BB&T MERCHANT SERVICES

BB&T's Merchant Guide to Fraud Prevention

As a BB&T Merchant Services client, you can expect superior products and service. Our goal is to provide you with resources and tools to help you grow and protect your business. This guide provides information on types of fraud, susceptible processing methods, and indicators to identify and prevent potential fraud that may result in chargebacks and losses to your business.

Fraud Types

- Customer purchases your goods or services using stolen cards or card numbers. In a non-EMV environment, this can lead to chargebacks you are liable for repaying.
- Customer tests stolen cards to see if they will be authorized by purchasing a small dollar amount. This is commonly known as "AuthTesting" and is most common through a website.
- Owners and employees process personal or company cards through the merchant payment system. This is done by issuing credits to an individual's card, processing a transaction to their own card for a cash advance or processing payments for a different business entity.
- An individual or entity asks you to be their representative or partner by opening a merchant account in your name to process transactions on their behalf.

Susceptible Processing Methods

- **Wires** – Fraudsters will often place an order with a company that includes additional funds and a request for a wire transfer for shipping or other funds movement. With the wire, the fraudster will receive cash from a stolen card. The fraudster may also request you add funds to the wire to send to an individual or a third party.
- **Card-Not-Present Transactions** – The customer pays through a website or through mail/telephone orders. Because the card and cardholder are not present, you cannot verify the identity of the cardholder. Individuals who have stolen cards and card numbers often target websites because of the lack of verification of cardholder identity.
- **Force-Entered Transactions** – Allows the merchant to bypass the authorization process by manually entering a previously obtained authorization code. Submitting fictitious authorization codes may create chargeback risks. Ensure you obtain a valid authorization code and do not accept one provided by the client.

Fraud Indicators

- Customer uses multiple cards that have the same first six digits in the card number, or asks to pay for a single order with multiple cards (also known as split transaction), or pay for a single order with multiple transactions of a certain amount.
- Customer places an order and has someone else pick up the merchandise.
- You receive email or telephone orders from an unfamiliar company with a generic email address (such as Yahoo, Gmail or Hotmail) or a phone call through a telecommunications relay service line, especially if you do not have a website or advertise that you accept orders by email.
- Customer requests you run a transaction to wire funds to pay for shipping or "insurance" fees.
- Customer requests you ship their purchases to an alternate address.
- Customer needs the order to be completed urgently and wants immediate notification of the transaction being processed and product being shipped.
- Customer requests you acquire a merchant account to accept their payment for a particular job or service.
- Any transactions that appear out of normal business activity including, but not limited to, large or unique orders, multiple orders, orders from outside typical geographic footprint or orders for items that could be easily re-sellable.

Best Practices

- Use the password protect option for the credit (refund) function on your terminal so only certain employees can issue refunds on credit cards. Create multiple users for virtual terminals and maintain strict user permissions. Only allow administrative personnel the ability to perform refunds.
- Verify the name on the card with the customer's identification, such as driver's license, before processing every transaction.
- Always ask for another card or form of payment after receiving a declined authorization. Do not attempt to run the declined card again. This will make you liable for chargebacks and will create a hold for the customer.
- Reach out to your third-party provider about fraud monitoring tools and enable what is available (such as velocity filters and IP address blocking) to protect your website from fraud attacks.
- Add a verification tool such as CAPTCHA to your website.
- In a face-to-face environment always insert CHIP cards into the terminal.
- In a non-face-to-face environment, always include the card verification value (CVV) and customer address with the transaction and only process if you receive an exact match result code for both. It is an individual business decision to ship if CVV doesn't return an exact match. Be aware this could lead to a chargeback you are unable to remedy.
- Remember, an authorization should be seen as an indication that account funds are available and the card has not been reported lost or stolen. It is not proof the true cardholder engaged in the transaction.

If you have questions on additional fraud prevention, please contact our Merchant Client Support Center at 877-672-4228, Monday through Friday from 8:30 a.m. to midnight ET and Saturday from 10:30 a.m. to midnight ET.

Additional Resources

- The BB&T Merchant Agreement
- Visa's website: https://usa.visa.com/support/small-business/fraud-protection.html
- MasterCard's website: https://www.mastercard.us/en-us/merchants.html. Choose "Safety & Security."
- Discover's website: www.discovernetwork.com, select "Business Resources" and then "Fraud & Security."

Thank you for choosing BB&T as your financial partner.

BB&T Merchant Services

BB&T, Member FDIC. BB&T Merchant Services are subject to business type and credit approval.