Wells Fargo Merchant Services

Guide to Processing Card Payments

Welcome!

Thank you for selecting Wells Fargo Merchant Services

This *Guide to Processing Card Payments* brings together 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.

At Wells Fargo, we strive to build long-term 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.

Together we'll go far

 GTP 06/18

Table of Contents

Important resources

When calling us, please have the following items handy: Your merchant ID number, business name, address, taxpayer ID number, and the checking account you use with your merchant account.

Area or Topic	Specific Need	Contact Information
Customer Service	For all inquiries, account changes and security questions	**1-800-451-5817** 24 hours a day, 7 days a week
Wells Fargo Activation Group	To begin processing payments, equipment training, and setup	**1-800-939-6703** Mon-Fri 9 a.m. to 9 p.m. ET
Terminal Support Team	For terminal and printer assistance	**1-800-622-0842**
Clover® Go	Technical support	**1-866-277-4820**
Card processing software support	For questions regarding any card processing software issues	**1-800-365-1998** Mon-Fri 5 a.m. to 7 p.m. PT
Payment gateways	Authorize.Net	**1-866-277-4820**
	SecureNet	**1-888-231-0060**
	Payeezy Solutions	**1-855-448-3493**
	PayPal	**1-888-883-9770**
Authorization assistance	Visa® / Mastercard® / Discover® /American Express® Voice Authorization Unit (VRU) for Referrals and Code 10 Operator	**1-800-626-4480** 24 hours a day, 7 days a week
Media retrieval fax unit	For use when faxing in receipt copies and/or chargeback information	**Fax 402-933-1840**
Supplies reorder	To reorder supplies, call Customer Service	**1-800-451-5817** Mon-Fri 5 a.m. to 6 p.m. PT
	To order online	**shopmerchantsupplies.com**
Merchant products and services	To add and enhance your merchant account with products such as Gift Card, call Customer Service	**1-800-451-5817**
Business Track® · ClientLine® Reporting · Payment Tax Reporting · Dispute Manager	Sign up online today	**BusinessTrack.com**
	For technical assistance during enrollment in Business Track reporting	**1-800-285-3978** Mon-Fri 8 a.m. to 10 p.m. ET
	For general questions regarding our online reporting tools available through our Business Track homepage	**1-800-451-5817**

Online resources

Area or Topic	Contact Information
Wells Fargo Merchant Services	wellsfargo.com/biz/merchant
Wells Fargo Payment Network Information	wellsfargo.com/paymentnetworks
Visa resource for merchants	visa.com/merchant
Mastercard resource for merchants	mastercardmerchant.com
Discover resource for merchants	discovernetwork.com
American Express resource for merchants	americanexpress.com/merchant
Clover® detailed instructions	help.clover.com
Authorize.Net	authorize.net
SecureNet	securenet.com
Payeezy Solutions	firstdata.com/ecommerce
PayPal	paypal.com

Payment processing

In person payment processing:

Credit card processing

When your customer pays for products or services with a credit card, you can accept payments with:

- a traditional magnetic stripe card
- an EMV chip card
- mobile payments, including Wells Fargo Wallet™, Apple Pay®, Google Pay™, and Samsung Pay[1]

The card information is verified and the card issuer provides an authorization to Wells Fargo Merchant Services to indicate the availability of funds at the time of the purchase. If the card is damaged or the transaction does not take place in person, you can manually key in the card number; this may result in additional fees.

After you obtain an authorization and settle the transaction, the funds are transferred from your Wells Fargo Merchant Services account to your bank. You can have the funds transferred into any deposit account, but Wells Fargo can deliver your Visa®, Mastercard®, Discover®[2], and American Express®[3] transaction funds as soon as the next business day with a Wells Fargo deposit account.

Debit card processing

Debit cards access funds from the cardholder's bank account. There are two types of debit: PIN-based debit and Non-PIN debit. PIN-based debit transactions require cardholders to swipe or insert their cards at the point-of-sale and enter their PIN to authenticate the cardholder and authorize payment for goods or services. Cardholders do not sign a receipt. Non-PIN debit transactions require cardholders to swipe or insert their card at the point-of-sale or have the card number entered by a cashier and sign a receipt.

[1] Apple Pay, Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries.
Android, Google Pay, and the Google Logo are trademarks of Google LLC.
© 2017 Samsung Electronics America, Inc. Samsung and Samsung Pay, are trademarks or registered trademarks of Samsung Electronics Co., Ltd. Use only in accordance with law. Other company and product names mentioned may be trademarks of their respective owners. Samsung Pay is available on select Samsung devices.

[2] For Discover transactions, next day funding is only available for merchants with full service Discover processing (i.e., the authorization, processing, and settlement through Wells Fargo Merchant Services), and not available to merchants only using Wells Fargo Merchant Services to authorize Discover transactions.

[3] For American Express transactions, next day funding is only available for merchants where Wells Fargo Merchant Services (WFMS) is responsible for the authorization, processing and settlement of American Express Cards. It does not apply to merchants that have a direct relationship with American Express, where WFMS is responsible for only authorization and/or capture of American Express Cards, and American Express is responsible for processing and settlement.

Payment processing

Online payment processing:

Payment gateway

The payment gateway is a link between your website (or the website hosting your goods or services) and your payment processor (Wells Fargo). When your customer makes an online purchase, the information from your website must be sent through a payment gateway to obtain an authorization and for a payment card transaction to be completed. Payment gateways work with a variety of online payment service providers such as shopping carts and mobile wallets.

Getting started

There are a few simple steps to get started with your online merchant account.

Step 1 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
- SecureNet Payment Systems users will receive an email containing an activation link that enables merchants to create a login and password from merchantsupport@securenet.com
- PayPal Gateway users will receive an email with login and password from wells.fargo.products@first data.com
- Payeezy Gateway users will receive an email with login and password from wells.fargo.products@first data.com
- If you already have a payment gateway, Wells Fargo will send an email from wells.fargo.products@first data.com containing a merchant login and password, or merchant identification and terminal identification

Step 2 Review the information in this document to ensure that your website is ready to begin processing card payments.

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

Step 4 Start processing card transactions!

Authorization and authentication

Authorization

An authorization is an approval on a cardholder account for a sale amount. All card sales require an authorization from the card issuer to verify that the card is valid and has sufficient funds or credit line to cover the amount of the transaction. The card issuer provides an authorization and approval code to Wells Fargo.

Authorization 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. In addition, if the transaction is disputed at a later date, it is also important to retain the authorization code as proof of approval.

To obtain voice authorization, call our Authorization Center at 1-800-626-4480.

Visa, Mastercard, Discover, and American Express no longer require merchants that are able to accept chip card payments to obtain signatures for card-present credit or debit transactions. However, merchants can still use a customer signature as a cardholder verification method as required by individual state or local laws. Merchants who are not enabled to accept chip-card payments are responsible for the costs associated with card present fraud.

Authorization Codes and Messages

Code / Message	Response Definition
00 – Approved	A two to six digit approval code is provided.
02 – Declined	A business should never accept the card once declined and should request another form of payment.
03 – Pick Up Card	Please hold the customer's card. The card issuer wants the card returned to them. The merchant should never accept the credit card for payment when this response is received.
04 – Referral or Call Center	The card issuer requests direct contact with the merchant in order to authorize the sale. The merchant must contact the Wells Fargo Voice Authorization Center
08 – Invalid Debit Card	The cardholder account number was entered incorrectly.
10 – Invalid Account Number	The cardholder account number was entered incorrectly.
14 – Invalid Expiration	The cardholder expiration date was entered incorrectly.
15 – Invalid Transaction	Verify the customer information was entered correctly.
44 – Unable to Connect	This response indicates that the card issuing bank 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 / Pick-up Card	Decline – Do not try again
Waiting for Line	This response indicates that the phone lines are currently busy.
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.
Hold Card	Please hold onto the customer's card (if it's safe to do so). The card issuer requests that the card be removed from circulation. The merchant should never accept a card for payment when this response is received.

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

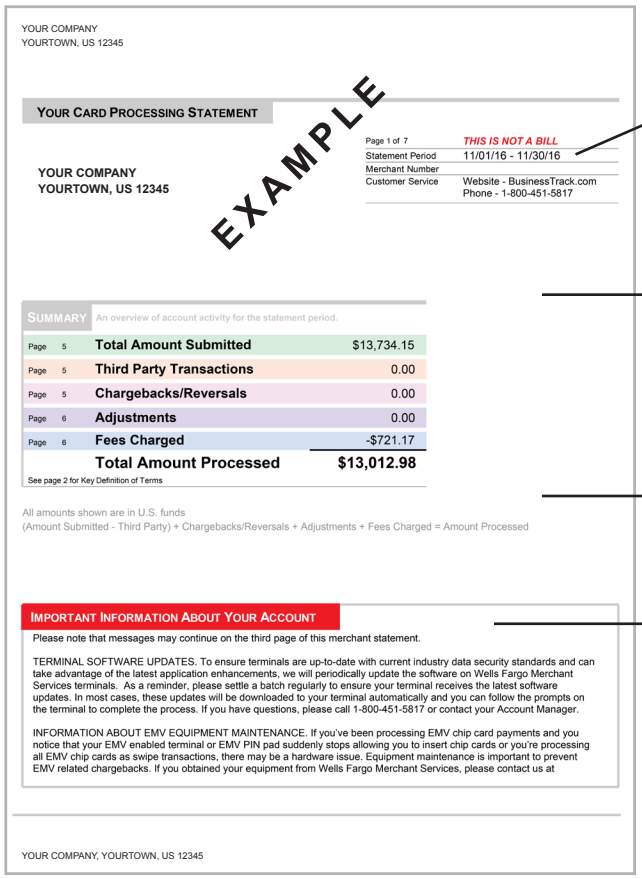
To maximize authorizations, take advantage of fraud protection services offered by Wells Fargo such as AVS and credit card security codes. Also consider using the additional fraud protection services provided by your payment gateway.

Please go to the section **Managing fraud and losses** for more information on fraud protection strategies and best practices.

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



YOUR COMPANY
YOURTOWN, US 12345

YOUR CARD PROCESSING STATEMENT

EXAMPLE

YOUR COMPANY
YOURTOWN, US 12345

Page 1 of 7 — THIS IS NOT A BILL
Statement Period 11/01/16 - 11/30/16
Merchant Number
Customer Service Website - BusinessTrack.com
Phone - 1-800-451-5817

SUMMARY An overview of account activity for the statement period.

Page 5	Total Amount Submitted	$13,734.15
Page 5	Third Party Transactions	0.00
Page 5	Chargebacks/Reversals	0.00
Page 6	Adjustments	0.00
Page 6	Fees Charged	-$721.17
	Total Amount Processed	$13,012.98

See page 2 for Key Definition of Terms

All amounts shown are in U.S. funds
(Amount Submitted - Third Party) + Chargebacks/Reversals + Adjustments + Fees Charged = Amount Processed

IMPORTANT INFORMATION ABOUT YOUR ACCOUNT

Please note that messages may continue on the third page of this merchant statement.

TERMINAL SOFTWARE UPDATES. To ensure terminals are up-to-date with current industry data security standards and can take advantage of the latest application enhancements, we will periodically update the software on Wells Fargo Merchant Services terminals. As a reminder, please settle a batch regularly to ensure your terminal receives the latest software updates. In most cases, these updates will be downloaded to your terminal automatically and you can follow the prompts on the terminal to complete the process. If you have questions, please call 1-800-451-5817 or contact your Account Manager.

INFORMATION ABOUT EMV EQUIPMENT MAINTENANCE. If you've been processing EMV chip card payments and you notice that your EMV enabled terminal or EMV PIN pad suddenly stops allowing you to insert chip cards or you're processing all EMV chip cards as swipe transactions, there may be a hardware issue. Equipment maintenance is important to prevent EMV related chargebacks. If you obtained your equipment from Wells Fargo Merchant Services, please contact us at

YOUR COMPANY, YOURTOWN, US 12345

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 **Summary** summarizes card activity and related charges for the statement period. Use the page numbers to help you quickly find details.

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

Key card processing terms in plain language

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

Third-Party Transactions — These are transactions that are passed directly to third party service providers for processing and/or funding. Common third-parties include American Express®and Discover®.

Chargebacks/Reversals — Those transactions that are challenged or disputed by a cardholder or card issuer. A Chargeback equals the transaction amount that is disputed by the cardholder or card issuer. A Reversal is the amount that was initially resolved against the merchant, but has subsequently been resolved in favor of the merchant.

Adjustments — The amounts added to or deducted from your account to resolve processing and billing discrepancies.

Fees Charged — Transaction-based and/or fixed amounts charged for specific card processing services.

Interchange Charges — These are the variable fees charged by card payment networks for processing transactions. Factors that affect Interchange Charges include card type, information contained in the transaction, and how/when the transaction was processed.

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, fees, and chargebacks/reversals. Please note that some fees shown on this statement may not be deducted from your account until several business days after the receipt of this statement.

Merchant Number — The unique account number assigned to every merchant and merchant location. You'll find it at the top of your statement.

Reporting

Business Track® account management solution

Business Track is a secure online account management and reporting portal for your merchant account. Business Track is available to you 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 **BusinessTrack.com** and answering a few questions to initiate your enrollment.

The Business Track portal gives you access to powerful reporting and analysis tools including:

- **ClientLine® Reporting** – View payment processing information such as sales, bank deposits, and statements, and create and schedule custom reports viewable online or available via email.
- **Dispute Manager** – Receive, view and respond to chargeback and retrieval disputes online.
- **Payment Tax Reporting** – Quick and easy access to tax information.

There's no charge for using ClientLine Reporting and Payment Tax Reporting. Dispute Manager is also available at no extra charge for most businesses. If you have any questions about these services, please call your Wells Fargo Merchant Services Account Manager or a customer service representative.

ClientLine Reporting

Benefits

- Gain anytime access – manage your accounts at a time that is convenient for you
- Minimize cost – view, print, and download your merchant processing statements at no extra cost and before your paper statements are mailed[4]
- Perform historical / trend analysis – for more robust account information
- Streamline reconciliation – download information for easy analysis
- Security – manage user access with passwords

Dispute Manager

Dispute Manager 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. For access to Dispute Manager, go to the **User Preferences** pull down menu on the Business Track homepage and select **Request Application**. Or call Customer Service.

(continued)

[4] Enrolling in Business Track online reporting will not automatically stop delivery of your monthly statement by mail.

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

Payment Tax Reporting

Payment Tax Reporting provides merchants with quick and easy access to their payment card processing tax reporting information through the Business Track homepage. The solution provides merchants the ability to easily view and manage their tax information through a centralized tool.

Benefits

- View tax validation reports
- Access gross reportable sales reports
- Retrieve copies of your 1099-K forms

Interchange

What is interchange?

Interchange is the standardized electronic exchange of bank card transaction data between merchant acquirers and card issuers in accordance with card payment network 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 paid by merchants to card issuers and the card payment networks for each card payment transaction, which is included in your processing cost. The fee compensates the card issuers 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 payment networks will quote the lowest rate for a transaction assuming that a number of requirements are met. A downgrade, or non-qualified transaction, is a card sales transaction that does not meet all requirements for the lowest rate and will process at interchange levels that carry higher costs. 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 payment networks' requirements are not met, the transaction will be categorized at a different and more expensive interchange level.

What can I do to qualify for the best 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:

- **Make sure your customer properly inserts their EMV chip card into the terminal**

  Using a keypad to enter card information rather than inserting an EMV chip card into the terminal is a common reason for a downgrade. Hand-keyed information has a higher risk of error and/or fraud because only the card number and expiration date are needed for a transaction. When a card is inserted into an EMV enabled terminal, it captures the full track data on the embedded microchip of the card.

- **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.

(continued)

- **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.

- **Establish procedures to limit the number of voice authorizations**

  Voice authorizations do not capture electronic authorization codes required to qualify for the lowest transaction rates. Therefore, these transactions are subject to interchange downgrades. Only utilize voice authorizations when prompted by your point-of-sale device.

- **Send settlements on time**

  A merchant must settle transactions in order to receive their funds. Settling means submitting the approved card transactions to Wells Fargo Merchant Services. We then forward your settlement request to the payment networks who confirm the transaction with the card issuer.

  Be aware that transactions have to be settled within a specific amount of time after authorization to avoid higher interchange rates. Wells Fargo recommends daily settlement of all transactions. Periodically check that the phone/data lines on your equipment are working correctly to avoid late settlement. The equipment can also be programmed to automatically settle transactions at times you specify.

- **Review the *Cost Management Strategies Guide***

  This guide provides many of the reasons for 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 *Cost Management Strategies Guide* is available online at **wellsfargo.com/biz/managecosts**. You can also view a quick video about managing cost at **wellsfargo.com/managepaymentcosts**.

Dispute process

What can I do when a customer disputes a transaction?

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 (for chargeback transaction only), 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, please fax a clear and legible copy of the sales record. Please respond by the reply by date on the retrieval request. 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 withdrawn funds from Wells Fargo for the transaction, and Wells Fargo withdraws funds from the merchant account as stipulated in the Merchant Agreement and card payment network 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.

(continued)

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 Dispute Manager, 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 Dispute Manager.)

Card issuers have the right to issue chargeback 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 funds from your account are immediately withdrawn 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, there will be a due date on the request form indicating when you must 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 issues the claim.

If you have already issued a credit to your customer, 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 as 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 by the due date on the request form 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

(continued)

You may also need to provide:

- 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 we will deposit funds into your account. 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 funds from your account will be withdrawn accordingly. A reversal is not a guarantee that the chargeback has been resolved in your favor.

What tools are available to manage chargebacks?

Dispute Manager

Dispute Manager is the optional online tool accessible through the Business Track portal with simple enrollment steps at BusinessTrack.com. Once enrolled for the Dispute Manager service, chargebacks are posted to your account enabling you to investigate and resolve chargebacks in the most efficient manner possible. Dispute Manager also provides information required on media retrieval requests for outstanding, reversed, and expired disputed transactions. (Also see **Reporting** section.)

Managing fraud and losses

In person payment processing:

How can I prevent fraud & chargebacks?

- Have proof the card was present by making sure all cards swiped through or inserted into your terminal.
- Get an imprint whenever a card has to be manually keyed into a terminal. Be sure that all of the transaction information shows up on the imprinted copy including the amount, merchant name and location.
- If the credit card is declined when swiped through or inserted into your terminal, do not continue to try and get an authorization. Instead you should request a new form of payment from the cardholder.
- Verify that the number on the screen matches the number on the card.
- Obtain an authorization number for the full amount of the sale – do not break the sale into several smaller amounts.
- When handling a refund, always issue a credit to the card account used for the original sale. Clearly disclose your return policy.
- Settle transactions promptly. In cases where settlement is delayed more than 5 days, we recommend obtaining a new authorization.

What if I think a transaction is suspicious?

Call the Authorization Center at 1-800-626-4480 and ask for the Code 10 Operator, which indicates that you suspect a fraudulent transaction.

(continued)

When should I not accept a card payment?

- Hologram does not appear on the card or if it appears altered. Look for the hologram on Visa (flying doves), Mastercard (interlocking globes), Discover (celestial sphere of interlocking rings), and JCB (logo cards) cards. For American Express, some cards contain a holographic image on the front or back of the plastic to determine authenticity. Not all American Express Cards have a holographic image.
- Card shows signs of tampering (i.e., signature panel shows evidence of erasure; the account number or name on the front of the card looks uneven or misaligned).
- Card is unsigned. Ask for identification and have the customer sign the card in your presence. If the customer refuses, do not accept the card.
- Transaction is occurring either prior to the valid date or after the expiration date on the card. Ask for another form of payment.
- Account number on the face of the card and the number displayed on the terminal do not match, even if an authorization is received.
- For card not present transactions; multiple transactions on one card or similar cards with a single billing address but multiple shipping addresses.

Managing fraud and losses

Online payment processing:

Payments made online are classified as "card not present" transactions because the card is not physically processed by a card swipe terminal. 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.

Payment network compliance

The payment networks exist for the purpose of facilitating payment transactions. To most effectively manage fraud and risk in today's business environment, the payment networks 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 an online 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

(continued)

How can I reduce fraud and chargebacks?

Here are some tips to consider when setting up your website or order processing system that may help 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 accept your terms and conditions online.
- 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 "2" or 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 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.

(continued)

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 1-800-626-4480 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.

Data breach protection, plus PCI Compliance assistance – at no extra cost

We are committed to helping you protect your data in the event of a data breach with a program specifically designed for businesses that accept payments over the internet or that use independent software vendor (ISV) point of sale software.

- To help you survive a data breach, you now have up to $50,000 in protection for each merchant ID (up to $500,000 for your business) from Royal Group Services.[5] There is no additional cost to you for this protection and no deductible.
- To help you prevent data breaches, we have made it easy for you to certify your PCI DSS[6] compliance by using Trustwave. When you use Trustwave to certify your compliance, we will cover the cost.
- You could save on fees. If you're not certified, you may be paying a monthly non-compliance fee for each merchant ID. If you're already certified by another provider, you could avoid non-compliance fees by registering at **www.pci.trustwave.com/wellsfargo**.

[5] This product is not being offered or sold by Wells Fargo Bank, N.A. or Wells Fargo Merchant Services, L.L.C. It is offered directly through a third party provider, Royal Group Services. For more details, visit www.royalgroupservices.com/breachprotection.

[6] Payment Card Industry Data Security Standard

Data security and industry compliance

The card payment networks exist for the purpose of facilitating payment transactions. To most effectively manage fraud and risk in today's business environment, the card payment networks 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, Discover, and American Express information security programs. PCI Data Security Standards protect cardholders while minimizing the risk to your business.

Although Visa, Mastercard, Discover, and American Express programs are based on the PCI Data Security Standards, each card payment network 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. The program then assigns penalties 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. The program then assigns penalties for entities that either 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.

(continued)

American Express Data Security Operating Policy (DSOP)

As a leader in consumer protection, American Express has a long-standing commitment to protect Cardmember Information and the 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.

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

Online resources

- **pcisecuritystandards.org**
- **visa.com/cisp**
- **mastercard.com/sdp**
- **discovernetwork.com/merchants/data-security/disc.html**
- **americanexpress.com/datasecurity**

Payment Application Data Security Standard (PA-DSS), validated payment applications

The Payment Card Industry Security Standards Council (PCI SSC) mandates that all businesses that use a payment application to process card payments ensure that it has been validated to comply with the PA-DSS. Merchants who are not compliant may no longer be able to process card payments. To verify that your payment application is compliant, please visit **pcisecuritystandards.org/security_standards/vpa**.

Card payment network news and updates, as well as compliance and regulation information are available online at **wellsfargo.com/biz/merchant/service/manage/network**.

Operating Procedures Guide

The *Operating Procedures Guide* contains rules and regulations from the card payment networks and Wells Fargo Merchant Services. It describes the process for submitting bank 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 **wellsfargo.com/merchantoperatingguide**.

Risk monitoring

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

These risk reviews may result in a change to your reserves, funding limits, or delay funding, as explained in your *Merchant Agreement*. We will notify you within three (3) business days of these reviews. If you anticipate changes in your processing activity, please call Customer Service at 1-800-451-5817 to proactively discuss changes to your original *Merchant Agreement*.

When should you contact Customer Service to update your Merchant Agreement?

- Change to your estimated card processing volumes
- Change to your estimated average dollar value per transaction
- Change in product 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 to your merchant account profile such as address, DBA name, legal name, entity type or legal structure, and primary contact information
- Change to your bank account information or tax ID number

Merchant products and services

Wells Fargo Merchant Services offers a variety of secure payment processing products and services designed to increase sales and customer satisfaction. Wells Fargo Merchant Services features seamless integration to multiple payment processing systems, full automation of reporting and operational tools, and comprehensive equipment and software.

Call our Customer Service at 1-800-451-5817 for additional information on the products and services described in this section.

PIN debit acceptance

PIN debit transactions require cardholders to swipe or insert their cards at the point-of-sale and enter their PIN to authenticate the cardholder and authorize payment for goods or services. Cardholders do not sign a receipt. With PIN debit payment, electronic deposits are made to the merchant account automatically, simplifying daily deposit reconciliation. PIN debit is a preferred method of payment for many customers because it's quick to process and minimizes the potential for fraud.

EMV chip card acceptance

If you have not upgraded to EMV chip card enabled equipment – you may be putting your business at risk – and missing opportunities to better serve your customers. EMV technology offers benefits to both consumers and businesses. EMV technology offers more secure transactions to help reduce counterfeit card fraud. It also prepares your POS equipment to accept mobile wallets and contactless payments, giving customers more purchasing options with EMV chip cards, smartphones, and other devices.

Mobile device payment acceptance

Many merchants want to accept the latest in payment technology, and we'll make sure you're equipped. Contactless payment solutions communicate with a card, smart phone or watch, via a wireless signal. You can accept contactless payments using your EMV enabled terminal or customer facing PIN pad. At the point-of-sale, cardholders can hold their mobile device near the terminal, making purchases quicker and more convenient for consumers and merchants. This solution is ideal for merchant environments that have a high volume of sales and depend on the merchant's ability to process transactions quickly.

Clover Check Acceptance (also known as TeleCheck)

Clover Check Acceptance turns paper checks into electronic items at the point-of-sale. Your customers will have a fast, secure, and more convenient way to pay and you'll benefit from a reduction in bank fees, check returns, and check handling expenses.

Mobile products

Sometimes business opportunities don't happen near an electrical outlet or phone line. That's why we offer mobile products to help you accept payments on site, online, or on the go. You can accept credit, signature debit, and PIN debit cards. Our mobile products deliver fast and secure transactions. They'll also help you obtain authorizations in seconds and improve your cash flow. We also have mobile products that work with your existing smartphone or tablet.[7] These lightweight, compact designs help you grow your business by quickly, easily, and reliably taking card payments anywhere you have customers.

Gift cards

Gift cards have become a popular choice for gift giving. Wells Fargo Merchant Services offers closed loop stored-value cards. With the closed loop stored-value cards, a consumer purchases a gift card from you with cash, check, credit, or debit card for any dollar amount. The card is activated and the amount purchased is recorded on the card by swiping a magnetic stripe card through a point-of-sale terminal. You can customize your gift cards with your name and logo imprinted on them. These gift cards can only be used to purchase goods/services at your business.

Wells Fargo Merchant Services can help you set up a closed loop stored-value card program for your business. Call our Customer Service at 1-800-451-5817 to establish your gift card program.

[7] Mobile access with data plan is required. Available for iPhones, iPads, and selected Android smartphones and tablets.