People's United Merchant Services

A subsidiary of People's United Bank®

Welcome to Payment Processing

Growing your business just got easier

It's our pleasure to serve you

Thanks for choosing us for your payment processing needs. We are honored that you put your trust in our company and our people. Your business is important to us, and we look forward to helping you reach your goals.

Our customer support teams are staffed with courteous, well-trained personnel to assist with any questions. This merchant processing guide includes important processing information, quick tips and best practices to get you up and running and help you along the way. This guide also includes basic information on how to activate your account, access reports, and help protect your valuable information.

We are excited about the opportunity to support your card processing needs and assure you of our strong commitment to quality service and product support.

So, let's get started.

Resources at your fingertips

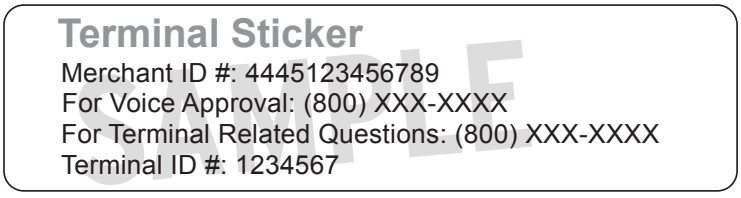
Welcome kit

We are excited that you have selected us as your solution for bankcard processing and wish you success and profit in the years to come. Your welcome kit contains the tools that will assist you in the process of accepting transactions electronically or on paper (if you are not utilizing a point-of-sale terminal). Your kit contents will vary depending on your processing needs and may include a welcome letter, processing guide, Quick Reference Card, plus some of the items described below.

Please note, if you are receiving a dial terminal via purchase, lease or rental, or are re-programming an existing terminal, you will receive a terminal sticker and Quick Reference Card. If you are receiving equipment, the terminal sticker is not in the welcome kit, it is on the device. If you are utilizing a value added reseller, you will not receive a terminal sticker or a Quick Reference Card.

Equipment sticker

This sticker contains two important telephone numbers. One is to obtain a voice authorization, and the other is to contact our Merchant Technical Support department, staffed 24 hours per day, seven days a week. Please discard any previous voice authorization procedures and/or stickers you may have. This process should only be used when you are unable to authorize electronically. The phone numbers on the merchant sticker are the telephone numbers provided specifically for you. If for some reason you lose your sticker, please refer to the enclosed Quick Reference Card.



Terminal quick reference guide

This guide will walk you through the most commonly used functions on your point-of-sale terminal. Please keep your guide near your terminal for quick access.

Sales/credit drafts

Sales/credit drafts may be used for manual processing or when a printer receipt is not available.

Decals

Decals should be displayed within your business to identify the card types you have elected to accept.

Activation

Let's get down to business. Activating your merchant processing account is the first step.

Many of you will have the support of our Merchant Activation Team (MAT), a highly trained group of individuals who will get you up and running right away. Or, if your account was sold to you via an independent representative, your representative will have left you their contact information.

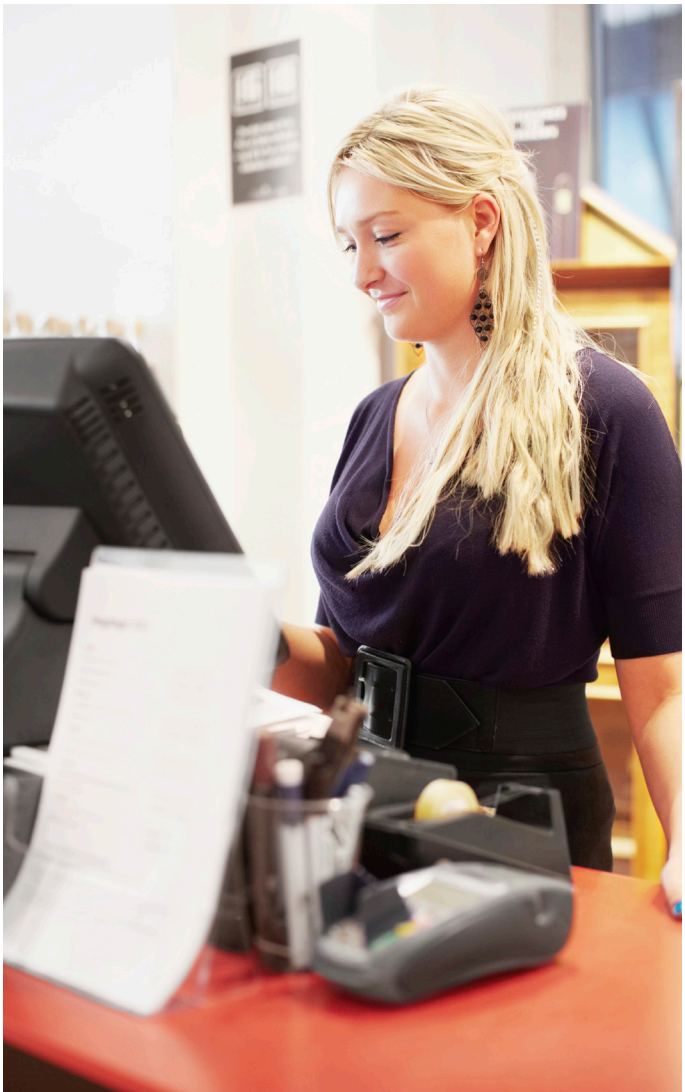
If you receive your equipment or you already own your own point-of-sale hardware, please contact the MAT.

- A representative will help you with re-programing your equipment and/or any training needs you might have right away.

If you're using software or a PC-based system, contact the MAT to confirm receipt of your setup sheet.

- The MAT will assist you in working with your vendor to make sure you're ready to process transactions as soon as possible.

When you call, please have your MERCHANT ID or CHAIN NUMBER ready. You'll find these numbers on your equipment packing slip or on your terminal sticker.



Online data and reporting

Success is about creating advantages. Analyzing and managing the data behind your payment processing program is the most effective way to deliver customer service and profitability. That's a competitive advantage for you and your customers.

We have an innovative online management tool that brings important data to your desktop when you need it most. Log in to iQ at accessmyiq.com and you can quickly and efficiently manage your merchant data in an environment with increased security.

Getting started

If you have selected iQ as part of your product set, then you will automatically receive an email with your logon instructions once you start processing with us. When it arrives, simply click on the link in the email to get started.

Once you are in accessmyiq.com, and need help, just click on the Help link in the right-hand corner of the screen for information on getting started, watch how-to-videos and other helpful features.

Key features

- View summary data including settlement, ACH deposits, authorizations and rejects for up to 36 months.
- Research card activity for up to 18 months.
- Access online reports and billing statements.
- View chargeback and retrieval data, including status and images associated with the case.
- Receive proactive alerts to keep you updated on key items.

Payment processing services

You know your business better than anyone. You know exactly what it takes to keep your customers coming back. We can help you protect and strengthen your customers' relationships. We want to understand you, your business and what you want to achieve. All of our products and services work independently or together to make sending and receiving payments simpler for you and your customers.

Card acceptance

We have direct links to all major networks. We make payments simple for your customers with credit, debit and EBT options. The more options you provide, the more your business can grow.

Gift card solutions

Gift giving made simple. Simple for consumers, simple for you. Enjoy increased sales and revenues by adding gift card solutions to your customers' wish lists.

Check services

For consumers who prefer check payments, we have electronic and paper check processing services to keep them satisfied, and help keep your costs and risks to a minimum.

Data security solutions

You don't have to sacrifice growth and productivity to make security a priority. We have programs and resources to help you protect your business while keeping a step ahead of the threats and the competition.

Technology features

Technology is a tremendous enabler; however, it comes with concerns about reliability and security. We can help you maintain smooth operations with increased security with our integrated technology platform and the latest in secure software and hardware systems.

Mobile solutions

The age of mobile payments is taking hold. As more and more businesses and consumers adopt mobile devices, the more these devices will be used in new types of payment scenarios. Your business needs to be ready.

Card data security

Merchants like you have important data security responsibilities. If you process, store, or transmit cardholder data, you must comply with the Payment Card Industry Data Security Standard (PCI DSS). If you don't comply – and validate your compliance annually – you could lose your ability to offer these services.

We understand that PCI DSS compliance can be intimidating. That's why we offer the following services that provide access to easy-to-use tools to help simplify PCI compliance and provide financial protection in the event your business suffers a breach.

PCI Assist

We have partnered with Trustwave®, an industry leader in information security and compliance, to bring you PCI Assist. PCI Assist is a set of online tools that have been specially developed with **Level 4 Merchants*** in mind. It can help you implement basic security requirements, adopt best practices and follow important steps that lead to your PCI DSS compliance and validation.

Here's how PCI Assist works:

1. Navigate to PCI Assist at **https://pci.trustwave.com/pci-assist**.
2. You'll then register in TrustKeeper®** for a customized experience based on the way you process payments.
3. You'll be asked simple questions to determine how you accept credit card payments.
4. TrustKeeper will point you to the correct PCI wizard that corresponds to your business. The PCI wizard steps you through your Self-Assessment Questionnaire to validate compliance. It will also let you know if Vulnerability Scanning is necessary.

That's it. A few simple steps and you are on your way to protecting your business. Remember, it's important that you log in to PCI Assist and validate your compliance as soon as possible, ideally within 90 days of signing up with us.

*Level 4 Merchants are those processing less than 1 million transactions annually from all acceptance channels with one card brand, or those processing less than 20,000 electronic commerce transactions annually with one card brand.
**TrustKeeper PCI Manager is a registered trademark of Trustwave Holdings, Inc.; use of this solution requires your agreement to terms of use directly between yourself and Trustwave Holdings, Inc

Breach Assist

Our Breach Assist program protects you from certain financial losses your business can incur with an actual or even suspected cardholder data breach. With Breach Assist, you're provided an indemnification waiver for losses of **up to $100,000** per merchant location and **$500,000 per incident***.

Breach Assist helps with critical breach related expenses like forensic audit expenses, issuer card replacement and issuer monitoring costs, card-brand fines, and account data compromise recovery costs. The program also covers forensic expenses related to certain types of employee card fraud and card skimming if that type of investigation is ordered by the card brands.

Breach Assist also includes **up to $25,000** for post-breach hardware and software upgrades that involve investment in new payment card industry technologies such as EMV dual interface terminals, point-to-point encryption solutions and tokenization solutions.

*We are not an insurance company and Breach Assist is not insurance. Breach Assist provides a contractual indemnity waiver for amounts merchant would otherwise be contractually obligated to reimburse/indemnify us and is subject to the terms and conditions of participation in the program.

Card acceptance

There is a difference between the right way and the wrong way to process payments at the point-of-sale. Depending on what industry you're in, these differences can have a very big impact on your fees, risks and expenses.

The following is a guide to processing payments. For more information, please visit our helpful online how-to videos and documents. Our skilled and knowledgeable customer service representatives are also available to assist you.

In general, transactions fall into two categories:

Card Present:
The consumer's card is presented in a face-to-face environment

Card-Not-Present:
The consumer's card is not present at the point-of-sale

Card present best practices
(retail, restaurant, etc.)

1. Validate the physical card

- Verify that the "valid from" and expiration dates are current.
- Check to see that the card is signed on its signature block.
- If applicable, determine that the user of the card resembles any photograph on the card marked for identification.
- Printing on card appears distinctly and clearly, and letters are not fuzzy or crooked.
- Embossed characters are straight, correctly spaced and uniform in size, height, style and alignment.
- There are no signs of tampering or alterations on the signature panel, the security hologram, any of the embossed numbers or the magnetic stripe.
- Signature panels do not appear discolored, glued, taped or painted. Any attempts at erasure should expose the word "VOID."
- The embossed account number is the same as the number displayed and/or printed by the terminal if you are using a terminal that reads and displays, or reads and prints, the magnetic stripe information on the card.
- If you have this security feature, the last four digits of the cardholder's account number that you manually key into the terminal or point-of-sale software match the terminal display.

2. Swipe or dip the card through the point-of-sale system

Avoid key entry whenever possible. If you must enter numbers manually, be sure to get an imprint of the card and include the CVV2/CVC2/CID in the authorization request. If an imprint of the card is obtained, it is imperative that those receipts are locked and secured at all times. You are responsible for any misuse of cardholder information.

3. Authorize the transaction

- ALL transactions must be authorized.
- Review the authorization response and take the appropriate action:

Response	Action
Approved	Ask the customer to sign the sales receipt
Declined	Return the card to customer and ask for another form of payment. Do not re-attempt the transaction.
Call or Call for a voice authorization	Please refer to the Quick Reference Card for phone number
Pick Up	Keep the card if you can do so peacefully

NOTE:
If anything about the card or the card user is suspicious, call the voice authorization operator with a "Code 10" authorization request. The operator will ask you a series of questions designed to determine if the card or card user is fraudulent. These questions are deliberately asked so as not to alarm or alert your customer. Be sure to follow the operator's instructions precisely, but don't place yourself or anyone on your staff in physical danger by confronting a customer. If a cardholder refused to allow you to retain the card, do not engage in any physical confrontation.

4. Request a signature and be sure that the signature on the transaction receipt matches the signature on the card

- A signature is not always required on certain small ticket transactions. Check with the Contact Center for more details.

5. Settle the transactions daily

- Depositing or settling your transactions is the process that provides you with payment for card transactions that you accept. For electronically processed card transactions using a terminal, you should balance and transmit transactions to the designated process at least daily.

Card-not-present best practices

(phone order, e-commerce, etc.)

1. Authorize the transaction

- Verify that the "valid from" and expiration dates are current.

2. Utilize fraud prevention tools such as:

- Address Verification Service (AVS) to check the cardholder's address given at the time of the sale against the address on file with the cardholder's bank.
- CVV2/CVC2 to verify the security code located on the signature panel of the card.
- If you receive an authorization but are suspicious of fraud, ask more questions.
- Remember, it's your responsibility to assure you're dealing with a legitimate cardholder. If you don't take these fraud protection steps, you could be putting your business at risk.

3. Ensure timely processing between the time the order is placed and the time you deliver the goods

- Your transaction date should be the same as your shipment date and not be greater than 7 days from the authorization date.
- Do not charge your customer before you have shipped your goods.

4. If you process transactions via the Internet on a PC-based system, your system must be configured to send proper attributes required by the card brands.

- These attributes include but are not limited to the eCommerce indicator. With this indicator, you are providing data that will assist you in qualifying for the best processing rates available.

5. Settle the transactions daily

Card acceptance best practices information is high level and not inclusive of all data elements required to qualify for optimal interchange qualification or fraud prevention.

Voice authorization procedures

It is recommended that you use voice authorization procedures for the following reasons:

- You process paper transactions (non-electronic).
- You are unable to obtain an authorization through your point-of-sale terminal.
- You receive the message "Call Center" on your point-of-sale terminal.

Please follow the procedures below when calling for a voice authorization:

- Dial the Voice Authorization Center toll-free number located on your voice authorization sticker.
- Our automated voice authorization system may ask for the following:
  - Your MERCHANT ID
  - Cardholder account number (the account number is 13-16 digits in length)
  - Card expiration date (the date is four digits in the format of MMYY)
  - Dollar amount of the transaction (provide the amount in U.S. dollar and cents)
- If approved, you will be provided with an authorization number. Record number on sales draft.
- To complete the transaction, obtain a manual imprint of the card using the same draft where the caller recorded the authorization number. Once you receive an approval, request that your customer sign the sales draft.
- If you obtained a voice authorization due to a terminal malfunction, hold all drafts until your replacement terminal arrives, **then manually enter all transactions using the off-line function key** (refer to your Terminal Quick Reference Guide for proper procedures).

Authorize the transaction.

- ALL transactions must be authorized.
- Review the authorization response and take the appropriate action:

Response	Action
Approved	Ask the customer to sign the sales receipt.
Declined	Return the card to customer and ask for another form of payment. Call for a voice authorization.
Pick Up	Keep the card if you can do so peacefully.

Please follow the procedures below when calling for an Address Verification (AVS):

- Dial the Voice Authorization Center toll-free number located on your voice authorization sticker.
- Please have the following information available:
  - Your MERCHANT ID
  - Cardholder account number (the account number is 13-16 digits in length)
  - Card expiration date (the date is four digits in the format of MMYY)
  - Street number (up to the first five numbers, example, if address is 123 Main Street, enter into the system 123)
  - Zip code (five or nine digits)

Wait for a response. The system indicates whether the address and zip code match, are partially correct, or are invalid. (Consult your company guidelines for appropriate action regarding invalid address information.)

Handling returns and exchanges

It is important to properly display your store return policy. It helps to limit returns and maintain your chargeback rights.

It's a good idea to noticeably display your return and exchange policies in the store, and also print them on sales receipts. Network rules may require you to refund a transaction if your policies are not clearly made known and posted as No Returns, Store Credit Only or Exchange Only.

- Ask for the customer's receipt and card used for the original transaction. The credit must be applied to the card used for the original transaction.
- Follow the appropriate steps to process the credit transaction.
- Provide the customer with the cardholder copy. File the merchant copy.
- If at any point you suspect fraud, contact Voice Authorizations for a Code 10 call and follow the operator's instructions.

Additional guidelines

1. If you maintain a policy of permitting refunds, exchanges, returns or adjustments for cash customers, you must maintain the same policy for persons making purchases using a card. If you set any limits on refunds or returned merchandise, they must be clearly disclosed to the cardholder at the time of the sale on the sales draft.

2. You may limit acceptance of returned merchandise and canceled services, or establish a policy of making price adjustments, if you make proper disclosure and deliver the purchased goods or services to the cardholder at the time of the card transaction. You have made proper disclosure at the time of the card transaction if the following or similar words are legibly printed on all copies of the sales draft being presented to the cardholder for signature:

    - "No refund" – Merchant will not accept merchandise in return or exchange and will not issue a refund to a cardholder.
    - "Exchange only" – Merchant will only accept merchandise in immediate exchange for similar merchandise or a price equal to the amount of the original card transaction.
    - "In-store credit only" – Merchant will accept merchandise in return and will deliver to the cardholder an in-store credit for the value of the merchandise returned, which may be used only in the merchant's place of business.
    - Whichever policy you select must appear in letters approximately 1/4 inch high and in close proximity to the space provided for the cardholder's signature, and the sales draft must be signed by the cardholder.

3. Card transactions completed as telephone order, mail order, Internet order or any other transactions are not face-to-face between you and a cardholder cannot be covered by any restrictive return policy for which verification of proper disclosure cannot be made. For Internet orders, the website must have a "click to accept" or other acknowledgment button that the cardholder must use to show acceptance of the return and exchange policies.

4. You must deliver to us a credit voucher for a refund or adjustment to the cardholder account and deliver to the cardholder a copy of the credit voucher at the time the refund or adjustment is made. You must include the refund date and amount, cardholder account number and a brief description of the refund or adjustment on the credit voucher, in sufficient detail to identify the card used and the original transaction. The amount of the credit voucher must not exceed the amount of the original transaction, except for any amount that you agree to reimburse the cardholder for return postage.

5. You should not make a refund or adjustment for a card transaction in cash, except when required by law. You may not deliver a credit voucher to us for any refund or adjustment of a purchase not originating as a card transaction with the same cardholder requesting the refund or adjustment, a card transaction not made with you or a card transaction not originally processed by us. You will not complete a credit voucher for a card issued to you or your employees, except for a valid refund of a transaction originating with you. You may not receive money from a cardholder and subsequently deliver to us a credit voucher to make a deposit to the cardholder's account.

6. Your refund policy may not be valid if a cardholder is returning merchandise because it was defective, misrepresented or otherwise not suitable for the purpose intended.

FACTA: Account number truncation on receipts

Legislation now requires all merchants who accept credit cards for goods/services and generate electronic receipts to print the cardholder receipt with only the last four digits of the cardholder account number, as well as suppress the card expiration date.

You may already be aware of this legislation, commonly referenced as Cardholder Account Truncation. Many of the state laws impose significant merchant penalties for non-compliance — some as high as $10,000 per occurrence and even the possibility of a Class D felony.

Visa and MasterCard have followed suit and are also mandating this requirement. Both card organizations are making this effort in order to:

- Facilitate increased cardholder account number security
- Ensure consistency across Visa and MasterCard brands
- Provide a standardized approach for terminal vendors
- Align with the recent legislation in several states in the United States

Interchange management

Interchange is a fee assessed by the card associations, which are passed through to the card- issuing bank. This fee can account for 80 to 95 percent of the total cost of accepting a card payment, making it the largest cost component of the transaction.

The interchange fees you pay are due in large part to:

- The type of card presented (credit, rewards, debit, corporate, etc.)
- Your industry or Merchant Category Code (MCC)
- How the transactions are processed at the point-of-sale

When transactions are not processed properly for your specific type of business, you can end up paying higher interchange fees or surcharges. Unfortunately, some surcharges are unavoidable. Those are typically associated with the type of card being used, such as a rewards card or commercial card. But by closely managing interchange expenses, your business can keep a larger share of profit for each transaction you process.

Top 10 opportunities to manage interchange expense

1. Follow Card Present and Card-Not-Present Card Acceptance best practices identified earlier in this guide.
2. Avoid key entering transactions at the point-of-sale
   - Consider ZIP code checks at the point-of-sale if key entry is necessary.
3. Settle transactions on a daily basis.
4. Authorize all transactions.
5. Utilize AVS (Address Verification Service) on all Card-Not-Present transactions.
6. Make sure you're set up with the right MCC code.
7. Consider transmitting Sales Tax, Customer Code and Line Item Detail (also known as Level II and Level III data on commercial card transactions).
8. Always use the most up-to-date equipment or point-of-sale software version.
9. Evaluate PIN debit acceptance.
10. Review your reports and transaction data regularly and report any issues.

Chargebacks and retrievals

Chargeback and retrieval procedures

Once you are processing your credit card transactions successfully, there are a few operational procedures that you will want to become familiar with. This section reviews some of the most common situations that may occur when a cardholder requests a copy of a sales draft or disputes a processed credit card transaction. Since Visa and MasterCard mandate time frames and requirements, it is important to review the procedures that you must follow when addressing these types of situations. As always, please view our online self-help tools or contact customer service if you have questions regarding these procedures or any other chargeback related issues.

Here are a few tips to help quickly resolve chargebacks:

- Be sure to log into your online reporting tool to access retrieval and chargeback notices on a daily basis.
- Respond to the chargeback notice as soon as possible within the specified time frame. Make sure your response addresses all of the cardholder's claims using as much detail as possible.
- If a partial credit has been issued, explain why the full credit was not provided.
- If the ink on your draft is light, please take steps to make it darker on a copy machine prior to submission. Sales drafts that are scanned or faxed must be legible.

The following are typical reasons a chargeback occurs:

1. Unauthorized mail order or telephone orders
2. Duplicate processing of sales drafts
3. Non-receipt of merchandise
4. Missing signature or missing imprint of the card
5. Authorization not requested or declined
6. Cardholder dispute, price, terms or delivery
7. Breach of contract terms

Bankcard retrieval request

Merchants are required to maintain original sales drafts for a period of 12 to 24 months, depending on the network. A cardholder is permitted to request a copy of sales or credit drafts within this time frame. This is known as a Retrieval Request.

Upon receipt of a Retrieval Request from a cardholder bank, we will notify you via your online reporting tool.

A legible copy of the sales draft must be faxed or mailed to the address or fax number indicated on the Retrieval Request within the specified time frame. It is important that you retain a copy of the draft for your records.

A Retrieval Request is not a chargeback. In many instances, supplying a legible copy of a sales draft may prevent chargebacks. Failure to supply the requested draft within the specified time could result in a non-reversible chargeback and a debit to your merchant checking account.

Credit card security – skimming is a crime

It's important to keep your customers' credit card information secure. Skimming is one way that criminals illegally obtain credit card information.

What is skimming?

Skimming is any illegal activity that helps criminals obtain credit card account information to produce counterfeit cards.

What is a skimming device?

Skimming devices record and store credit card account information – they are small and portable and may resemble a pager.

How does skimming work?

Usually, someone in the workplace uses a small "skimming" device to steal information electronically from a credit card's magnetic stripe. That information is put onto a counterfeit card and used to make fraudulent purchases.

Be on the alert for skimming activity:

- If you see anyone using a device that is not part of the day-to-day activities
- Anyone offers you money to record account information
- Anyone asks for customer account information over the telephone point-of-sale

Basic equipment troubleshooting

From time to time, you may have questions about how your processing equipment operates.

To resolve equipment problems, first check to be sure:

1. **The equipment has not been unplugged.**
2. **There is power running to the electrical outlet your equipment is using.**
3. **Your phone line is properly connected and is not being used by another device such as a fax machine or computer modem.**
4. **The printer is not out of paper.**
5. **Your terminal's magnetic card reader isn't dirty – check this by folding a clean piece of paper in half and sliding it through the reader three times.**

If your printer isn't working, you may complete a transaction by imprinting the credit card or neatly printing the information on the sales draft and getting the customer's signature. Also, remember to always get an authorization. Make sure to safely store this information in a locked, secure area.

NOTE: If you do not get an imprint and do not get an authorization, you are at a higher risk for chargebacks.

Keep well stocked with these important supplies: printer paper, sales drafts and credit vouchers. This will ensure that you have sufficient supplies during peak periods. Store these materials in a cool place, as overexposure to heat can negatively affect these products.

Contact us

Once you've activated your account, questions will inevitably arise.

From time to time, you will need the occasional tweaks that go hand in hand with business growth. When you do, we will be there to provide strategies, solutions and ongoing support. Our skilled and knowledgeable customer service representatives are ready to assist you.

Give us a call, and let's see how we can help.

Merchant Services Contact Center

Please refer to your Quick Reference Card for the Merchant Services phone number.

People's United Merchant Services

A subsidiary of People's United Bank®

P008 04.16