Payment Processing Handbook

Thank you for selecting Bridgeway Payment Systems for your payment processing needs. We are focused on providing the best service and products in the industry.

This Payment Processing Handbook provides important information that will help you process payments efficiently and securely. Tips are also provided that will help you reduce your overall cost of accepting payments.

Please feel free to give us a call anytime as your success is our top priority: 1-877-995-9198.

Terminal Support: 24 hours / 7 days a week

Customer Service: 7:00 AM to 9:00 PM CST
Let’s get started!

What should I do first?

• Login to view your processing activity, deposits, and merchant statements online at www.portal.elevateqs.com If you have not received an email containing your login credentials please email support@bridgewaypayments.com.

• Place the Merchant Services Quick Reference Guide and applicable equipment quick reference guides close to your point-of-sale for easy access to helpful phone numbers and processing instructions.

• Validate your PCI Compliance by visiting https://bridgeway.pcitoolkit.com/version3 Please review the enclosed PCI Brochure for more information.

• Review the Payment Processing Services for other matters that may benefit your business.

• Review and communicate the important Best Practices contained throughout the rest of this guide to all associates that will be processing customer payments in your business. These Best Practices will help you reduce fraud and manage your processing expense.
Payment Processing Services

Bridgeway Payment Systems has many products and services that will help you strengthen your customer relationships.

Card Acceptance
Whether you prefer a traditional terminal, a web based terminal, or a tablet based point-of-sale, we have a solution that will process your customers’ debit and credit card payments.

Check Services
It’s more important than ever to accept any type of payment your customers prefer. We can help take the worry out of processing paper or electronic checks.

Gift Card Solutions
Increase sales, revenue, and customer loyalty by providing gift cards.

E-Commerce
Let us help you enhance your online presence by providing simple and secure payment methods for your website.

Mobile
Mobile payment sales are increasing at a rapid rate. Let us help you take payments on the go as well as provide your customers a way to pay with their mobile device.
Best Practices

Reducing the Risk of Fraud on Card Present Transactions

- **Validate the physical card**
  - Verify the expiration dates are current
  - Verify the signature is present on the back of the card
  - If a photo is present, compare the photo to the customer
  - Confirm there are no signs of tampering with the card – review the signature panel, numbers, hologram, and magnetic strip
  - Ensure the number embossed on the front of the card matches the truncated number on the receipt

- **Always swipe the card or dip the chip**
  - Take extra caution if the customer requests you to manually key a transaction
  - Avoid key entry whenever possible. If you must enter the numbers manually, be sure to:
    - get a clear imprint of the card
    - enter the address information when prompted and ensure a match response is received
    - enter the CVV2/CVC2/CID code and ensure a match response
  - Credit and debit cards that are embedded with a security microchip provide further protection to assist in decreasing the risk of fraudulent transactions and chargeback disputes. Look at the card and if there is a chip, always insert the card into the chip reader at the first instance.
Best Practices

Reducing the Risk of Fraud on Card Present Transactions, Continued:

• If the terminal displays ‘Insert Chip’ when the card is swiped through the terminal and the card in question does not have a chip on it, do not proceed with the transaction
• If the terminal displays ‘Insert Chip’ and the chip when inserted cannot be read by the terminal, do not proceed with the transaction

• Settle your transactions daily.
• Do not accept declined transactions or split a declined transaction into smaller amounts.
• If you suspect fraud, please contact the Voice Authorization Center (1-800-990-2265) and let them know you have a “Code 10” authorization request.

Reducing the Risk of Fraud on Card-Not-Present Transactions

• Ensure the card has not expired.
• Obtain as much information as possible: the credit card number, full name, address, expiration date, CVV2/CVC2 and contact telephone number. Enter the details correctly in the terminal and do not store the CVV code.
• If taking payments via a website, contact your gateway provider to ensure you have all appropriate fraud options set up correctly.
• Keep all copies of correspondence including invoices, emails, quotations, faxes, proof of delivery, etc.
Best Practices

Reducing the Risk of Fraud on Card-Not-Present Transactions, Continued:

• Remember, an authorization only confirms that funds are available and that the card has not been reported lost or stolen. It’s important that you are diligent in ensuring you have authorization from the owner of the card for the full amount of the transaction.
• Ensure timely shipment of goods. Your transaction date should be the same as your shipment date and not be greater than 7 days from the authorization date.
• Settle daily.

Reducing the Risk of Fraud for online purchases

• Ensure you have a clear refund/return policy on your site.
• Remember, it is your responsibility to utilize risk management tools provided by your gateway.
Returns and Exchanges

Bridgeway Payment Systems recommends you prominently display your refund policy in-store, on your website, and on your sales receipts to limit returns and support your chargeback presentment. Keep in mind, network rules may require you to refund a transaction even if your policy is clearly identified as No Returns or Store Credit/Exchange Only.

- Ask for the customer’s receipt.
- Refund to the card used for the original transaction.
- Provide the customer with a copy of the refund receipt including refund date, amount, cardholder account number (truncated), and a brief description of the refund.
- Maintain the same return policy for cash customers as you do for those making purchases with a card.
- Proper disclosure must be made at the time of the original card transaction if you limit returned merchandise and cancellation of services. If merchandise is defective, misrepresented, or not suitable for intended use, your refund policy may not be valid.
- For internet orders, there must be an acknowledgment button that is selected prior to the order being submitted.
- The amount of the refund must not exceed the amount of the original transaction, except for any amount you agree to refund for postage.
- Refund adjustments should not be made in cash, except if required by law.
- It’s recommended that a password be required to enter a refund in the point-of-sale device to reduce the potential for unauthorized refunds/fraud. Change this password often and do not use generic passwords such as 9999.
A chargeback is a reversal of a credit card transaction and usually occurs when a customer raises a dispute with their financial institution (also known as the issuer) in relation to a purchase made on their card. A chargeback may cause the original amount of the sale and a chargeback fee to be deducted from the merchant’s account. A retrievals is a request of information by the cardholder. Retrievals may or may not turn into chargebacks.

The card associations (Visa/MasterCard/Discover/American Express) mandate timeframes and requirements for responding to chargebacks and retrievals. It is important that you follow proper protocol and respond quickly to any request.

**Common reasons for chargebacks:**

- Transaction not recognized by the cardholder
- Transaction not authorized by the cardholder
- Duplicated transaction
- Cancelled recurring transaction
- Goods/services not received or not as described or faulty
- Fraud

**In order to get quick resolution, a few best practices are recommended:**

- Be sure to log into the online merchant reporting tool to view your retrieval and chargeback notices on a daily basis.
- Respond to chargeback and retrieval notices as soon as possible and within the timeframe specified. Make sure to address all of the cardholder’s claims using as much detail as possible.
- If a partial credit was issued, explain why full credit was not provided.
- Ensure all documentation is clear and legible.
Chargebacks and Retrievals

Voice Authorizations

*Voice authorizations are recommended for the following reasons:*

- You are unable to obtain an authorization from your point-of-sale device
- You receive the message “Call Center” when trying to process a transaction

*Please follow the procedure below when calling for a voice authorization:*

- Dial the Voice Authorization number located on your terminal or Merchant Service Quick Reference Card.
- Enter the following information when prompted:
  - Merchant ID
  - Cardholder account number
  - Card expiration date
  - Dollar amount of transaction
- If approved, record the authorization number on the sales draft.
- Obtain a manual imprint of the card and obtain a signature from the cardholder.
- Please note, you will not be paid for this transaction until the authorization number is entered into your point-of-sale device and settled. Once your device is operational or you receive a replacement device, manually enter the transaction using the off-line function (refer to the quick reference guide for the point-of-sale device).
Managing Processing Expense

Higher fees and surcharges can occur when transactions are not processed properly. Fees are typically determined by:

- The type of card presented (credit, debit, rewards, business, etc.)
- The merchant MCC (Merchant Category Code) or industry
- How the transaction is processed

While you can’t control the type of card presented or your industry, there are many opportunities to manage your processing expense related to how the transaction is processed:

- Follow the Card Present and Card-Not-Present best practices outlined earlier in this document.
- Avoid key entry if at all possible. If you must manually enter the card number, ensure the zip code is entered.
- Settle your transactions on a daily basis.
- Ensure you are set up with the proper MCC code.
- When processing a commercial card, enter the sales tax and customer code (also known as Level II data).
- When processing a large commercial card transaction, also consider entering the line item detail (also known as Level III data).
- If you process a high volume of debit transactions, evaluate PIN debit acceptance.
- Review your merchant statement and transaction activity regularly and promptly report any issues.
- Ensure all staff are properly trained on proper transaction processing procedures.
Contact Us

Should you have questions please reach out to us so we can help. You can find important numbers on your Merchant Services Quick Reference Card.

**Customer Service:** 1-877-995-9198

**Terminal Support:** 24 hours / 7 days a week

**Customer Service:** 7:00 AM to 9:00 PM CST