on or between the Cardholder’s check-in date and checkout date. Merchant must record on the guest folio and/or Sales Draft or transaction record the date, amount and approval code for each additional authorization so obtained.

A final or additional authorization is not necessary to comply with basic authorization requirements if the actual transaction amount does not exceed the sum of the authorized amounts plus 15% of all such authorized amounts.

**Delivery of Sales Draft**
If Merchant alters or prepares an additional Sales Draft in order to add delayed or add-on charges previously consented to by the Cardholder, Merchant will mail a copy of the amended Sales Draft to the Cardholder with an explanation of the charges.

**2. VISA/MasterCard/Discover Reservation Service**
If Merchant is a lodging merchant (hotel, motel, or inn) and accepts VISA, MasterCard or Discover cards to guarantee reservations, Merchant must participate in the VISA/MasterCard/Discover Reservation Service and comply with all of the following procedures:

(a) Reservation Procedures.
Accept all VISA, MasterCard and Discover Cards for reservations requested under the VISA, MasterCard and Discover Reservation Service.

Inform the Cardholder that the accommodations will be held until checkout time the following day unless cancelled by 6:00 p.m. establishment time on the scheduled arrival date. For resort establishments requiring cancellation prior to 6:00 p.m. establishment time on the scheduled arrival date, the cancellation time and date may vary but must not exceed 72 hours prior to the scheduled arrival date. For Discover, resorts may move the 6:00 p.m. (local time) deadline back no more than three hours to 3:00 p.m. (local time), provided that the cardholder has been verbally informed of the date and time the cancellation privileges expire. In these cases, the Cardholder must be provided with the specific written cancellation policy including the date and time the cancellation privileges expire. If a reservation for such an establishment is made less than 72 hours before scheduled arrival, the procedure permitting cancellation by 6:00 p.m. establishment time on the scheduled arrival date must be made available to the Cardholder.

The merchant must obtain and maintain a record of the following information for the guaranteed reservation:

- Cardholder’s name as it appears on the Card, if present
- Card Number and Card expiration date, if present, unless prohibited by law
- Anticipated arrival date and length of stay
Exhibits

- The cancellation policy in its entirety, inclusive of the date and time the cancellation privileges expire
- Any other pertinent details related to the reserved accommodations

(b) Cancellation Procedures.
Accept all cancellation requests from Cardholders provided the cancellation request is made prior to the specified cancellation time.

Provide the Cardholder a cancellation code and advise the Cardholder that it must be retained to preserve his rights in case of dispute. If requested, provide the Cardholder written confirmation of the cancellation including the VISA, MasterCard or Discover account number, expiration date and name embossed on the Card, the cancellation code, date of cancellation, the name of the Merchant’s employee that processed the cancellation, and the details related to the accommodations cancelled.

(c) Scheduled Arrival Date Procedures.
If accommodations reserved under the VISA/MasterCard Reservation Service have not been claimed or cancelled prior to the specified cancellation time, the room(s) must be held available in accordance with the reservation.

If the Cardholder does not cancel the reservation or does not check in within the prescribed time, deposit a Sales Draft or transaction record for one night’s lodging plus applicable tax indicating the VISA or MasterCard account number, expiration date and name embossed on the VISA or MasterCard card, and the words “Guaranteed Reservation/No Show” on the Cardholder’s signature line. If a MasterCard card was used to guarantee the reservation, the room number assigned to the Cardholder also must be included on the Sales Draft or transaction record.

Obtain an authorization for the “No Show” transaction by following the authorization procedures for lodging transactions.

(d) Alternate Accommodations.
If accommodations reserved by a Cardholder pursuant to a guaranteed reservation or advance deposit are unavailable, the Merchant must provide the Cardholder with at least comparable accommodations for one night at another establishment.

Provide transportation for the Cardholder to the location of the alternate establishment. If requested, provide the Cardholder with a 3-minute telephone call. If requested, forward all messages and calls for the Cardholder to the location of the alternate establishment.

Provide all services in this section at no charge to the Cardholder.
(e) Record Retention.
Guest folios, pre-registration cards and reservation forms/information are considered items related to sales draft, which are required to be retained for a minimum of six (6) months after the transaction date or for such longer period of time required by then-current payment network regulations.

(f) Reservation Clerk Procedures.
Reservation Clerk requests from Cardholder:
- Cardholder name, account number and card expiration date
- Cardholder phone number and billing address
- Date of arrival and intended length of stay

Reservation Clerk provides to Cardholder during call:
- Confirmation code and the importance of keeping confirmation code for future reference
- Hotel name and location
- Accommodation request (non-smoking room, king size bed)
- Room rate and applicable taxes
- A written confirmation notice, if requested by Cardholder
- Cancellation deadline (date and time)
- Cancellation code and the importance of keeping cancellation code for future reference
- A written cancellation notice, if requested by Cardholder

3. Advance Lodging / Deposit Policy
This Section 3 provides the additional procedures for Merchant to follow if Merchant chooses to use the VISA Advance Lodging Deposit Service or the MasterCard Advance Resort Deposit service. To use these procedures, Merchant must be a lodging merchant (hotel, motel or inn) offering overnight accommodations. If Merchant uses the VISA Advance Lodging Deposit Service or the MasterCard Advance Resort Deposit service, Merchant will comply with all of the following procedures:

(a) Reservation Procedures.
Accept all VISA and MasterCard Cards for advance deposit when the Cardholder agrees to the Advance Lodging Resort Deposit Service.

Determine the amount of the Advance Lodging/Resort Deposit Transaction by the intended length of stay, which must not exceed the cost for 14 nights’ accommodation for lodging. The amount of the Advance Lodging/Resort Deposit transaction must be applied to the total obligation.

Inform the Cardholder (i) of the advance deposit requirements and (ii) of the cancellation policy requirements and (iii) that, for lodging, the accommodations will be held for the number of nights used to determine the amount of the Advance Lodging/Resort Deposit transaction.
Obtain the Cardholder’s account number, Card expiration date, the name embossed on the Card, telephone number, mailing address, and scheduled date of arrival or embarkation and, for lodging, the intended length of stay.

Inform the Cardholder that if changes in the reservation are requested, written confirmation of such changes will be provided at the Cardholder’s request.

Advise the Cardholder that (i) if he/she has not checked in by check-out time the day following the last night of accommodation used to determine the amount of the Advance Lodging/Resort Deposit transaction or (ii) the reservation was not cancelled by the specified time and date, the Cardholder will forfeit the entire amount of the Advance Lodging/Resort Deposit transaction or a portion of that amount in accordance with Merchant’s stated policy. Under no circumstances is an additional deposit of a transaction resulting from the Cardholder’s failure to cancel or use the reservation allowed under the Advance Lodging/Resort Deposit Service.

Quote the rate of the reserved accommodations, the amount of the Advance Lodging/Resort Deposit transaction and the exact Merchant location. Provide the Cardholder with a confirmation number (advising that it must be retained) and with the actual date and time the cancellation privileges expire.

Complete a Sales Draft or transaction record for the amount of the advance deposit, indicating the Cardholder account number, Card expiration date, the name embossed on the Card, the Cardholder’s telephone number and mailing address, the words “Advance Deposit” on the signature line, the Cardholder’s confirmation number, the scheduled arrival or embarkation date, and the last day and time the cancellation privileges expire without forfeiture of the deposit if the accommodations are not used.

Follow normal authorization procedures for lodging transactions, as applicable; but regardless of any otherwise applicable floor limit, all advance deposits made with MasterCard Cards must be authorized if the amount exceeds $50.

If the authorization request results in a decline, so advise the Cardholder and do not deposit the Sales Draft.

If authorization is approved:
Mail the Cardholder copy of the Sales Draft and the written lodging cancellation policy to the address indicated by the Cardholder within three business days from the transaction date. Submit the Sales Draft or transaction record in accordance with usual procedures as specified in the Agreement.
If a Merchant accepts Discover Cards and takes advance deposit for reservations, Merchant must comply with the following requirements:

- The amount of the deposit may not exceed the cost of seven (nights lodging (plus applicable taxes) and the deposit must be applied to the Cardholder’s entire bill.
- Hold reserved accommodations until checkout time following the last day covered by the advance deposit.
- Specify a reservation cancellation time frame including the date and time when cancellation privileges expire.
- Fully reimburse an advance deposit when the Cardholder cancels a reservation within the specified time frame.
- Provide a written disclosure informing the Cardholder of his or her rights and obligations and that failure to cancel a reservation within the specified timeframe may result in forfeiture of all or part of an advance deposit.

(b) Cancellation Procedures.
Accept all cancellation requests from Cardholders provided the cancellation request is made prior to the specified cancellation date and time.

Provide a cancellation number and advise the Cardholder that it must be retained to preserve his/her rights in the case of a dispute.

For the cancellation of a lodging reservation, complete a Credit Voucher for the entire amount of the Advance Lodging/Deposit transaction. Include on the Credit Voucher the Cardholder account number, Card expiration date, the name embossed on the Card, mailing address, the cancellation number and the words, “Advance Deposit” (if VISA) or “Deposit Cancellation” (if MasterCard) on the signature line.

Mail the Cardholder a copy of the Credit Voucher to the address indicated by the Cardholder within three business days from the transaction date.

(c) Alternate Accommodations (VISA Advance Lodging Deposit Service only)
Lodging Merchants must comply with the following provisions for VISA Card transactions:

- If accommodations that were reserved under the Advance Lodging Deposit Service are unavailable, complete and deliver to the Cardholder a Credit Voucher for the entire amount of the Advance Lodging Deposit Transaction.
Provide the following services at no charge to the Cardholder:

- At least comparable accommodations at an alternate establishment for the number of nights used to determine the amount of the Advance Lodging Deposit transaction, not to exceed nights, or (ii) until the reserved accommodations are made available at the original establishment, whichever occurs first.
- Transportation to the location of the alternate establishment and return transportation to the original establishment. If requested, transportation to and from the alternate establishment must be provided on a daily basis.
- If requested, two three-minute telephone calls.
- If requested, forwarding of all messages and calls to the location of the alternate establishment.

**d) Reservation Clerk Procedures – Sales Draft Checklist**

To accept an Advance Deposit reservation, the reservation clerk must explain the terms of the reservation, cancellation, and refund policy procedure to the cardholder or travel agent.

To process an Advance Deposit reservation, the reservation clerk or travel agent completes a sales draft filling in the merchant identification and cardholder information as listed below. It is recommended that the merchant note on the sales ticket any special terms and conditions regarding its refund policy. Send the cardholder a written reservation confirmation, a copy of the sales draft, and your cancellation and refund policy.

NOTE: Merchants must properly identify the prepayment date as the transaction date when submitting Advance Deposit transactions.

Reservation Clerk requests from Cardholder:

- Cardholder name, account number and card expiration date
- Cardholder phone number and billing address
- Date of arrival and intended length of stay

Reservation Clerk provides to Cardholder during call:

- Confirmation code
- Total amount of advance deposit
- Advance deposit requirements, cancellation policy requirements and the actual date and time that the cancellation privileges expire

Reservation Clerk provides transaction information to Cardholder on Sales Draft:

- Transaction date (date of prepayment)
- Authorization code
- “ADVANCE DEPOSIT” on signature line
- Hotel merchant name and location
- Scheduled arrival date and intended length of stay
• Cancellation deadline (date and time)
• Written cancellation policy
• Mail copy to guest.

Reservation Clerk Procedures -- Credit Voucher Checklist
• To process an Advance Deposit Cancellation, Merchant uses a credit voucher (or Merchant’s terminal and printer) and Reservation Form. Mail a copy of the credit voucher reflecting the cancellation to the cardholder
• Cardholder name, account number and card expiration date
• Cardholder mailing address
• Advance Deposit cancellation code
• Total amount of credit
• Write “ADVANCE DEPOSIT” (for VISA) or “DEPOSIT CANCELLATION” (for MasterCard) on signature line.
• Mail copy to guest.

4. Priority/Express Check-Out Service
This section provides the procedures for Merchants to follow if Merchant chooses to offer Priority/Express Check-Out Service. If Merchant offers Priority/Express Check-Out Service, Merchant will comply with all of the following procedures.

Priority Check-Out Procedures. (VISA and MasterCard Only)
1. Accept all VISA and MasterCard Cards when a Cardholder requests the Priority/Express Check-Out Service for lodging.

2. Provide the Cardholder with a Priority/Express Check-Out Agreement, which must include, but is not limited to, the following information:
   • Embossed card data
   • Hotel name
   • Hotel city and country (and state/province, if applicable)
   • Transaction amount indicated in transaction currency
   • Identification of transaction currency
   • Transaction Date
   • Description of goods or services (optional)
   • Space for Cardholder signature
   • Space for guest check-in date
   • Space for guest check-out date
   • Space for room rate
   • Space for salesperson’s initials
   • Authorization dates, amounts and approval codes (if applicable)

3. Inform the Cardholder that the Priority/Express Check-Out Agreement must be completed and signed; the mailing address must be included to receive a copy of the hotel bill supporting the final transaction amount.
4. Obtain the completed Priority/Express Check-Out Agreement and ensure the Cardholder account number identified is identical to the account number imprinted on the Sales Draft or transaction record.

5. On the Cardholder's date of departure, complete the Sales Draft indicating the total amount of the Cardholder's obligation and the words “Priority Check-Out” (for VISA) or “Signature on File -- Express Checkout” (for MasterCard) on the signature line.

6. Follow normal authorization procedures for lodging transactions.

7. At Cardholder's request, provide the Cardholder a copy of the Sales Draft, the itemized lodging bill, and the signed Priority/Express Check-Out Agreement -- either on-site or mailed to the address provided by the Cardholder on the Priority/Express Check-Out Agreement within three business days of the Cardholder's departure.

**Priority Check-Out Procedures. (Discover Only)**

1. Require the Cardholder to sign the registration card at the time of check-in acknowledging for all charges.

2. Obtain an Authorization for the estimated amount of the accommodations at check-in.

3. Complete Sales Data at checkout by entering the total amount of charges incurred during the stay, including restaurant bills, telephone charges, convenience bar charges, missing item fees and miscellaneous expenses.

4. Write the words “Priority Checkout” on the Cardholder signature line of the Transaction Documentation.

5. Obtain a final Authorization Code for any additional amounts from the check-in estimate to equal the total amount to be billed to the Cardholder.

**Record Retention.**

The itemized lodging bill and the signed Priority/Express Check-Out Agreement supporting a Priority/Express Check-Out transaction must be retained for a minimum of six months after the transaction date or for such longer period of time required by then-current payment network regulations.
**Address Verification Service (AVS)** is a service that verifies the cardholder’s billing address in order to help combat non-face-to-face fraud.

**AFD** is an automated fuel dispenser device – point-of-sale payment processing equipment used by oil and gas merchants.

**Authorization** is a number or code obtained by you when a credit card transaction is accepted by the issuer of such credit card. Authorization is based on the cardholder status and available credit. The authorization number/code is always included on the merchant sales draft.

**Authorized User** is a person, other than the cardholder, whose signature appears on a card.

**Average Ticket Price** is the average value per credit card or debit card transaction processed by you.

Banking Day is any day the bank branch where you have your merchant bank account is open for business (excluding Saturdays, Sundays, and holidays).

**Card** is any credit card or debit card approved by Global Payments.

**Cardholder** is the person whose name is embossed on a card.

**Chargeback Fees** are fees that the cardholder bank may collect for items that result in a chargeback. A merchant may be subject to the Association Chargeback Fees if the merchant failed to follow card acceptance and authorization procedures and the card issuer has a valid chargeback.

**Chip Card** is a credit or debit card that contains an embedded computer microchip that securely stores encrypted confidential information such as the cardholder’s account number and Personal Identification Number (PIN).

**Chip-Enabled** is a description for equipment that is certified as being compliant with the industry-standard specifications for processing chip cards.

**Code 10** is a universal code that provides merchants with a way to alert the Authorization Centre that a suspicious transaction is occurring without alerting the cardholder (or other person presenting the bankcard). The Code 10 operator asks a series of questions that can be answered with yes or no response. Follow the operator’s instructions. NEVER ENDANGER YOURSELF.
**Commercial Card** is a business card, corporate card, fleet card or purchase card issued for commercial use, often with a higher discount expense than consumer cards.

**Consumer Card** is a card issued to a consumer.

**Contactless (or proximity payment)** is a payment functionality that uses radio frequency ("RF") technology to exchange transaction data between a chip card and an RF-enabled POS terminal, permitting card or device transactions without swiping the magnetic stripe or using a contact chip interface. The payment networks' proprietary names for such functionality are MasterCard PayPass™ and Visa payWave™.

**Credit Card** is a valid and unexpired card approved and processed by Global Payments under your Merchant Agreement. This term may also be used to refer to offline signature-based debit cards, which do not require the cardholder to enter a PIN, and which are processed by the merchant in the same manner as credit card transactions.

**Credit Voucher (or Credit Draft)** is a record of a return or refund transaction presented to Global Payments by the merchant for processing by debiting the merchant bank account and crediting the cardholder’s account.

**Data Storage** is the temporary or permanent retention of account data in any form (including logs) for subsequent processing, retrieval, or other use.

**Data Storage Entity (DSE)** is any entity other than the acquiring Member, merchant, or TPP that stores MasterCard account data on behalf of merchants, web hosting providers, and payment gateways. They may include terminal drivers and processors. Storage may be temporary or permanent and in any form (including logs).

**Debit Card** is a card providing access to the Interac Direct Payment service or such other debit network organization approved and processed by Global Payments under your Merchant Agreement. In the case of Interac Direct Payment service, the user must be in possession of both the card and its corresponding PIN. Please refer to “credit card” definition above for signature-based debit card transactions.

**Draft Deposit Service** is a service that lets you use a point-of-sale terminal to deposit sales drafts and credit vouchers to your merchant bank account.

**Electronic Commerce (or ecommerce) Transaction** is a transaction conducted over the Internet or other network using a cardholder access device, such as a personal computer or terminal. Additionally, such transactions may be referred to as web-based transactions or E-business.
**EMV** refers to chip standards managed by EMVCo, formed by **Europay International**, **MasterCard International** and **VISA International**. EMVCo’s primary role is to manage, maintain and enhance the EMV Card Specifications to ensure worldwide interoperability and universal acceptance of chip payment cards.

**End of Day** is a procedure where you instruct the terminal to transfer funds to your merchant bank account.

**Equipment** is an imprinter, point-of-sale (POS) terminal, printer, or any other device approved by Global Payments for transactions covered by your Merchant Agreement.

**Extending Credit** means allowing customers to purchase goods and services from you using a MasterCard or VISA card.

**Factoring (or Draft Laundering)** is a merchant’s presentation to Global Payments of what would otherwise be a sales draft but is not, because the underlying transaction is not between the merchant and the cardholder.

**Floor Limit** is the maximum amount of any single credit purchase you can accept without obtaining an authorization from Global Payments. Unless otherwise noted, the floor limit is zero. However, payment networks have established higher floor limits for qualifying quick-pay transactions, which floor limits are subject to modification from time-to-time by the payment networks.

**Interac Direct Payment service** means allowing customers to pay for goods and services by debiting money directly from their accounts using a point-of-sale terminal with PIN verification.

**Issuer** means the financial institution that holds a contractual agreement with, and issues a card to, the cardholder.

**Link** is the network between the point-of-sale station and Global Payments’ host computer.

**Magnetic Stripe** is the stripe on a bankcard of magnetically encoded cardholder account information.

**Member** is the bank that is party to your Merchant Agreement for the purpose of complying with operating rules and regulations of the applicable payment network, e.g., National Bank of Canada for MasterCard International and Canadian Imperial Bank of Commerce (CIBC) for VISA International and VISA Canada.

**Merchant Bank Account** (sometimes referred to herein as a “deposit account”) is an approved account maintained at a Member branch or another financial institution that you have designated in writing as an account for VISA, MasterCard, other credit card deposits, and **Interac** Direct Payment transactions.
**Glossary of Terms**

**PCI Self-Assessment Questionnaire** is a compliance questionnaire required annually for merchants, Third Party Processors and Service Providers) to determine adherence to PCI DSS.

**Personal Identification Number (PIN)** is a cardholder’s individual, confidential code, known only to such cardholder, which is used to verify the cardholder’s identity and to activate an *Interac* Direct Payment transaction at the point-of-sale.

**PIN** is a Personal Identification Number.

**PIN Pad** is the equipment into which a cardholder enters a PIN to verify his or her identity.

**Point-of-sale (POS) Terminal** is the electronic device located on your premises that you use to authorize credit card transactions, deposit credit card sales drafts, and process *Interac* Direct Payment transactions.

**Point-of-sale Station** is a terminal, printer and, if appropriate, PIN pad which are inter-connected at your premises.

**POS** stands for “point-of-sale.”

**Printer** is the equipment that produces a record of a transaction.

**Proximity Payment (or contactless)** is a payment functionality that uses radio frequency (“RF”) technology to exchange transaction data between a chip card and an RF-enabled POS terminal, permitting card or device transactions without swiping the magnetic stripe or using a contact chip interface. The payment networks’ proprietary names for such functionality are MasterCard *PayPass™* and Visa *payWave™*.

**Receivables** are the amounts owing to you by VISA, MasterCard, American Express, Discover, *Interac*, or any other payment network as a result of a transaction processed under the terms and conditions of your Merchant Agreement.

**Recurring Payments** are a series of transactions in which sales drafts are processed by the merchant on an ongoing basis unless and until the arrangement is cancelled by the cardholder.

**Reserve Account** is an account established by Global Payments or Member to secure the performance of your obligations under your Merchant Agreement.

**Retrieval Request** is the request for either an original or legible copy of the transaction information document or substitute draft as identified in the electronic record.
Sales Draft (sometimes referred to herein as a “transaction receipt”) is a paper or electronic record of a sale, rental or service transaction that the merchant presents to Global Payments for processing so that the cardholder’s account can be debited and the merchant bank account may be credited.

Terminal is the equipment that meets Global Payments’ specifications and into which you enter information with respect to a transaction.

Third Party Processor (TPP) is a MasterCard Third Party Processor requires registration directly with MasterCard if the TPP provides services to MasterCard member financial institutions.

Third Party Servicer (TPS) is a VISA Third Party Servicer that includes non-members other than the merchant and processor that receive, pass, or store transaction data on their internal systems on behalf of the Member, the merchant, or another Third Party. TPS includes merchant vendors, including web hosting company or shopping cart, and media back-up company. These merchant vendors are classified as Merchant Servicers. Also includes Independent Sales Organizations (ISO), loyalty program vendor, risk management vendor, chargeback vendor and credit bureau that provide services to member financial institution or its merchants.

Transaction is any sale that is paid for with a card, or any adjustment or return that is credited to a card.

Truncation is a printer’s suppression or masking of a card’s expiration date and all but four digits of the account number on the cardholder receipt.

TSTR means the Interac-specific technical specifications and testing requirements.

UnionPay (UP) means the payment network headquartered in Shanghai, China as a bankcard network operator for processing inter-bank and international bankcard transactions.

Visa Debit Service means allowing customers to pay for goods and services by debiting money directly from their accounts using a point-of-sale terminal with PIN verification of the customer’s Visa Debit card.

VisaNet Processor is a processor Member, financial institution or merchant directly connected to VISA’s proprietary network for transaction authorization. A non-member processor VisaNet registration and member financial institution processor designation are required by VISA.

Voice Authorization is the authorization of a transaction that is obtained by telephoning a Global Payments voice operator.