WELLS FARGO

Wells Fargo Merchant Services

Guide to processing online payments

Together we'll go far

Welcome!

Thank you for selecting Wells Fargo Merchant Services!

By choosing Wells Fargo, a leader in merchant payment processing, you have made one of the most important decisions you will make in your business.

This *Guide to Processing Online Payments* brings together all the information you need to get started right away. Please take a look inside before you begin processing transactions to optimize the payment processing features and benefits available to you. Keep this guide in a convenient location for quick and easy reference. We also invite you to visit our website for additional information at www.wellsfargo.com/biz/merchant.

At Wells Fargo, we strive to build long-term and prosperous relationships with our merchants by providing great service, valuable products, and reliable support. Do not hesitate to let us know how we can support you and your financial success.

Thank you for your business and *welcome* to Wells Fargo.

Best regards,

Mark J. Baumli

Mark J. Baumli
Senior Vice President
Wells Fargo Merchant Services

Table of Contents

Getting Started 4

Authorization 5

Managing Fraud & Losses 7

Reporting 11

Merchant Statement 12

Interchange 13

Risk Monitoring 15

Dispute Process 16

Association & Industry Compliance 21

Glossary 23

Contacts & Resources 30

Getting Started

Thank you for choosing Wells Fargo Merchant Services for your online payment processing needs. There are just a few simple steps to get you started with your Internet merchant account.

Step 1 To get started, you will receive two separate emails with your login and setup instructions within one to two business days. The email(s) will originate from one of the following **depending on the payment gateway you chose**.

- Authorize.Net gateway users will receive an email containing an activation link that enables merchants to create a login and password from Support@Authorize.net
- CyberSource gateway users will receive two separate emails with user name and password instructions from Registration@cybersource.com
- PayPal gateway users will receive an email with login and password from wells.fargo.products@wellsfargomerchantservicellc.com
- If you already have a payment gateway, Wells Fargo will send an email from wells.fargo.products@wellsfargomerchantservicellc.com containing a merchant login and password, or merchant identification and terminal identification

Step 2 Review the information in this document to ensure that you and your website are ready to begin processing.

Step 3 Follow the instructions from your payment gateway for converting from test mode to live transaction processing.

Step 4 Start processing transactions!

Customer Service is available to help you

800-451-5817

24 Hours a Day, 7 Days a Week

Authorization

Authorization is the process by which card issuers approve, decline, or request more information on a transaction. All card sales require an authorization from the organization that issued the cardholder's card (card issuer) to verify that the card is valid and the account has sufficient funds to cover the amount of the transaction. The card issuer provides an authorization and approval code to Wells Fargo.

It is not a guarantee that you will receive payment for the authorized/approved transaction, and it does not mean that the person using the card is the rightful cardholder.

Authorization Codes & Messages

Code / Message	Response Definition
00 - Approved	A 2 to 6 digit code follows approval.
02 - Declined	The merchant should never accept the card once declined but request another form of payment.
04 - Referral	This response indicates that the card issuer requests direct contact with the merchant in order to authorize the sale. The merchant must contact the Authorization Center for Visa®/MasterCard®/American Express®/Discover®.
Hold Card / Call Center	The card issuer requests that the card be removed from circulation. The merchant should never accept the credit card for payment when this response is received.
Call Center	This response indicates that the card issuer requests direct contact with the merchant in order to authorize the sale. The merchant must contact the Authorization Center for Visa/MasterCard/American Express/Discover.
10 – Invalid Account Number	The cardholder account number was entered incorrectly.
Invalid Merchant number	The network does not recognize the merchant account number. Verify the merchant number was entered correctly and make sure the account is still in an active/open status.
Waiting for Line	This response indicates that the phone lines are currently busy.
44 – Unable to Connect	This indicates there is a problem with the equipment or network. The merchant should contact the Terminal Help Desk at 800-622-0842.

Authentication

Authentication and verification methods are essential in maintaining the efficiency and integrity of your online business. The following are the key data elements during authorization designed to minimize fraud:

- Address Verification Service (AVS) reduces exposure to fraud by ensuring that the address attached to the payment card matches the billing address the customer enters on the website
- Credit Card Security Codes (CVV2, CID, CVC2) are important Internet security features providing a security code on the card that helps validate that the customer placing the online order is the actual cardholder

To maximize authorizations, take advantage of fraud protection services offered by Wells Fargo such as AVS and credit card security codes. Also consider using the additional fraud protection services provided by your payment gateway.

Please continue to the next section "Managing Fraud & Losses" for more information on fraud protection strategies and best practices.

Managing Fraud & Losses

In the card industry, Internet generated transactions are classified as "card not present" transactions because the card is not physically processed by a card swipe terminal. According to Visa, MasterCard, American Express and Discover rules, merchants that accept card payments and do not obtain a signature at the time of sale are responsible and liable for transactions in the event of a cardholder dispute. Cardholder disputes can result in chargebacks, meaning that the transaction amount is debited back to your account.

To help mitigate fraud and manage chargebacks, make every effort to know your customer. The amount of exposure you have to Internet fraud depends on your business policies, operational practices, fraud prevention and detection tools, other risk controls and the type of merchandise you sell. All employees should have a thorough understanding of the fraud risk associated with any Internet transaction. It is your responsibility to check and validate orders before shipping in order to minimize fraud and/or electronic shoplifting. Address verification and credit card security codes electronically verify that the information the customer input on the order screen matches their card issuer's records.

Association Compliance

In the payment card industry, the card associations exist for the purpose of facilitating payment transactions. To most effectively manage fraud and risk in today's business environment, the card associations have implemented comprehensive security requirements defining how cardholder data must be stored, managed, and processed to keep it secure.

Merchants conducting business over the Internet are required to transmit an eCommerce Indication (ECI) flag on purchases completed on the Internet. Most Internet payment gateways have been certified to pass this flag. Check with your payment gateway provider to ensure that your payment gateway has been certified.

What Are Some Signs That A Transaction Could Be Fraudulent?

- Larger than normal orders
- Orders that include several of the same items, particularly if the item has a high resale value
- Rush or overnight orders
- Orders from Internet addresses making use of free email services
- Ship-to address is an international address; Nigeria, Indonesia, Russia, and Central and Eastern Europe historically have particularly high fraud rates
- Multiple purchases on the same day
- Orders shipped to a single address but made on multiple cards
- Multiple transactions on one card or similar cards with a single billing address but multiple shipping addresses
- Billing address provided by customer to the merchant does not match with AVS

How Can I Reduce Fraud & Chargebacks?

Here are some tips for you to consider when setting up your website or order processing system that may help you reduce your fraud and chargeback exposure:

On Your Website

- Provide your Customer Service telephone number on your website and in all email correspondence with the cardholder. This enables customers to contact you directly prior to calling the card issuer to initiate a dispute.
- Publish your return policy on your website and include it in the email confirmation of the order. Require that the cardholder "Click to Accept" your terms and conditions
- Ensure the business name you provided that is to appear on the cardholder's statement accurately reflects the name you use to do business. This will reinforce your name recognition starting with the website where they ordered goods/services, to the card transaction. Be consistent in including this name on all correspondence and packaging.

Order Processing

- Ask the customer for both a card type and an account number and make sure they match, for example, Discover account numbers begin with a "6", MasterCard account numbers begin with a "5", American Express account numbers begin with a "3", and Visa account numbers begin with a "4".
- Make it your policy to request the name of the card issuer and the customer service phone number from the back of the credit card for any sale over a pre-set amount. If the customer doesn't know the issuer's name, the card number could be stolen.
- Always ask for the cardholder's contact information including billing address, day and evening telephone numbers, and email address. Orders with a "ship to" address that is different from the billing address are riskier. Program your system to compare the "ship to" and "bill to" addresses to each other and to any prior information you have about the cardholder.
- Develop and maintain a "negative file" of previous fraudulent names, addresses, zip codes, card numbers, and fraudulent companies. Compile a zip code listing to draw attention to areas in which you've experienced high fraud. Ensure a firewall is installed to protect stored information.
- For Visa cards, ask for the non-embossed number, which appears above the first 4 digits. It should match the first 4 digits of the card number.
- Request the credit card security code, also known as CID, CVV2, and CVC2. This is the value printed on the card to help validate:
  - ⇒ the cardholder has possession of the card
  - ⇒ the card account is legitimate

    Note: CID value can also be validated on non-U.S. cards

Order Processing (continued)

- Use AVS to verify cardholder information. At a minimum, the zip code should match before the transaction is approved. Visa and Discover require AVS in order to qualify for the best interchange rates.
- Depending on the response, you will need to decide if you want to process the transaction or take additional steps to verify the customer information. Card issuers will not decline transactions based on the AVS information. It is important that you retain the AVS response and a record of your follow up actions, if any, for possible future use during the chargeback process. The AVS messages are:
  - ⇒ Y – Exact match on street address and 5- or 9- digit zip code
  - ⇒ A – Address matches, zip code does not
  - ⇒ Z – Zip code matches, address does not
  - ⇒ N – No match
  - ⇒ U – Address information is unavailable or card issuer does not support AVS
  - ⇒ R – Card issuer authorization system is unavailable; retry later
  - ⇒ E – Error in address data; unable to complete check
  - ⇒ G – Non-U.S. card issuer not participating in AVS; Visa only
  - ⇒ S – Address information is unavailable or card issuer does not support AVS; MasterCard only
- In the U.S., Visa, MasterCard, and Discover card issuers should provide an AVS response. If you receive a "U" response on a Visa transaction only, fraud chargeback liability rests with the card issuer, not with the merchant. If you receive an unauthorized purchaser chargeback on a Visa transaction where you received a "U" response, you can successfully defend chargebacks due to fraud by providing the AVS message with your media or chargeback requests.
- Message "G" may be passed to you in a variety of ways depending on your choice of gateway. Examples are "Address not verified – international" or "unrecognized." Please check your payment gateway manual for further information.
- Process real-time authorizations in order to provide immediate response to cardholder.
- Only process sales transaction when the goods or services have been sent to the customer. For items that may experience longer delivery times such as furniture, the customer cannot be charged until the item has been shipped.
- Send a confirmation by email to the customer so they may immediately verify the transaction.
- Send a delivery confirmation email to the cardholder once the goods have been shipped with the reminder that their card will now be charged, providing your business name and the dollar amount of the transaction.
- Use an online phone directory to verify a customer's phone number and address as belonging to that customer.
- For best practices, use Verified by Visa and MasterCard SecureCode® programs because they significantly reduce the number of chargebacks.

After The Transaction Has Been Processed

- Respond immediately to a customer's request for information about a transaction. It's to your advantage to satisfy customer concerns and resolve disputes so that chargebacks can be avoided.
- Monitor your authorization declines to identify trends and add that information to your negative file.
- Obtain a new authorization if the original expires before shipment, i.e., if more than 7 days have elapsed between the authorization date and the shipment. For example, if an item is on back order, get another authorization prior to shipping in order to verify cardholder is still approved for the transaction.
- Ensure control of any cardholder data that you maintain internally to prevent that information from being misused.

What If I Think A Transaction Is Suspicious?

- Call the Authorization Center at 800-626-4480 and ask for the Code 10 Operator, which indicates that you suspect a fraudulent transaction.
- Call or email the customer to request additional information. Use a phone directory to validate the day and evening phone numbers provided by the customer.
- Send a note to the customer's billing address to confirm the order, rather than the "ship to" address.

Reporting

ClientLine®

Wells Fargo Merchant Services provides reports through ClientLine®, an Internet-based service that provides merchants with fast access to transaction information. ClientLine allows you to check the activity on your account. You are able to view deposits, credits, and checking account transfers, all with a simple mouse click. By having detailed transaction activity available on a daily basis, you can easily reconcile your account as your business grows.

ClientLine is automatically available to you – at no additional cost – when you open a merchant account with Wells Fargo Merchant Services. We automatically send you an email providing a user ID for quick and easy enrollment. If you are not enrolled at the time of setup, you can do so easily by visiting www.myclientline.net and answering a few questions to initiate your enrollment.

Benefits

- Gain anytime access – manage your accounts at a time that is convenient for you
- Minimize cost – eliminate the storage and cost of paper statements with easy access to online merchant statements
- Perform historical / trend analysis – for more robust account information
- Streamline reconciliation – download information for easy analysis
- Security – manage user access with passwords

electronic Integrated Disputes System (eIDS)

eIDS is the optional service designed to help you manage retrieval requests and chargeback disputes more effectively. It is part of a comprehensive solution that enables research and the online exchange of information between you and Wells Fargo for dispute management. You can enroll in eIDS from the Portal Main Menu on the ClientLine application or by calling Customer Service at 800-662-0842.

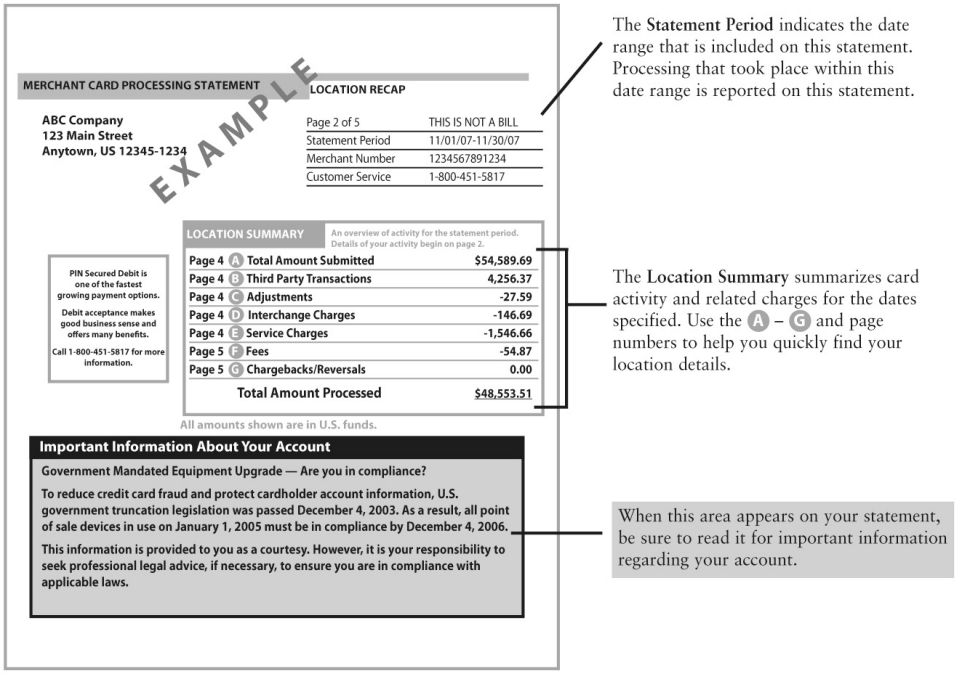
Benefits

- Save time – streamline the chargeback and retrieval management process
- Be more independent and efficient – manage cases online for faster and easier dispute resolution
- Enhance your business organization – control workflow in the back office in real-time, and increase your audit functionality
- Decrease losses – respond quickly to retrieval requests and decrease the possibility of a chargeback resulting from a non-response
- Reduce costs – save on mail and fax expenses and gain efficiencies through better time management and financial controls

Merchant Statement

Wells Fargo Merchant Services provides a monthly statement of your transaction activity in a format designed to facilitate account reconciliation.

How To Read Your Statement



The **Statement Period** indicates the date range that is included on this statement. Processing that took place within this date range is reported on this statement.

The **Location Summary** summarizes card activity and related charges for the dates specified. Use the A – G and page numbers to help you quickly find your location details.

When this area appears on your statement, be sure to read it for important information regarding your account.

Top 10 Card Processing Terms in Plain Language

Location Recap — This is your Merchant Card Processing Statement, which includes an activity summary and supporting detail for the dates specified.

Merchant Number — A unique account number assigned to each merchant and merchant location. Find it at the top of your statement.

Total Amount Submitted — The total dollar amount of card transactions submitted and processed during the Statement Period.

Third Party Transactions — These transactions are passed directly to a third party service provider for processing and/or funding.

Adjustments — Amounts credited to or deducted from your account to resolve processing or billing discrepancies.

Interchange Charges — These variable amounts are established by the Card Associations for processing transactions. Factors that influence interchange charges include card type, information contained in the transaction, and how/when the transaction was processed.

Service Charges — Also known as Discount Rate; amounts charged to authorize, process and settle card transactions.

Fees — A range of transaction-based and/or fixed amounts for specific card processing services.

Chargebacks/Reversals — Transactions that are challenged or disputed by a cardholder or card-issuing bank. A Chargeback is the amount that is disputed by the cardholder or card-issuing bank. A Reversal is the amount that was previously resolved against the merchant but now is resolved in favor of the merchant.

Total Amount Processed — The total amount processed is the dollar amount that Wells Fargo Merchant Services deposits into your bank account for the statement period, net of third party transactions, adjustments, charges, fees, and chargebacks/reversals. Please note however that the fees shown on this statement in item F may not be deducted from your account until several business days after receipt of this statement.

Interchange

What Is Interchange?

Interchange is the standardized electronic exchange of payment card transaction data between merchant Acquirers and card issuers in accordance with card association rules. Different factors, including the way the transaction was processed and the card type used can determine the level of interchange.

What Is An Interchange Fee?

An interchange fee is captured from merchants by card issuers and the card associations for each card payment transaction. The fee compensates the card issuer for advancing payment to the merchant until settlement from the cardholder. It is a necessary expense when you offer customers the convenience of payment by card. These fees also pay for the electronic payment system that enables merchants to offer more payment options and make more sales to a wider customer base with the speed and security demanded by the marketplace.

What Is A Downgrade?

Card associations quote the lowest rate for a transaction, which is based on the assumption that a number of requirements will be met. A downgrade occurs when the sales transaction does not meet the card association's criteria, and as a result the transaction is processed at a higher interchange rate. Rates can vary according to the card type, industry type of the merchant, and the way a transaction was processed. If one or more of the card association's requirements are not met, the transaction will be categorized at a different and more expensive interchange level.

What Can I Do To Qualify For Better Interchange Rates?

The interchange rates you pay can be affected by your payment processing account configuration and the steps you take to complete each transaction. It is important to understand the factors affecting interchange rates to help you manage them and minimize downgrades. Below are things you can do to qualify for better interchange rates:

- Use correct Merchant Category Code (MCC) – Make sure your business is categorized correctly or you may not be receiving the best interchange rate for which you could qualify.
- Use Address Verification Service (AVS) – Merchants need to submit the billing address and zip code for card not present transactions to qualify for the lower interchange rate; AVS uses the billing information associated with a card to verify the cardholder's address.
- Send settlements on time – Merchants have to settle transactions within a specific amount of time after authorization to avoid downgrades; Wells Fargo Merchant Services recommends daily settlement of all transactions.

What Resources Does Wells Fargo Provide On Interchange?

"The Merchant's Guide to Achieving Better Interchange Rates" describes many of the reasons you may experience higher interchange rates and suggests steps that you can take to avoid them. Wells Fargo will help you take advantage of those opportunities to reduce downgrades and enjoy better rates. The Merchant's Guide to Achieving Better Interchange Rates is available online at: www.wellsfargo.com/biz.managecosts

The "Visa, MasterCard, and Discover Interchange Matrix" is designed to help you process at the best rate available to you. This document provides a summary of the primary qualification criteria established for each interchange level. The Visa, MasterCard, and Discover Interchange Matrix is available online at: www.wellsfargo.com/downloads/pdf/biz/merchant/qualification.pdf.[1]

What is a Discount Rate?

American Express does not charge interchange and instead charges you a discount rate and depending upon your industry, sometimes an additional transaction fee. Therefore, there is not an interchange matrix for American Express.

American Express Operating Regulations state that Discount means the amount that we charge you for accepting the Card, which amount is: (i) a percentage (Discount Rate) of the face amount of the Charge that you submit; or a flat Transaction fee, or a combination of both; and/or (ii) a Monthly Flat Fee (if you meet our requirements).

The "Debit Network Fee Schedule" provides applicable debit network, switch, service, and administrative fees passed through on all PIN Debit transactions. The Debit Network Fee Schedule is available online at: www.wellsfargo.com/downloads/pdf/biz/merchant/debit_fee_schedule.pdf

Additional information is available online at:

- www.wellsfargo.com/biz/merchant
- www.visa.com/merchant
- www.mastercardmerchant.com
- www.discovernetwork.com

[1] For more specific information about interchange program qualifications and fees, please refer to your Visa, MasterCard, and Discover Interchange Qualification Matrix and the corresponding interchange fee schedules for your account.

Risk Monitoring

Wells Fargo Merchant Services periodically evaluates merchant accounts to ensure they are in compliance with their Wells Fargo Merchant Agreement. During our periodic reviews you may be contacted for updated financial information or to provide additional information that supports processing level changes such as increased sales volume and/or higher average dollar value per transaction.

These risk components may change your reserves, funding limits, or delay funding, as explained in your Merchant Agreement. We will notify you within three (3) business days of changes made or if any further action will be required. If you anticipate changes in your processing activity, please call Customer Service at 800-451-5817 to proactively discuss changes to your original Merchant Agreement.

When Should You Contact Customer Service To Update Your Merchant Account Information?

- Change to your estimated card processing volumes
- Change to your estimated average dollar value per transaction
- Changes to your products and/or services sold
- Change in the number of days between delivery of goods or services and when you charge a customer's account
- Change, perhaps unforeseen, to your overall operations that may result in additional chargeback, refund, or credit activity
- Change to your merchant account profile such as settlement account, address, DBA name, legal name, entity type or legal structure, and primary contact information

Dispute Process

When your customer disputes the validity of a transaction on their card statement, a media retrieval request or chargeback occurs. The chargeback amount and a chargeback fee will be applied, so it is in your best interest to gather as much information about the transaction as possible and respond directly to the customer and quickly in order to prevent loss of funds.

What Is A Media Retrieval Request?

The customer will contact their card issuer about the transaction in dispute. The card issuer will then send a request for information to Wells Fargo regarding the sale. This request is called a media retrieval request. After Wells Fargo Merchant Services faxes or mails you a copy of the media retrieval request, you have fourteen (14) calendar days from the date on the request to fax a clear and legible copy of the sales record. If you do not respond, the media retrieval request can result in a chargeback to your account that is not reversible.

If you deposit electronically, you are responsible for retaining and fulfilling requests for copies of transactions for a minimum of 18 months.

What Is A Chargeback?

A chargeback is a transaction that has been disputed by the cardholder or the card issuer. The card issuer has debited Wells Fargo for the transaction and Wells Fargo debits the merchant account as stipulated in the Merchant Agreement and card association rules. Common reasons for chargebacks:

- The card was fraudulent
- Cardholder disputes the quality or receipt of merchandise
- The amount charged to the card was incorrect
- Processing errors were made during the transaction
- Proper authorization was not obtained
- Merchant did not fulfill a retrieval request

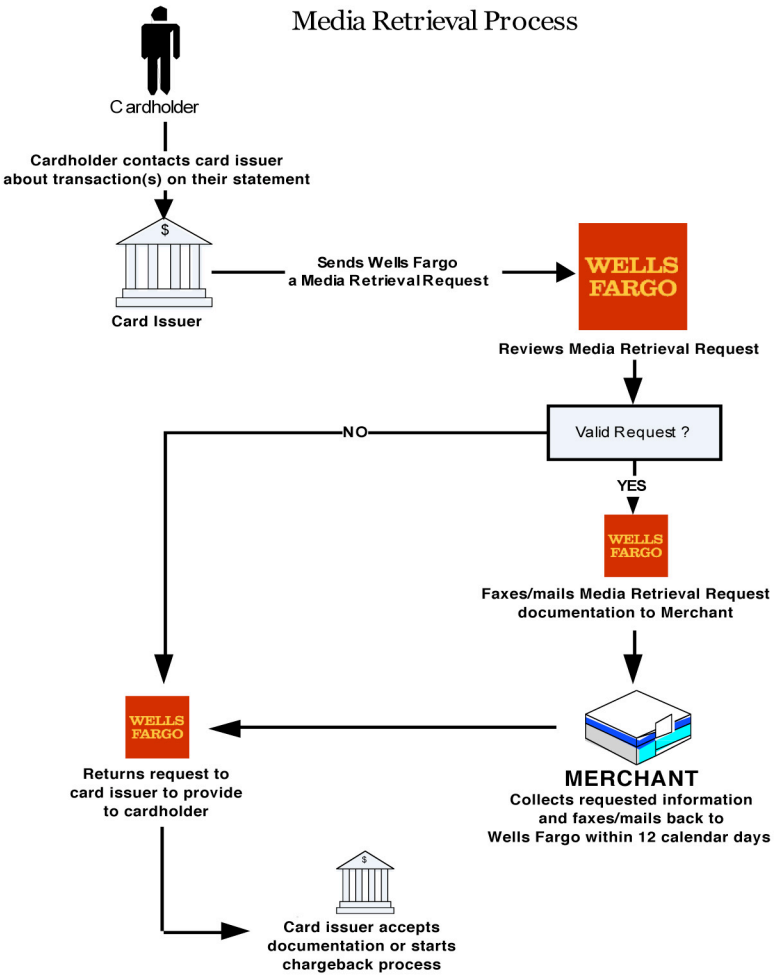
How Does The Dispute Process Work?

After the cardholder has disputed a transaction, the card issuer typically has two options depending on what the cardholder has indicated as the reason for the dispute:

1. Request a copy of the sales draft, also known as a media retrieval request.
2. Request that the transaction be charged back to the merchant, also known as a chargeback request.

Wells Fargo Merchant Services will fax or mail you copies of these requests so that you can provide a response. If you are enrolled in eIDS, the Internet-based dispute management tool, you can also obtain copies online. (See last portion of this “Dispute Process” section, as well as the “Reporting” section for more information about eIDS.)

Card issuers have the right to charge back transactions for up to 120 days. (**Note**: The 120 days may start later than the date of the actual purchase.) If the card issuer has submitted a chargeback request, then your account is immediately debited for the amount of the dispute and will not be reversed until Wells Fargo Merchant Services has submitted your defense for review by the cardholder and/or card issuer.



What Do I Do?

When Wells Fargo Merchant Services faxes or mails you a chargeback request, you have fourteen (14) calendar days from the date on the request to return, via fax, a clear and legible response. It is important to gather as much information about the transaction as you can and provide a comprehensive response to the request to help resolve the issue quickly. The chargeback and a chargeback fee are applied so it is in your best interest to resolve the customer dispute before the card issuer initiates a chargeback.

If you have already issued a credit, provide copies of the credit record, including the date and amount that the account was credited. Please respond to chargeback notices, even if you have issued a credit.

When Should I Respond?

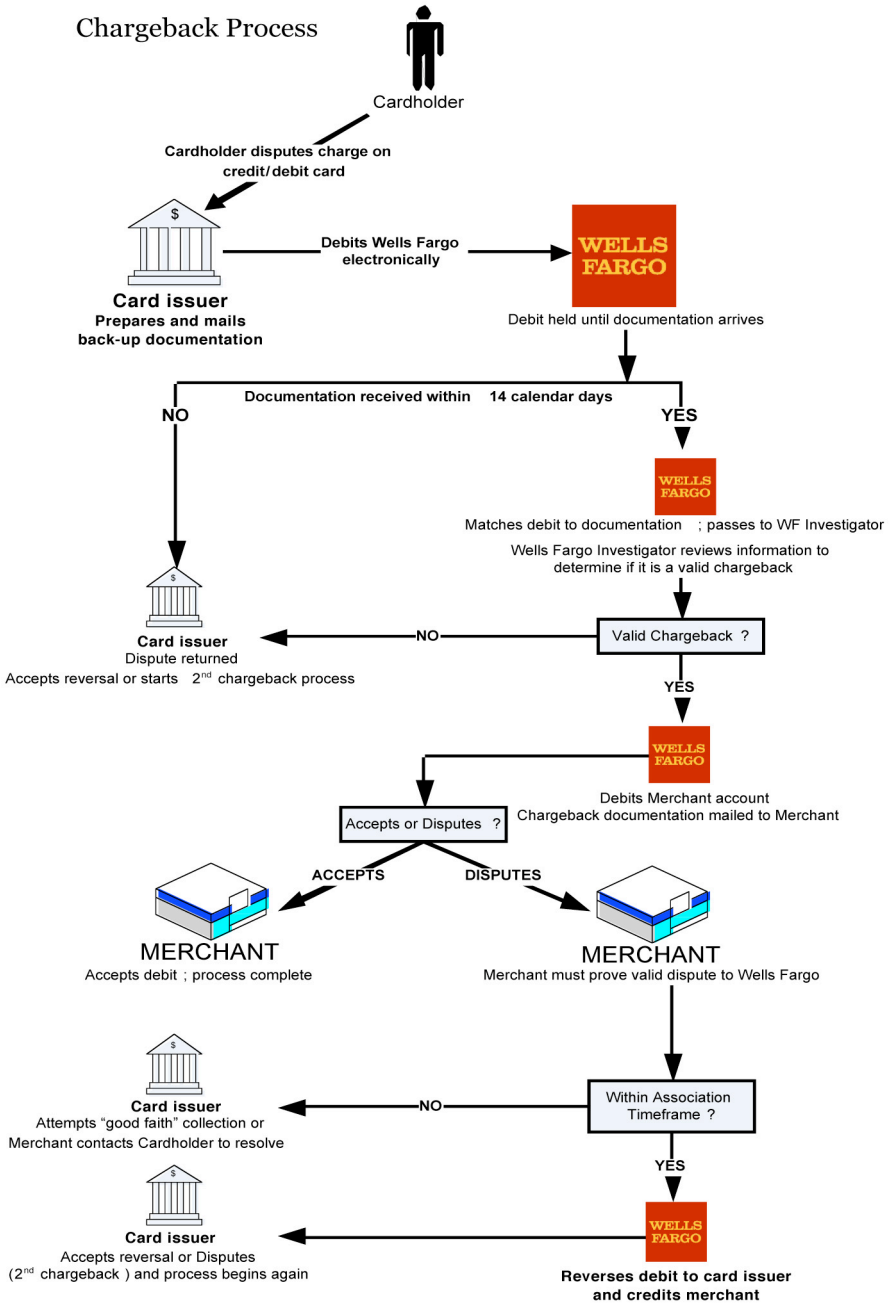
Immediately. It is best to research and respond as soon as possible since you no longer have the goods and your account has been debited for the sales amount or the disputed amount. Please be sure to respond quickly with a comprehensive defense in order to attempt to get the debit reversed. If you do not respond to a chargeback notice or if you respond after the chargeback notice period has ended, you will not be able to reverse the chargeback.

How Do I Dispute A Chargeback?

To dispute a chargeback, provide a clear copy of the sales order within fourteen (14) calendar days showing:

- Date of original sale/credit
- Cardholder's account number and name
- Description of goods and/or services
- Total amount of the sale
- Total amount of chargeback
- Date of authorization and approval code
- Dated cover letter detailing the reasons for requesting a review of the chargeback, including information about the steps taken to prevent the chargeback, and documentation to support your dispute. It is very important to clearly explain why the customer's complaint is not valid.
- Any other supporting documentation such as AVS code, delivery confirmation, bill to/ship to address, any correspondence with the cardholder, and credit card security code (CVV, CID, CVC2) response

If your dispute and documentation support a reversal of the chargeback to the card issuer and is received within the reversal timeframes, Wells Fargo Merchant Services will reverse the item back to the card issuer and your account will be credited. It is important to note that the reversal is contingent upon the acceptance by the card issuer and/or the cardholder. The item may be presented a second time and your account will be debited accordingly. A reversal is not a guarantee that the chargeback has been resolved in your favor.


Chargeback Process
Cardholder
Cardholder disputes charge on credit/debit card
Card issuer
Prepares and mails back-up documentation
Debits Wells Fargo electronically
WELLS FARGO
Debit held until documentation arrives
Documentation received within 14 calendar days
NO
YES
WELLS FARGO
Matches debit to documentation ; passes to WF Investigator
Wells Fargo Investigator reviews information to determine if it is a valid chargeback
Valid Chargeback ?
NO
Card issuer
Dispute returned
Accepts reversal or starts 2nd chargeback process
YES
WELLS FARGO
Debits Merchant account
Chargeback documentation mailed to Merchant
Accepts or Disputes ?
ACCEPTS
DISPUTES
MERCHANT
Accepts debit ; process complete
MERCHANT
Merchant must prove valid dispute to Wells Fargo
Within Association Timeframe ?
NO
Card issuer
Attempts "good faith" collection or
Merchant contacts Cardholder to resolve
YES
WELLS FARGO
Card issuer
Accepts reversal or Disputes
(2nd chargeback) and process begins again
Reverses debit to card issuer and credits merchant

What Tools Are Available To Manage Chargebacks?

Resolve Chargeback Tool

Wells Fargo Merchant Services has developed an online tool to provide merchants with suggestions for effectively responding to a chargeback. The Resolve Chargeback Tool is available online at: www.wellsfargo.com/biz/merchant/service/manage/chargeback

Once you have selected the criteria prompted by the Resolve Chargeback Tool, the final result is a screen with instructions providing the best methods to handle/resolve the chargeback based on the information provided.

electronic Integrated Disputes System℠ (eIDS℠)

eIDS is the optional online tool accessible from the ClientLine online reporting application with simple enrollment steps at www.myclientline.net. Once you are enrolled for the eIDS service, chargebacks are posted to your account enabling you to investigate and resolve chargebacks in the most efficient manner possible. eIDS also provides information required on media retrieval requests for outstanding, reversed, and expired disputed transactions. (See also "Reporting" section.)

Association & Industry Compliance

In the payment card industry, the card associations exist for the purpose of facilitating payment transactions. To most effectively manage fraud and risk in today's business environment, the card associations have implemented comprehensive security requirements defining how cardholder data must be stored, managed, and processed to keep it secure. All merchants are required to be compliant with PCI Data Security Standards even if they are not required to validate that compliance.

Payment Card Industry (PCI) Data Security Standards

The Payment Card Industry (PCI) Data Security Standards apply to all credit card and debit card transactions for Visa, MasterCard, Discover, American Express, and JCB transactions. These security standards are internationally recognized best practices for cardholder data security and are intended to ensure that cardholder data is appropriately protected at all points in the course of a transaction.

Wells Fargo requires all of its merchants and their service providers to comply with the PCI Data Security Standards, as well as the Visa, MasterCard, American Express and Discover information security programs. PCI Data Security Standards protect cardholders while minimizing the risk to your business.

Although Visa, MasterCard, American Express and Discover programs are based on the PCI Data Security Standards, each card association maintains its own compliance program and reserves the right to take independent action for non-compliance with these standards.

Visa Cardholder Information Security Program (CISP)

Visa's CISP program defines which entities are required to validate their compliance with PCI Data Security Standards and the method of that validation. Penalties may be assessed for entities that either fail to meet their validation requirements or are otherwise identified as non-compliant with the PCI Data Security Standards.

MasterCard Site Data Protection (SDP)

MasterCard's SDP program defines which entities are required to validate their compliance with PCI Data Security Standards and the method of that validation. Penalties may be assessed for entities that fail to meet their validation requirements or are otherwise identified as non-compliant with the PCI Data Security Standards.

Discover Information Security and Compliance (DISC)

Discover's DISC program is designed to support the mandatory requirements set forth by PCI Data Security Standards by safeguarding cardholder information and limiting data compromises. Quality management security services provided through DISC help merchants prevent information system security events and attacks leading to identity theft and payment card fraud.

Note: All merchants are required to be compliant with PCI Data Security Standards even if they are not required to validate that compliance.

American Express Data Security Operating Policy (DSOP)

As a leader in consumer protection, American Express has a long-standing commitment to protecting Cardmember Information and their Data Security Operating Policy for US Merchants ensures that it is kept secure. The DSOP is designed to address the threat of Cardmember Information compromise by implementing the PCI Data Security Standard. These enhanced safeguards and protections help improve customer trust, increase profitability and enhance a company's reputation.

PCI Data Security Standards Online Resources

- www.pcisecuritystandards.org
- www.visa.com/cisp
- www.mastercard.com/sdp
- www.discovernetwork.com/fraudsecurity/disc.html
- www.americanexpress.com/datasecurity

Payment Application Best Practices (PABP) Validated Payment Applications

Visa has developed a program in which payment applications are reviewed to ensure merchant compliance with the PCI Data Security Standards for the protection of cardholder data. In order to protect merchants from the financial and reputation damage associated with improper disclosure of cardholder data (e.g., an information security breach), Wells Fargo Merchant Services requires that all merchants utilizing payment application use only PABP validated applications. A list of these applications can be found at: www.visa.com/cisp

Card association news and updates, as well as compliance and regulation information are available online at: www.wellsfargo.com/biz/merchant/service/manage/associations

Operating Procedures Guide

The "Operating Procedures Guide" contains a summary of the key operational rules and regulations from the card associations. It describes the process for submitting payment card transactions for payment, obtaining authorizations, responding to chargebacks and media retrieval requests, and other aspects of our services. This guide provides information to assist you with the management of your payment processing account within the guidelines of your Merchant Agreement.

The Operating Procedures Guide is available online at:
www.wellsfargo.com/downloads/pdf/biz/merchant/guide_operating.pdf

Glossary

Term	Definition
ABA Routing Number	Directs electronic ACH deposits to the proper bank institution. Also referred to as a Transit Routing Number.
Automated Clearing House (ACH)	The paperless funds transfer system maintained by the Federal Reserve or other entities that have networks to exchange electronic funds transfer items.
Acquirer	Any bank, financial institution, or other company that maintains a merchant's credit card processing relationship and receives all transactions from the merchant to be distributed to the card issuers.
Address Verification Service (AVS)	A service provided in which the merchant verifies the card member's address with the card issuer. This is not a guarantee that a transaction is valid. Required by Visa for Internet card processing.
Adjustment	A debit or credit to a cardholder or merchant account to correct a transaction error.
Arbitration	The process followed by the card associations to determine whether a card issuer or an Acquirer has ultimate responsibility for a chargeback. Either member initiates this process after the re-presentment process is completed.
Association	See Card Association.
Authorization	Approval of a payment card transaction by the card issuer or approved independent service providers for a specified dollar amount. An authorization indicates only the availability of the card member's credit limit at the time the authorization is requested.
Authorization Approval Code	A number issued to a participating merchant by the Authorization Center that confirms the authorization for a sale or service.
Back-end Processor	A data processing company that contracts with Acquirers to provide communication and processing systems that connect with the interchange systems for clearing and settlement services on behalf of those Acquirers. (In some cases the Acquirer may act as its own back-end processor.)

Term	Definition
Bank Identification Number (BIN)	The six-digit range of numbers assigned by the Federal Bureau of Standards and used by card companies to identify their financial transactions. The Discover range begins with '6' (6xxxxx), the MasterCard range begins with '5' (5xxxxx), the Visa range begins with '4' (4xxxxx), and the American Express range begins with "3" (3xxxxx).
Batch	Usually a day's worth of transactions, including sales and credits to be processed by the card processor.
Card	See Payment card.
Card Association	Any entity formed to administer and promote cards, including but not limited to MasterCard International, Visa USA or Visa International, which are licensing and regulatory agencies for payment card activities.
Card Identification Number (CID)	The four-digit security number on the front of the American Express card the merchant can use to validate that the physical card is in the cardholder's possession at the time of the transaction. This helps prevent unauthorized or fraudulent use of the card.
Card Issuer	The card association member that issued a payment card to an individual and maintains that cardholder relationship. Also referred to as Issuer.
Card Not Present	A transaction where the cardholder does not physically provide the card to the merchant for processing (i.e., online, phone, fax).
Card Present	A transaction where the cardholder presents the card to the merchant for payment as demonstrated by swiping the card through a POS terminal or imprinting the credit card.
Card Validation Code (CVC2)	Card Validation Code. The three-digit security number on the back of the MasterCard card the merchant can use to validate that the physical card is in the cardholder's possession at the time of the transaction. This helps prevent unauthorized or fraudulent use of the card.
Card Verification Value (CVV2)	Cardholder Verification Value. The three-digit security number on the back of the Visa card the merchant can use to validate that the physical card is in the cardholder's possession at the time of the transaction. This helps prevent unauthorized or fraudulent use of the card.
Cardholder	An individual who has been issued a payment card and any authorized user of that card.

Term	Definition
ClientLine	The Internet-based service that makes a wide variety of merchant payment card account information available online. These reports provide a complete view of batches, cardholder information, and checking account transfers.
Credit	A refund or price adjustment given for a previous purchase transaction.
Credit Limit	The credit line set by the card issuer for the cardholder's account.
Credit Slip	A paper or electronic representation of credit that is issued to a cardholder on a prior credit card sale.
Currency Conversion	The process by which transaction currency is converted into the currency of settlement or the currency of the card issuer for the purpose of facilitating the authorization, clearing, and settlement reporting.
Decryption	The decoding system that computer software uses to unscramble information sent in code through the Internet. Decryption is the opposite of encryption.
Digital Certificate	Electronic identification used by consumer and merchants in specific Internet security systems. With digital certificates, the user and merchant can identify one another before conducting online transactions.
Discount Rate	A fee that Wells Fargo charges merchants for depositing, processing, and monitoring their daily card transactions. This fee is subject to changes in interchange fees and bank policies. For American Express discount means the amount that American Express charges a merchant for accepting the American Express® Card, expressed as (i) a percentage (Discount Rate) of the face amount of charges that the merchant submits or (ii) a flat transaction fee, or a combination of both.
Downgrade	Transactions that do not meet the guidelines of the assigned rate are subject to a fee, which is the difference between the assigned rate and the processed rate.
eCommerce	Conducting business online to include purchasing products and services over the Internet.
Electronic Check	An electronic check, or eCheck, payment moves funds directly from the consumer's bank account to the merchant's bank account.
Electronic Commerce Indicator (ECI)	A transaction data field used by eCommerce merchants and Acquirers to differentiate Internet merchants from other merchant types. Visa and MasterCard require that all eCommerce merchants use the ECI.
Electronic Integrated Dispute System (eIDS)	The Internet-based service that facilitates the management of chargebacks and retrieval requests.

Term	Definition
Encryption	The coding system that protects messages traveling between two points, such as a browser and a merchant's server, by scrambling the information. Used when card information is traveling over the Internet.
Firewall	A specifically programmed computer that connects a local network to the Internet and for security reasons allows only certain kinds of messages in and out.
Fulfillment	The response to a media retrieval request.
Imprint	When a credit card cannot be swiped through a terminal, it is necessary to imprint the embossed card information using a manual imprinter.
Interchange	The standardized electronic exchange of payment card transaction data between Acquirers and card issuers in accordance with card association rules.
Interchange Fees	Fees generally collected from Acquirers on the value of their card sales and paid to card issuers.
Interchange Network	An electronic network maintained by Discover, MasterCard, American Express, or Visa that exchanges data relating to the value of card sales and credits among Acquirers and card issuers.
Issuer	See Card Issuer.
Magnetic Stripe Reading (MSR)	When the credit card is swiped through the terminal to record the card information. Obtaining a magnetic strip reading proves the card's presence at the time of a transaction.
Mail Order / Telephone Order (MO/TO)	A transaction initiated by Internet, mail, phone, or fax; this is a card not present transaction.
MATCH	A shared database maintained by the card associations that lists all merchants terminated for cause by Acquirers.
Media	The documentation of monetary transactions (e.g., sales records, credit records, computer printouts, etc.)
Media Retrieval Request	A media retrieval request occurs when the customer requests more information about a transaction appearing on their credit card statement. The card issuer usually makes the request to the Acquirer for a copy of the original sales ticket.
Member	A financial institution that is a member of Visa and/or MasterCard.

Term	Definition
Merchant	The seller of goods and/or services; retailer or any other person, firm, or corporation that accepts credit cards, debit cards, or both.
Merchant Account	Also known as the Merchant Deposit Account. The funds from authorized transactions are "settled" into your merchant account with Wells Fargo Merchant Services.
Merchant Agreement	The written contractual agreement between a merchant and Wells Fargo Merchant Services, L.L.C., containing each party's respective rights, duties, and warranties with respect to the acceptance of cards.
Merchant Bank	The bank that enters into an agreement with a merchant to accept deposits generated by payment card transactions; also known as the Acquiring Bank.
Merchant Category Code (MCC)	Merchant Category Codes are special numbers assigned by the card associations to merchant types for identification and tracking purposes.
Merchant Identification Number (MID)	The number that identifies each merchant to the merchant processor for accounting and billing purposes.
Net Delivery Exposure (NDE)	The number of days between the time a cardholder is charged and when the order is fulfilled.
Non-Qualified Fees	See Downgrade.
Payment card	A credit card or debit card issued by a bank or other financial institution under brands Visa, MasterCard, American Express or Discover.
Payment Gateway	When a cardholder enters their card number on the merchant's website, the payment gateway automatically captures the data and securely forwards it to Wells Fargo Merchant Services for payment processing.
Re-presentment	The second stage in the chargeback process occurring when the Acquirer responds to the chargeback by returning a disputed transaction to the card issuer.
Retrieval Request	See Media Retrieval Request.
Sales Draft	Evidence of purchase of goods or services by a cardholder from merchant using a card, regardless of whether the evidence is in paper or electronic form, all of which must conform to card association rules.

Term	Definition
Secure Payment Page	A secure payment page assures customers that their payment information is encrypted for privacy and data integrity before it's sent over the Internet. This page is typically identified by the "s" in https:// (instead of http://). Payment gateway providers make this necessary eCommerce link possible by hosting the payment gateway software and individual secure payment pages on their own servers.
Secure Socket Layer Encryption (SSL)	The method of securing information traveling over the Internet. SSL is now the predominant security protocol for online transactions. Messages between the merchant's server and the consumer's browser are automatically encrypted (scrambled) when sent, and then decrypted (unscrambled) when received. This process prevents unauthorized persons from reading the data.
Seller or Online Seller	An individual or business that sells products or services and is capable of accepting payment for products and services via a merchant account.
Seller Account or Online Seller Account	The bank account a merchant identifies as the sole account from which monthly and/or transaction fees are debited.
Seller Bank	(Acquirer or Processor) The financial institution with which a merchant contracts to accept credit cards for payment of goods and services.
Seller Fees	Merchants are charged several types of fees for screening and processing online payments. Fees for products and services include, but are not limited to costs for the following: – Monthly Online Account – Discount rate – Per item charges for credit card and electronic check transactions – Chargebacks
Service Level Agreement (SLA)	Stated objectives or timeframe committed to merchant by the Bank for delivery of services.
Settlement	The transfer of funds in payment of amounts due to or from a member.
Shopping Cart	Shopping cart is software that allows buyers to select multiple products to purchase while having a single "check-out" experience. Payment gateways do not include shopping cart software. There are many shopping carts available. Check your payment gateway's website for a list of all compatible carts.
Signed Volume	Projected annual card volume ($) anticipated for a new merchant. Used to track the risk of an account.

Term	Definition
Standard Industry Code (SIC)	Special numbers assigned by the card associations to merchants for identification and tracking purposes. MasterCard uses MCC (Seller Category Code), while Visa uses SIC (Standard Industry Codes).
Terminal Identification Number (TID)	The number provided by the Bank to the merchant to identify the type of processing.
Transaction	An act between a merchant and a cardholder that results in either a paper or an electronic representation of the cardholder's intent to pay for goods or services received from the act.
Transit Routing Number	See ABA Routing Number.
Third Party Processor	A non-member agent employed by an Acquiring bank that provides authorization, settlement, and non-merchant services to a merchant.
Unauthorized Transaction	Any sale for which a cardholder does not provide his/her specific authorization (This should not be confused with the failure to receive an authorization response from the card issuer.)
Virtual Terminal	This is the online transaction terminal located in the merchant back office of the gateway. It allows merchants to key-enter transactions and perform other account maintenance functions.

Contacts & Resources

Contact Numbers

When calling us, please have the following items handy: your merchant ID number, business address, Taxpayer ID number, and the checking/savings account you use for settlement.

Customer Service	For all inquiries, account changes, security questions Tel 800-451-5817 24 Hours a Day, 7 Days a Week	
Payment Gateways	Authorize.Net	877-477-3938
	CyberSource	866-322-7924
	PayPal	888-883-9770
Authorization Assistance	Voice Authorizations for Visa® / MasterCard® / American Express®/Discover® Tel 800-626-4480 24 Hours a Day, 7 Days a Week	
Chargeback Help Desk	For media retrieval request and chargeback support Tel 800-451-5817 24 Hours a Day, 7 Days a Week	
ClientLine / eIDS	For all inquiries and ongoing support Tel 800-451-5817 24 Hours a Day, 7 Days a Week	

Online Resources

Wells Fargo Merchant Services	**www.wellsfargo.com/biz/merchant**
Visa	**www.visa.com/merchant**
MasterCard Merchant Services	**www.mastercardmerchant.com**
Discover	**www.discovernetwork.com**
Authorize.Net	**www.authorize.net**
CyberSource	**www.cybersource.com**
PayPal	**www.paypal.com**