

# New Account Reference Guide

## Welcome to BBVA Compass Merchant Services

Thank you for choosing BBVA Compass as your Merchant Services provider. BBVA Compass is dedicated to providing your business with the solutions and support you need to grow your business.

# Let's Get Started

## Activate Your Account Today

It's important for all new merchants to receive training, so that you understand the importance of key processes regarding the operation of your point-of-sale device and to help protect your business from fraud, chargebacks and to help minimize your processing related expenses.

**1**

Contact the Merchant Activation Team at 1-800-239-1220 to schedule your telephone training appointment once you receive your initial shipment or e-mail notification informing you that your account is now ready for processing.

**2**

Prior to your scheduled telephone training appointment, gather the information that you received such as your terminal (if applicable), quick reference guide, overlay, etc. Having this information readily available will reduce your training time and allow you to get back to managing your business and accepting payment through BBVA Compass.

**3**

Now that you have completed your training, ensure that your customers know you accept credit cards. Be sure to place acceptance decals in a prominent place. You can order free signage online at [www.discovernetworkorders.com](http://www.discovernetworkorders.com).

# Contact Information

Enter your Merchant ID, Terminal ID, and Technical Support Help Desk number during your telephone training session. You may also wish to cut out this information and keep it close to your point-of-sale device as this information will be helpful to you in the future.

_____
Merchant Identification Number
_____
Terminal Identification Number (V#)
_____
Technical Support Help Desk
1-800-239-1220
_____
Customer Service / Supplies
1-800-291-4840
_____
Visa®, MasterCard®, Discover®
Network Voice Authorization Center
1-800-528-2121
_____
American Express® Voice
Authorization Center
1-888-857-6227
_____
Chargebacks / Retrieval Requests

1-800-552-8227
_____
Terminal Help Desk
1-800-390-7924
_____
CounterPASS / WebPASS Help Desk)
1-866-392-8326
_____
ExaDigm Wireless Help Desk
1-866-929-6883
_____
WAY Systems Wireless Help Desk
1-800-390-7924
_____
POS Partner Help Desk

# Frequently Asked Questions

## **When will funds be deposited into my business checking account?**

Visa®, MasterCard®, and Discover® Network transactions will be deposited into your BBVA Compass business checking account the next business day. This applies to transactions transmitted to BBVA Compass prior to 10:00pm MST. Deposits from American Express® can be expected within 3-5 business days, depending on your agreement with this card brand.

## **What are the hours of operation for customer service?**

Customer Service Representatives are available to assist you Monday – Friday, 7am – 7pm CST. You may reach Customer Service at 1-800-239-1220 or by e-mail at [merchant@bbvacompass.com](mailto:merchant@bbvacompass.com).

## **What are the hours of operation for the technical help desk?**

Terminal Help Desk:	800-552-8227	24/7
CounterPASS/WebPASS:	800-390-7924	24/7
ExaDigm Wireless Help Desk	866-392-8326	24/7
WAY Systems Wireless Help Desk	866-929-6883	24/7
POS Partner Help Desk	800-390-7924	24/7

## **When will the amount due listed on my statement be deducted from my business checking account?**

The total amount due will be deducted from your business checking account on the 15th of each month or the next business day should the 15th fall on a weekend or observed holiday.

## **How do I update my account information such as address and phone number?**

Submit a request via e-mail to [merchant@bbvacompass.com](mailto:merchant@bbvacompass.com) or fax your request to (205) 297-6159.

## **How do I submit a change in ownership, type of business or a change in the way I sell a product or service?**

Contact Customer Service at 1-800-239-1220 to establish a new account.

## **How can I perform a transaction that is for more than what I have been approved for?**

Contact Customer Service at 1-800-239-1220. Approval is not guaranteed

# Frequently Asked Questions (continued)

## **What is a Mid-Qualified, Non-Qualified Fee?**

Transactions are typically classified as qualified, mid-qualified, or non-qualified based on qualification requirements from Visa, MasterCard, and Discover Network.

A mid-qualified transaction occurs on any standard consumer card keyed with fraud controls including Address Verification Service (AVS) and an invoice number in addition to some reward cards.

A non-qualified transaction occurs on any standard consumer card keyed without fraud controls such as AVS and an invoice number and some reward cards. In addition, government, business, commercial, purchasing and international cards will qualify as non-qualified.

Qualification can also be affected by the timeliness in which a transaction is submitted. It is important to settle your transactions on a daily basis. For more information, contact Customer Service.

## **What is AVS and why should I enter it?**

The Address Verification Service (AVS) helps reduce the risk of fraudulent use of account numbers in card-not-present transactions. When a customer provides an address with an order, AVS automatically compares it to the billing address on file with the card issuer. This risk reduction measure is especially helpful to merchants conducting business via mail, telephone, or over the Internet. If the billing address and the card address on file do not match, you will receive a response code indicating this during transaction processing. In addition, it is imperative to utilize AVS to help minimize your processing expenses.

## **Why is it important that I enter the sales tax?**

The card brands require this data to be transmitted with the transaction. The data is typically passed on to the cardholder's reporting programs. In addition, it is imperative to enter the sales tax amount when prompted to help minimize your processing expenses.

# Frequently Asked Questions (continued)

## **What is a credit card verification number?**

A credit card verification number is a 3 or 4 digit number associated with a card that helps prevent fraudulent use. During a phone or Internet transaction, a credit card verification number is requested to ensure that the card being used is in the presence of the cardholder.

- Visa: CVV2 (Card Verification Value)
- MasterCard: CVC2 (Card Validation Code)
- Discover Network: CVV (Card Verification Value)
- American Express: CID (Card Identification Number)

On a Visa, MasterCard, or Discover Network card, you'll find the verification number on the back of the card in the signature panel as the last three (3) digits. American Express uses a four-digit code that's located just above the credit card number on the front of the card and to the right side.

## **What is a ticket request?**

When cardholders do not recognize transactions on their card statements, they typically ask their card issuer for a copy of the related transaction receipt to determine whether the transaction is legitimate. In this situation, the card issuer first tries to answer the cardholder's questions. If this cannot be done, the card issuer electronically sends a "request for copy" (also known as a "retrieval request" or "ticket request") to BBVA Compass.

Upon receipt of the request from the card issuer, BBVA Compass will request the transaction receipt and other supporting documentation from you. You must send a legible copy of the transaction receipt and supporting documentation to the number listed on the correspondence at your earliest convenience and no later than the date due. Placing a call to customer service will not resolve the request, the only resolution is to provide the requested information. Additionally, if you do not have the requested information you should send the documents you do have relating to the transaction in question. If requested information is not provided it may result in delayed deposits and/or irreversible chargebacks.

# Frequently Asked Questions (continued)

## **How do I process a refund for my customer?**

DO NOT PROCESS A VOID! A VOID DOES NOT REFUND YOUR CUSTOMER.

*Credit Transaction* – Select refund/credit on the terminal, swipe card or enter the account number, follow terminal prompts. You will need the invoice number from the original receipt or your records. Refer to your quick reference guide for terminal specific instructions.

*PIN-Based Debit Transaction* – Select ATM Return on the terminal, swipe card, and follow terminal prompts. The card must be present! If not, you will need to provide credit in another form, such as cash. You will need the invoice number/network ID from the original receipt or your records. Refer to your quick reference guide for terminal specific instructions.

## **FAQs – Terminal Responses**

### **Call Help – IC, ID, or IR**

Invalid response code, invalid download line, or invalid response message. Call the help desk for assistance.

### **Please Try Again – CE, LC, or TO**

Communications error – no answer, Communications error – lost carrier, or Connection made – no response. Try the transaction again.

### **Declined**

Request another payment type from the customer.

### **Invalid Card Type/Unsupported Card**

Your terminal is not enabled for this type of card. Contact Customer Service to explore adding this card type to your account

### **Invalid Card**

The card number is incorrect. Re-enter the card number.

### **Card Error**

The terminal is unable to read the magnetic strip on the card.

# Tips to Help Avoid Chargebacks

Most chargebacks can be attributed to improper transaction-processing procedures and can be prevented with appropriate training and attention to detail. The following best practices will help you minimize chargebacks.

## Point of Sale

- **Declined Authorization.** Do not complete a transaction if the authorization request was declined. Do not repeat the authorization request after receiving a decline. Instead, ask for another form of payment.
- **Transaction Amount.** Do not estimate transaction amounts. For example, restaurant merchants should authorize transactions only for the known amount of the check; they should not add on a tip.
- **Referrals.** If you receive a “Call” message in response to an authorization request, do not accept the transaction until you have called your authorization center. In such instances, be prepared to answer questions. The operator may ask to speak with the cardholder. If the transaction is approved, write the authorization code on the sales receipt. If declined, ask the cardholder for another card.
- **Expired Card.** Do not accept a card after its “Good Thru” or “Valid Thru” date.
- **Card Imprint for Key-Entered Card-Present Transactions.** If, for any reason, you must key-enter a transaction to complete a card-present sale, make an imprint of the front of the card on the sales receipt, using a manual imprinter. Avoid capturing an impression of the card using a pencil, crayon, or other writing instrument. This process does not constitute a valid imprint. Even if the transaction is authorized and the cardholder signs the receipt, the transaction may be charged back to you if the receipt does not have an imprint of the embossed account number and expiration date. If you do not have a manual imprinter, contact Customer Service at 1-800-239-1220 to purchase one.
- **Cardholder Signature.** The cardholder’s signature is required for all card-present transactions, except for qualified small-ticket transactions. Failure to obtain the cardholder’s signature could result in a chargeback if the cardholder later denies authorizing or participating in the transaction. When checking the signature, always compare the first letter and spelling of the surname on the sales receipt with the signature on the card. If they are not the same, ask for additional identification or make a Code 10 call.
- **Digitized Cardholder Signature.** Some cards have a digitized cardholder signature on the front of the card in addition to the hand-written signature on the signature panel on the back. Checking the digitized signature is not sufficient for completing a

# Tips to Help Avoid Chargebacks (continued)

transaction. Sales staff must always compare the customer's signature on the sales receipt with the hand-written signature in the signature panel.

- **Fraudulent Card-Present Transaction.** If the cardholder is present and has the account number but not the card, do not accept the transaction. Even with an authorization approval, the transaction can be charged back to you if it turns out to be fraudulent.
- **Legibility.** Ensure that the transaction information on the sales receipt is complete, accurate, and legible before complete the sale. An illegible receipt, or a receipt which produces an illegible copy, may be returned because it cannot be processed properly. The growing use of electronic scanning devices for the electronic transmission of copies of sales receipts makes it imperative that the item being scanned be very legible.

## **Customer Service**

- **Delayed Delivery.** If the merchandise or service to be provided to the cardholder will be delayed, advise the cardholder in writing of the delay and the new expected delivery or service date.
- **Item Out of Stock.** If the cardholder has ordered merchandise that is out of stock or no longer available, advise the cardholder in writing. If the merchandise is out of stock, let the cardholder know when it will be delivered. If the item is no longer available, offer the option of either purchasing a similar item or cancelling the transaction. Do not substitute another item unless the customer agrees to it.
- **Disclosing Refund, Return, or Service Cancellation Policies.** If your business has policies regarding merchandise returns, refunds, or service cancellation, these policies must be disclosed to the cardholder at the time of the transaction. Your policies should be pre-printed on your sales receipts; if not, write or stamp your refund or return policy information on the sales receipt near the customer signature line before the customer signs (be sure the information is clearly legible on all copies of the sales receipt). Failure to disclose your refund and return policies at the time of a transaction could result in a dispute should the customer return the merchandise.
- **Return, Refund, and Cancellation Policy for Internet Merchants.** This policy must be clearly posted to inform cardholders of their rights and responsibilities (e.g., if the merchant has a limited or no refund policy, this must be clearly disclosed on your website before the purchase decision is made to prevent misunderstandings and disputes). The limited or no refund policy must be displayed on a screen that requires the cardholder to "click and accept" the terms of your policy. This policy page cannot be bypassed.

## 5 Simple Steps to Safer Key-Entered Transactions

Can't swipe the stripe? It could just be a de-magnetized card...or maybe not. It's up to you to put more action into your key-entered transaction to help avoid the possibility of counterfeit fraud.

### When the Stripe Won't Swipe

1. Check the terminal to make sure it is working properly. If the terminal is okay and the problem appears to be with the magnetic stripe, follow your company procedures for key-entered transactions. Be sure to check the card security features and match signatures (steps 2-5 below).
2. Check the card's "good thru" date to be sure the card hasn't expired. If the transaction date is after the "good thru" date, the card has expired.
3. Obtain a manual imprint of the card.
4. Ask the customer to sign the imprinted sales draft.
5. Compare the signature on the card with the signature on the sales draft to be sure they match. Do not accept an unsigned card! If the card is unsigned, ask the cardholder to sign it in your presence, and to provide government identification (driver's license or passport). Compare the signatures on the transaction receipt, the card, and the additional identification.

If you suspect fraud, make a Code 10 call. Call your voice authorization center and say "I have a Code 10 authorization request." Follow the operator's instructions if you can do so safely.

## Take the Order – But Don't Get Taken In

Never ship a valuable order unless it checks out and has been authorized. Know the signs of possible fraud when the card is not present. Keep in mind...none of these by itself means you're being scammed – but several of them together might.

### Be alert for transactions with several of these characteristics:

- First time shopper
- Larger than normal orders
- Orders consisting of several of the same item

# Take the Order – But Don't Get Taken In (continued)

- Orders made up of “big-ticket” items
- Orders shipped “rush” or “overnight”
- Orders shipped to an international address

## **Maintain a customer database or account history to track buying patterns and compare individual sales for indicators of possible fraud:**

- 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
- Multiple cards used from a single IP (Internet Protocol) address

Check everything...never ship a valuable order unless it checks out and you've received a valid authorization.

# If the Card is NOT There – You Need to be MORE Aware

With the proper know-how and the right tools, mail order, telephone order and Internet merchants can detect fraud and potentially avoid associated card losses.

## **To stay ahead of criminals and reduce your fraud exposure:**

1. Ask the customer for the card expiration date and include it in your authorization request. An invalid or missing expiration date can be an indicator that the person on the other end does not have the actual card in hand.
2. Use fraud detection tools like the Address Verification Service (AVS) and Card Verification Value 2 (CVV2) as part of the authorization process.
3. Be on the lookout for questionable transaction data or other signs indicating “out of pattern” orders.

# If the Card is NOT There – You Need to be MORE Aware (continued)

## **If you suspect fraud:**

- Ask the customer for day/evening phone numbers, then call the customer with any questions.
- Ask for additional information (e.g., bank name on the front of the card).
- Separately confirm the order by sending a note via the customer's billing address, rather than the "ship to" address.

Report any suspicious activity to BBVA Compass at 1-800-239-1220.

## **Skimming is a Scam**

Skimming is a fraud scam in which a cardholder's account information is electronically copied, or "skimmed," off the card's magnetic stripe, often in the process of an otherwise valid transaction. The skimmed information is used to produce counterfeit payment cards that are, in turn, used from fraudulent transactions.

Skimming often occurs in card-present environments, such as restaurants and service stations, where transaction processing may occur out of sight of the cardholder. To skim a card, fraudsters typically use a small portable device to copy the magnetic stripe.

## **To prevent skimming, you should be on the lookout for:**

- Anyone operating an electronic device not normally used in your day-to-day business activities.
- Anyone offering you money to record account information.

If you suspect skimming activity is happening at your place of business, call BBVA Compass at 1-800-239-1220 or your company security immediately.

# Code 10 Calls

## Code 10 Calls

Code 10 calls allow merchants to alert card issuers to suspicious activity and take appropriate action when instructed to do so. You should make a Code 10 call to your voice authorization center whenever you are suspicious about a card, a cardholder, or a transaction. The term “Code 10” is used so the call can be made at any time during a transaction without arousing a customer’s suspicions.

### To make a Code 10 call:

- Keep the card in your possession during the call.
- Call your voice authorization center and say, “I have a Code 10 authorization request.” After basic merchant and transaction details are reviewed, you will then be transferred to the card issuer and connected to a special operator who will ask you a series of questions that can be answered with as simple “yes” or “no.”
- When connected to the special operator, answer all questions calmly and in a normal tone of voice. Your answers will be used to determine whether the card is valid.
- Follow all operator instructions.
- If the operator tells you to pick up the card, do so only if recovery is possible by reasonable and peaceful means.

Sometimes a sales associate may not feel comfortable making a Code 10 call while the cardholder is at the point of sale, or the sales associate may become suspicious of a cardholder who has already left the store.

Emphasize to your sales staff that they can make Code 10 calls even after a cardholder leaves the store. A Code 10 alert at this time may help stop fraudulent card use at another instruction, or perhaps during a future transaction at your store.

# Important Information About Unsigned Cards

## **If an unsigned card is presented, the merchant must:**

- Obtain usual authorization for the transaction;
- Ask the customer to provide confirming identification; and
- Require the cardholder to sign the card. You must not complete the transaction if the cardholder refuses to sign the back of their card.

## **What if the cards says “Ask for Photo I.D.” in the signature space?**

- The transaction cannot be processed unless the cardholder’s signature appears in the signature space.
- As noted on the cards, they are “not valid unless signed.”

## **Why do cards need to be signed?**

- The signature on the back of the card is one of a multi-layered set of security protections in place for cardholders and merchants. The presentation of a signed card allows a merchant to verify the cardholder’s identification by comparing the signature on the card to that on the sales receipt.

# Payment Card Industry (PCI) Data Security Standard (DSS)

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

**The PCI Data Security Standard consists of 12 basic requirements supported by more detailed sub-requirements.**

## **Build and Maintain a Secure Network**

*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data

*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

## **Protect Cardholder Data**

*Requirement 3:* Protect stored cardholder data

*Requirement 4:* Encrypt transmission of cardholder data across open, public networks

## **Maintain a Vulnerability Management Program**

*Requirement 5:* Use and regularly update anti-virus software

*Requirement 6:* Develop and maintain secure systems and applications

## **Implement Strong Access Control Measures**

*Requirement 7:* Restrict access to cardholder data by business need-to-know

*Requirement 8:* Assign a unique ID to each person with computer access

*Requirement 9:* Restrict physical access to cardholder data

## **Regularly Monitor and Test Networks**

*Requirement 10:* Track and monitor all access to network resources and cardholder data

*Requirement 11:* Regularly test security systems and processes

## **Maintain an Information Security Policy**

*Requirement 12:* Maintain a policy that addresses information security

### **Helpful Links:**

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

[www.visa.com/merchant](http://www.visa.com/merchant)

[www.mastercard.com/us/merchant](http://www.mastercard.com/us/merchant)

[www.discovernetwork.com](http://www.discovernetwork.com)

[www.americanexpress.com/merchant](http://www.americanexpress.com/merchant)

# Data Breach Insurance Program

In 2008, data breaches rose almost 50% compared to the year before, with nearly 40% of those breaches targeting businesses and another 20% targeting schools, according to the Identify Theft Resource Center (ITRC) and the Washington Post.

BBVA Compass, in partnership with Royal Group Services, delivers added peace of mind to business owners through our Data Breach Insurance Program. This program is a unique insurance offering designed for our customers to specifically meet the expenses resulting from a suspected or actual breach of card data.

The program is offered exclusively by Royal Group Services and underwritten by Great American Insurance Group, a financially strong insurance organization whose insurance companies are rate “A” by independent third party rating agencies.

## **Why do I need this coverage?**

If you suffer a suspected or actual data breach, the average cost for a Level 4 merchant is \$36,000 of unexpected costs in the form of audit expenses, card monitoring and replacement expenses, and fines. These costs could significantly affect revenue – and even jeopardize the existence of your business. This inexpensive policy reduces your monetary exposure when an assumed or actual data compromise occurs, thus providing peace of mind!

## **What does the program cover?**

- A mandatory forensic audit required by the Payment Card Industry Data Security Standard (PCI DSS) of a merchant when a data breach is suspected.
- The data breach can be either a system/network breach or the physical theft of the credit card data from stolen receipts, stolen computers, skimming, or even employee theft.
- Card replacement costs and related expenses resulting from the data breach.
- All Level 2, 3, and 4 merchants regardless of their level of compliance with the standard.

## **How can I learn more?**

Visit [www.royalgroupservices.com/bbvacompass](http://www.royalgroupservices.com/bbvacompass) for access to our web portal with vital program information including frequently asked questions as well as the ability to obtain your evidence of insurance for your records.

