# Welcome to Merchant Services

## Start processing payments today

CONTENTS:



M&T Bank

# Let's get started!

We're delighted you've chosen to partner with M&T Bank Merchant Services.® We're looking forward to working with you to provide efficient and effective payment processing solutions to meet your business needs.

You'll find what you need to know in the enclosed materials to set up your account, process transactions and view helpful data and information. Any equipment or software you've purchased may be shipped separately and should arrive within a few days.

**Please follow these three steps below to get started.**

## 1. Activate your account.

Your merchant services account is ready to use. If you have any questions, please refer to your laminated Quick Reference Card for customer support phone numbers.

## 2. Validate your PCI security compliance.

You have been automatically enrolled into Security Metrics, our preferred PCI partner. Complete your validation as soon as possible by following the directions in the email you receive from Security Metrics.

RETURN TO MAIN MENU

If you have any questions, please contact us at **1-800-724-7031.**

M&T Bank

# AVS Quick Guide

## ADDRESS VERIFICATION SERVICE

M&T Bank

### If the card is not there...you need to be more aware.

Card not present merchants can be held financially responsible for a fraudulent transaction, even if the issuer has approved it. This is because there is a greater chance of fraud due to the absence of a card imprint and cardholder signature. The good news is that there are effective tools available. To stay ahead of the crooks and reduce your fraud exposure, use fraud detection tools like the Address Verification Service (AVS) and Card Verification Value 2 (CVV2 – Visa), Card Verification Code (CVC – MasterCard), Card Identification Code (CID – Discover Network) as part of the authorization process.

A card not present transaction authorization indicates that the account is in good standing. It does not mean the true cardholder or a legitimate card is involved. That's why it's important to include fraud detection tools like AVS and CVV2/CVC/CID as part of the authorization process. To begin with, before performing an authorization consider the following:

### KNOW THE SIGNS OF POSSIBLE FRAUD

- First time shopper
- Larger than normal orders
- Orders consisting of several of the same item
- Orders made up of "big ticket" items
- Orders shipped "rush" or "overnight"
- Orders shipped to an international address
- Transactions with similar account numbers
- Shipping to a single address but transactions placed on multiple cards
- Multiple transactions on one card over a short period of time

***Be alert for transactions with several of these characteristics. Keep in mind that a transaction with one of these signs does not mean you're being scammed. But several of them together might. Never ship a valuable order unless it checks out and you received a valid authorization.***

### IF YOU SUSPECT FRAUD

- Ask the customer for day/evening phone numbers, then call the customer with any questions
- Ask for additional information. (i.e. bank name, bank phone, type of card, etc.)
- Separately confirm the order by sending a note via the customers billing address (not shipping address).
- Report suspicious activity to M&T Bank customer service at 1-800-724-7031.

### AVS

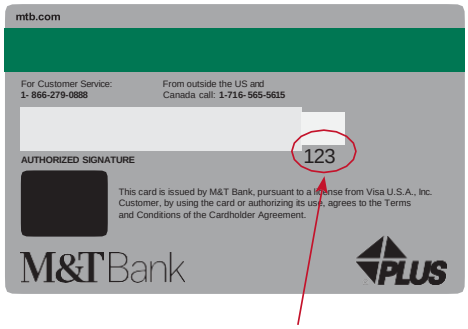
AVS allows card-not-present merchants to check a cardholder's billing address with the card issuer. The merchant receives a code indicating whether the address given by the cardholder matches the address on file with the card issuer.

**Caution:** When you receive a "partial match" or "no match" AVS response, you should take appropriate steps to assure yourself that the customer is not acting fraudulently.

| AVS Code | Definition | Explanation |
|---|---|---|
| A | Partial match | Street address matches, zip code does not match |
| N | No Match | Street address and zip code do not match |
| R | Retry | Issuer system unavailable, retry later |
| W | Partial Match | Street address does not match, zip code matches |
| X | Exact Match | Street address and zip code match |
| Y | Exact Match | Street address and zip code match |
| Z | Partial Match | Street address does not match, zip code matches |

## CVV2 / CVC2 / CID

In the card-not-present environment, CVV2 / CVC / CID is an excellent tool for verifying the customer has a legitimate card in hand at the time of the order. This code is located on the back of all cards and consists of the last three digits printed on the signature panel.




**This code is the last three digits printed on the signature panel located on the back of all cards.**

| CVV2 Code | Explanation |
|---|---|
| M | Exact match |
| N | Does not match |
| P | Code was not present |
| S | Code was present but not submitted |
| U | Code not verified |

| CID Code | Explanation |
|---|---|
| M | CID exact match |
| N | CID does not match |
| P | Not Processed |
| S | CID should be on card, but merchant indicates not present |
| U | Issuer is not certified |

**To protect CVV2 / CVC / CID from being compromised, NEVER keep or store a card's code once a transaction has been completed. Such action is prohibited, and it could result in association fines.**

RETURN TO MAIN MENU

M&T Bank

# PCI Compliance

## YOUR SIMPLIFIED PCI COMPLIANCE SOLUTION

M&T Bank

M&T is constantly thinking of credit card safety. Our commitment to help our merchants reduce credit card fraud is evident in the elements we've built into our merchant products and services. Our goal is simple: to help you keep your customer data from hackers and help protect your reputation.

Working with SecurityMetrics®, a leading Qualified Security Assessor ("QSA") that's been approved by the PCI Council, our merchants are automatically enrolled[1] in our PCI program and receive the benefits of an all-in-one, comprehensive PCI Compliance solution, unless a merchant opts out of this service. SecurityMetrics is a third party provider and is not affiliated with M&T.

### With your PCI program , you'll get:

- **Liability Warranty**[2] – Subject to certain terms and conditions, breach protection that provides reimbursement of up to $100,000 per merchant identification number in the event of a security breach
- **Self-Assessment Questionnaire ("SAQ") Assistance** – SecurityMetrics has a simple way to guide you through completion of the required SAQ based on your business type and mode of processing
- **IP Address Scanning** – SecurityMetrics will perform scanning as required depending on your business type and mode of processing
- **24x7 Support** – SecurityMetrics will be there for you when you need help. Visit M&T Security Metrics or call 1-801-705-5700
- **Email/Call Reminders** – SecurityMetrics will let you know if your submission is complete or when your next annual assessment is due

**For more information about PCI Compliance and M&T's PCI solution, contact our dedicated PCI team at SecurityMetrics today.**

**CALL** 1-801-705-5700

**VISIT** M&T Fraud Security PCI Compliance

RETURN TO MAIN MENU

[1] Merchants may opt out of this enrollment, but certain fees and conditions may apply.

[2] Premium Service Warranty is only available for merchants processing fewer than six million each of Visa®, MasterCard®, and Discover® cards transactions annually. Premium Service Warranty only applies to a confirmed breach of which M&T Bank has been notified by the card association. Premium Service Warranty is subject to other eligibility requirements and terms and conditions provided by RGS upon enrollment.  **mtb.com**

# Merchant Services

## PCI FAQ

M&T Bank

**What is PCI?** The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards, with a focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.)

**Does PCI apply to me?** The PCI DSS applies to any organization, regardless of size or number of transactions, that accepts, transmits, or stores any cardholder data.

**What steps do I need to take to become compliant with PCI DSS requirements?** M&T has provided you with access to a PCI portal through our preferred PCI partner SecurityMetrics. You will receive an email the month following the opening of your account to enroll. After enrollment you will be asked some scoping questions to determine which SAQ is required. We take the guesswork out and determine which SAQ applies to your situation automatically within the portal based on your responses.

**Can I choose to use a different PCI vendor, outside of SecurityMetrics, to become compliant?** Yes, however you need to provide proof of compliance from that vendor to M&T. You can provide proof of compliance to mtbmerchantservices@mtb.com.

**What is an SAQ?** A SAQ is a self-assessment questionnaire that the merchant needs to complete. There are various SAQs determined by the scoping questions.

**How long is compliance good for?** An SAQ is good for one year. However, if a merchant requires quarterly scans in addition to the SAQ, they may become non-compliant if scans fail within that year.

**What if I choose not to enroll and to not become compliant?** If a merchant fails to enroll and become compliant, they will be charged a $29.99 fee every month until compliant. You also are at risk of a data breach. The payment brands may, at their discretion, fine $5,000 to $100,000 per month for PCI compliance violations. A breach and resultant fines can be catastrophic to a small business. If a merchant does not enroll, they also forfeit their $100,000 of data breach coverage provided by M&T.

**During the SAQ I was asked about if I have a policy and procedure?** If you don't already have a policy/procedure for your employees, there is a template policy available to you within the portal. You can find this template via the PCI Policies section of the SecurityMetrics portal.

**My business has multiple locations, is each location required to validate PCI compliance?** If your business locations process under the same Tax ID, then typically you are only required to validate once annually for all locations. If applicable, you also need to have quarterly passing network scans for each location.

RETURN TO MAIN MENU

# EMV Quick Guide

## EUROPAY MASTERCARD VISA CHIP CARD

M&T Bank

EMV is one of the hottest topics in the payments industry. As a leading payments processor, Vantiv is at the forefront of the EMV migration in the United States. The rollout of EMV in the U.S. will affect the entire payments ecosystem, including the cardholders themselves. It is important for everyone to familiarize themselves with EMV and what it means to them.

### What is EMV?

EMV is a series of specifications that define a more secure method of payment. It was developed jointly by Europay, MasterCard and Visa in the mid-1990s. Even though the standards body is now owned by other brands as well, EMV still bears the initials of its original three members. The EMV standards are governed by the organization EMVCo. Visit EMVCo.com for more information.

The overarching goal of EMV is to facilitate secure global interoperability between chip cards and terminals for both credit and debit transactions. EMV introduces a small computer or "chip" to every payments device. This chip stores information, performs processing, contains secure elements that store secret information and performs cryptographic functions. The most important feature of EMV is the dynamic data generated with each transaction. This dynamic data makes it nearly impossible to create counterfeit cards or replay intercepted transactions.

### Why is the U.S. market implementing EMV?

EMV protects against counterfeit fraud through authentication of dynamic data residing on chip cards, smartphones and other devices that are EMV-compliant. EMV also provides risk management parameters at the card level and offers both online and offline PIN, to further protect everyone against lost and stolen fraud. Counterfeit fraud is growing in the U.S. With the rest of the world either in the process of migrating to or already migrated to EMV, counterfeit fraud in the U.S. has become a primary target for fraudsters.

### Why now?

Since EMV has been implemented in every other major payment market in the world, the global payments brands have now decided it is time for the U.S. to migrate. Current card associations' mandates and liability shifts for the U.S. are listed below.

| Visa | Mastercard | Discover | American Express |
|---|---|---|---|
| • Processors must support EMV<br>• Liability shift of counterfeit transactions<br>• Liability shift for AFD | • Processors must support EMV<br>• International ATM liability shift<br>• Liability shift of counterfeit transactions<br>• ATM Liability Shift<br>• Liability shift for AFD | • Processors must support EMV<br>• Liability shift of counterfeit transactions<br>• Liability shift for AFD | • Processors must support EMV<br>• Liability shift of counterfeit transactions<br>• Liability shift for AFD |

RETURN TO MAIN MENU

## M&T Merchant Services Team

1-800-724-7031

### General service questions

- Statement
- Billing
- Disputes
- Interchange

### Technical support services

- Point-of-sale (POS) terminals
- PC software questions

### Voice authorization

- Ability to receive manual voice authorizations for sales when your POS terminal or software does not work properly. Be sure to have your Merchant ID # from your terminal sticker.

## Address Verification System (AVS Codes)

Code definition explanation

Y = Exact match (V/M/A) street address and ZIP match
Partial match (D), street address matches only

A = Partial match (V/M/A) street address matches, ZIP does not
Exact match (D) street address and ZIP match

Z = Partial match (V/M/D/A) ZIP matches, address does not

N = No match (V/M/D/A) street address and ZIP does not match

U = Unavailable (V/M/D/A) not available for given account #
or their bank does not offer AVS

R = Retry (V/M) issuer AVS not available at current time

S = Unavailable (V/M/A) not available for given account #
or their bank does not offer AVS

W = Partial match (M) unavailable (D) 9 digit ZIP code matches,
street address does not match.

X = Exact (M/D) street address and ZIP match

E = Error occurred

C = Merchant did not key in AVS info

G = Unavailable (V/M) international issuer not participating in AVS

## VISA IAVS Codes

International AVS Codes

B = Street address match, postal code does not match

C = Street address and postal code not verified

D = Street address and postal code match

I = Address information not verified

M = Street address and postal code match

P = Postal code match, address not verified – incompatible format

(V)=Visa (M)=MasterCard (A)=American Express (D)=Discover

RETURN TO MAIN MENU


# Merchant Services

## Card Acceptance and Reference Guide

M&T Bank

## Welcome to M&T Bank Merchant Services, your premier provider of debit and credit card processing. Inside this booklet, you will find useful information and helpful tips to make it easier for you to process your Card Transactions.

The Card Associations also provide detailed processing information on their websites. We encourage you to visit the Card Association websites at:

- MasterCard® Resource Library
  https://www.mastercard.us/en-us/merchants/get-support.html
- Visa® Operating Regulations
  https://usa.visa.com/support/small-business/regulations-fees.html
- Discover®
  www.Discovernetwork.com
- American Express® Merchant Operating Guide
  www.americanexpress.com/merchantopguide
- OptBlue®
  https://optblue.com/

If, after reviewing this Guide and/or visiting the Association websites, you are unable to find the answer to your questions, please call an **M&T Bank Merchant Services Specialist at 1-8**00-724-7031 during the hours of 8am to 5pm (ET).

**This Guide is not a substitute for, or an amendment to, the Card Association Rules or your Merchant Services Agreement with M&T Bank**. Defined terms used in this Guide have the meanings used in your Merchant Services Terms and Conditions Agreement, Acceptance and Processing Terms or the Card Association Rules. In the event of a discrepancy or conflict between this Guide and the Card Association Rules or the Merchant Services Agreement, the Card Association Rules and Merchant Services Agreement will prevail.

By following the proper procedures outlined in your Merchant Services Agreement, following the Association Rules, and safeguarding against fraud, accepting credit and debit cards can help you grow your business.

# TABLE OF CONTENTS

# CARD TRANSACTION FLOW

*Processing a credit card transaction involves two steps: Authorization and Settlement.*

## STEP ONE: AUTHORIZATION

The Authorization process allows the Card issuer to approve or decline Transactions. Authorizing Transactions offers you the best protection against fraud and chargebacks. Typically Authorizations take only seconds to complete.

When requesting an authorization, you may receive one of the following responses:

**1. "Approved"**

- **Definition:** The Card issuer will allow the Transaction
- **Action:** Continue with the Transaction

**2. "Decline" or "Card Not Accepted"**

- **Definition:** The Card issuer will not allow the Transaction.
- **Action:** Return the Card to the customer and inform them that their Card issuer has declined the Transaction. Suggest that the customer call the Card issuer on the reverse side of their card for more information. Ask the customer for another form of payment

**3. "Call" or "Call Center"**

- **Definition:** The Card issuer wants you to call the voice Authorization center and provide more information before approving the Transaction
- **Action:** Hold the Card and call the voice Authorization center at 1-888-602-0323 for further instructions or ask for another form of payment

**4. "Pick Up":**

- **Definition:** The Card issuer wants you to keep the Card
- **Action:** Retain the Card, if this can be done peacefully

**5. "Code 10 Authorization"**

- **Definition:** This is a special request for Authorization when the Cardholder is suspected of trying to perform a fraudulent or unauthorized Transaction
- **Action:** Call the Voice Authorization Center at 1-888-602-0323 and state, "I have a Code 10 Authorization request." Keep the Card in hand when making the call. You may be transferred to a special operator. The operator will ask a series of questions that can be answered "yes" or "no." These questions allow you to verify the authenticity of the Card without alarming the Cardholder. If requested by the special operator, retain the Card, if this can be done by peaceful means

## STEP TWO: SETTLEMENT ("BATCHING OUT")

You need to settle each Transaction, in order to receive payment in your Merchant Deposit Account. To prevent inaccuracies, it is important to reconcile your Device and Transaction Records **PRIOR** to settlement. Once your Transaction Records are settled, the Transactions are sent to the Cardholder's bank to be added to the Cardholder's Card balance or deducted from the Cardholder's deposit account balance. The funds transfer typically occurs within two days. Once the transfer is complete, the deposit will post to your Merchant Deposit Account depending on your funding schedule.

# RECONCILING YOUR MERCHANT ACCOUNT

*Reconciling your merchant account involves two steps:* ***Daily Batch Reconciliation and Monthly Statement Reconciliation.***

## STEP ONE: DAILY BATCH RECONCILIATION

You should verify that each batch accepted in every Device matches the Transactions accepted at your location each day **PRIOR** to settling the batches. This includes tip adjustments if you are a restaurant or beauty salon. If your Device is set to auto-close, it's important that you reconcile your receipts with your Device prior to settling. If set on auto-close, ensure you received the auto-close receipt on the following day. If the batch did not auto settle, it is your responsibility to settle the batch according to instructions provided for your Device or third-party service provider.

If you manually close out your batches, also ensure that your receipts match your Device. Be sure to manually close the batch on time based on your funding schedule.

In all cases, batches submitted later than 24 hours after the approval date/time may be subject to additional fees and charges.

### STEP TWO: MONTHLY STATEMENT RECONCILIATION

You should always verify that the batches submitted daily match the batches reported on your monthly merchant statement. If you are missing a deposit or there appears to be an error in the rates or fees charged on the statement, please contact an **M&T Bank Merchant Services Specialist at 1-800-724-7031 from 8am to 5pm (ET)** to determine next steps. In some cases, you may need to re-enter the batch or research will be performed based on the issue. **You must notify M&T Bank of any errors within thirty days of your statement date.**

## MASTERCARD®, VISA®, AND DISCOVER® INTERCHANGE ("Interchange") AND AMERICAN EXPRESS® PROGRAM PRICING ("Program Pricing")

Card issuers incur costs when processing Card Transactions for their customers. This fee is called Interchange for MasterCard, Visa and Discover, and Program Pricing for American Express. Interchange and Program Pricing reimburses Card Issuers for the following:

- The cost of fraud and credit losses on Cardholder accounts
- The outstanding credit card balances between the date of purchase and receipt of Cardholder payment
- The operating cost of posting transactions to Cardholder accounts
- And other costs

MasterCard, Visa, Discover Network and American Express determine the Interchange or Program Pricing rates based on the type of Card used for the Transaction (Consumer, Commercial, International, Rewards, etc.) and how the Transactions are processed (Card-Present, Card-Not-Present, Restaurant, Hotel, etc.). Merchant services providers (also known as acquirers or processors), pay issuers a fee for each Transaction processed; it is the largest component of the fees M&T Bank Merchant Services charges your business for processing Card Transactions.

For more information on Interchange or Program Pricing, visit:

- MasterCard® Interchange Rates
  https://www.mastercard.us/en-us/about-mastercard/what-we-do/interchange. html
- Visa® Interchange Rates
  https://usa.visa.com/support/small-business/regulations-fees.html#1
- Discover® Interchange Rates
  https://www.discovernetwork.com/en-us/home/data/acqIntchgLanding.html (Verification Code: disc5379)
- American Express OptBlue® Program Pricing Rates
  Not available online, contact an M&T Bank Merchant Services Specialist at 1-800-724-7031 for more information

In addition to Interchange and Program Pricing Rates and Fees, there are also "pass-through" charges of various fees defined by the individual card brands. These are passed onto each merchant account based on card type accepted on your monthly merchant statement. These pass-through charges are typical for every merchant acquirer/processor in the industry. A standard listing of M&T pass-through fees can be found at: http://www.mtb.com/mstc

# PROCESSING TYPES

## PROCESSING CARD-PRESENT TRANSACTIONS

Card-Present Transactions are those that occur when there is face-to-face contact with the Cardholder. The business typically inserts, swipes, or waves (if contactless payment) the Card through a point-of-sale device to obtain an Authorization and requires the Cardholder to sign a sales slip. The sales slip is extremely important as it provides evidence of the Transaction. A copy of the sales slip is required to be given to the Cardholder and kept on file by the business a minimum of 36 months (3 years) for future reference.

The sales slip or invoice must contain the following items:

- Last 4 Digits of the Card Account Number
- Card Expiration Date
- Transaction Date
- Total Amount of the Sale
- Business Name
- City and State (where the Transaction occurred)
- Cardholder Name
- Cardholder Signature
- Authorization number

If your sales slip does not contain the items outlined above, please contact an M&T Bank Merchant Services Specialist at 1-800-724-7031 from 8am to 5pm (ET).

If you are unable to insert, swipe, or wave (if contactless payment) the Card, key-enter the Card account number into your Device. Be sure to record the Card account number manually and ask the Cardholder to sign a sales slip. Include the Authorization number on the sales slip.

## QUALIFYING FOR THE BEST CARD – PRESENT INTERCHANGE OR PROGRAM PRICING RATES

- Insert, swipe, or wave (if contactless payment) the Card
- Obtain a signature or PIN number if prompted
- Request one electronic Authorization per Transaction (all transactions MUST have a valid authorization code to avoid penalty fees for no authorization)
- Ensure the authorized amount is equal to the Transaction amount
- Settle Transactions no later than 1 day from the Authorization date

  ***Exception:*** *Restaurants, taxi cab drivers, and salons may NOT add a tip to the original, Authorized Transaction. There is a 20% variance between the authorized and settled amounts to compensate for tip adjustments. All other merchant transactions should be reauthorized for the difference between the authorized and settled amount if greater than 20%.*

## PROCESSING CARD-NOT-PRESENT TRANSACTIONS

Card-Not-Present Transactions are those that occur when there is no face-to-face contact with the Cardholder. The business receives the purchase requests via: mail, telephone, fax, or Internet. The business typically key-enters the Card account number through a Device to obtain an Authorization.

An Authorization for a Card–Not-Present Transaction does not guarantee the authenticity of a Card or Transaction.

A sales slip or invoice is extremely important to provide evidence of the Transaction. If possible, send the Cardholder a sales slip or invoice for the Cardholder to sign and return to you. A copy of the signed sales slip or invoice should be kept on file by the business for future reference.

The sales slip or invoice must contain the following items:

- Last 4 Digits of the Card Account Number
- Card Expiration Date
- Transaction Date
- Total Amount of the Sale

- Business Name
- City and State (where the Transaction occurred)
- Cardholder Name
- Cardholder Signature
- Authorization number

You may **NOT** submit a Transaction for payment until you ship the merchandise or provide the services ordered. This policy helps protect you from costly disputes by minimizing the possibility that customers are billed before receiving the goods or services they ordered. It applies to all Transactions except as noted below. The date the goods are shipped or the services provided is the Transaction date. Any shipping and handling charges should be included in the total Transaction amount Authorized.

## QUALIFYING FOR THE BEST CARD-NOT-PRESENT RATES INTERCHANGE OR PROGRAM PRICING RATES

- Key-enter the Card account number
- Complete Address Verification Service ("AVS") and Card Verification Value ("CAV2/CVV/CVV2/CID")
- Include customer service telephone number and order number when prompted by your software, gateway or terminal
- Request one Authorization per Transaction (all transactions MUST have a valid authorization code to avoid penalty fees for no authorization)
- Ensure the Authorized amount is equal to the Transaction amount
- Settle Transactions no later than 1 day from the Authorization date

  ***Exception:*** *You may complete two sales slips for a single Transaction ONLY if there are delayed delivery situations. The first sales slip represents a down payment for the goods or services and the second sales slip represents the balance due.*

Card-Not-Present businesses can be held financially responsible for fraudulent transactions, even if the Card issuer has approved it. This is because there is a greater chance of fraud due to the absence of the Card and Cardholder signature. There are security tools available to assist you in detecting and preventing fraudulent activity. The most common tools are Address Verification Services ("AVS") and Card Verification Value 2 (CAV2/CVV/CVV2/CID). Some software or gateways have fraud filters you can engage/adopt to assist with mitigating fraud. Your third-party vendor should be able to assist you with activating these features.

# ADDRESS VERIFICATION SERVICES ("AVS")

AVS is an automated program that allows a business to verify a US Cardholder's billing address (and some Canadian and European-issued cards may be eligible for AVS) during the Authorization process. The Card issuer compares the Cardholder address (street number and zip/postal code) submitted with the Authorization request to the billing address it has on file for the Cardholder. The business then receives a code indicating whether the addresses match.

| AVS Code | Definition | Explanation |
|---|---|---|
| A | Partial Match | Street matches, zip code does not match |
| E | Invalid | AVS data is invalid |
| N | No Match | Street and zip code do not match |
| R | Retry | Issuer system unavailable, retry later |
| S | Not Supported | Issuer does not support AVS |
| U | Unavailable | Information is unavailable |
| W | Partial Match | Street does not match, zip code matches |
| X | Exact Match | Street and zip code match |
| Y | Exact Match | Street and zip code match |
| Z | Partial Match | Street does not match, zip code matches |

***Caution:*** *When you receive a "No Match" or "Partial Match" AVS response, you should take the appropriate steps to assure yourself that the Cardholder is not acting fraudulently. Please refer to CARD ACCEPTANCE SECURITY on Pages 9-16.*

CAV2/ CVV2/CVC/CID is a three-digit number imprinted at the end of the Card account number on the signature panel on the back of the Card. This tool was designed to help validate that the customer has a genuine Card in their possession. You can confirm the CAV2/CVV2/CVC2/CID value with a US Card issuer when you request an Authorization.




| CAV2/CVV/CVV2/CID Code | Explanation |
|---|---|
| M | Exact match |
| N | Does not match |
| P | Code was not processed |
| S | Code was present, but not submitted |
| U | Code not verified |

***Caution:*** *When you receive anything BUT "Exact Match", you should take appropriate steps to assure yourself that the Cardholder is not acting fraudulently. Please refer to CARD ACCEPTANCE SECURITY on pages 9-16.*

## COMMERCIAL CARDS

*Commercial Cards are issued by MasterCard®, Visa®, Discover® and American Express®. They are also known as Business Cards, Corporate Cards, and Purchasing Cards.*

As more and more government agencies and companies discover the benefits of using Commercial Cards, (reduced paperwork and eliminating the relatively high cost of purchasing small dollar items), they are seeking suppliers that accept these Cards as forms of payment. If you already accept Cards today, you can accept Commercial Cards as well.

Typically, companies using Commercial Cards want more information about the Transaction than is available in a consumer Card Transaction. This information is used by government agencies and businesses to assist them in cost allocation, tax compliance, and vendor spending analysis.

To meet the needs of the Card users, MasterCard, Visa, and Discover have created three levels of information beyond a standard Card Transaction, which can help reduce additional interchange fees assessed on Commercial Card Transactions. For American Express Purchasing Card Level 2 qualification, the Customer Reference Number, Tax Amount, and Shipping Information including Destination Zip Code must be submitted by the merchant. Only certain Devices are capable of capturing and transmitting the additional information. For more information, please call an **M&T Bank Merchant Services Specialist at: 1-800-724-7031 from 8am to 5pm (ET).**

## RETURNS AND REFUNDS

You are the expert in your business. You have established return and refund policies necessary to run your business efficiently and to best serve your customers' needs. The Card Associations require that your return and refund policies are clearly disclosed to Cardholders and included on the sales slip. Disclosures can help you avoid costly misunderstandings and potential customer disputes.

To ensure your return, exchange, or refund policies are clearly disclosed to Cardholders, you may use any of the language suggested below that best represents your policies.

- "NO REFUND"
- "EXCHANGE ONLY"
- "IN-STORE CREDIT ONLY"
- "SPECIAL CIRCUMSTANCES"

For Card-Not-Present Return Policies, please refer to your Merchant Services Agreement regarding your obligations to disclose your policy.

If you and the Cardholder agreed to special terms (i.e. late delivery, delivery charges, insurance charges, etc.) or restrictions on returns, you should write the agreed upon terms on the sales slip. The Cardholder's signature on the sales slip is a good indication that they agreed to the special terms.

## VOIDS

From time-to-time, you may need to void a transaction. A void can only be performed in a batch that has not been settled. An example of when a void would be needed is an incorrect transaction amount. Instead of entering $100.00, the clerk enters the transaction as $1,000.00. If the batch has not been settled, a void can be performed to remove the $1,000.00 entry from the batch. The correct amount can then be re-entered.

***Caution:*** *A void will only remove the incorrect transaction from the batch. A void will not remove the authorization hold from a cardholder account. If you need to release the authorization hold, please call an M&T Bank Merchant Services Specialist at: 1-888-536-7000 from 8am to 5pm (ET). We will provide you with the card-issuing bank's telephone number to release the hold. You will need to supply the date of the hold, amount, and your merchant number so have it handy when you call.*

# CARD ACCEPTANCE TIPS

1. Display the appropriate MasterCard, Visa, Discover, and American Express Card decals to let Cardholders know that you accept these types of Transactions. Businesses are required to do so.
2. Ensure that your point-of-sale staff is informed of the proper procedures and review this Guide periodically.
3. Ensure your customer receipts are masked (only show last 4 digits) and that the expiration date of the card is not printing on customer receipts.
4. Request an Authorization for EVERY Card Transaction. If you fail to get a valid authorization code, you may be assessed a penalty fee by the card associations.
5. Use the AVS and CAV2/CVV/CVV2/CID for EVERY Card-Not-Present Transaction.
6. Submit AVS and CAV2/CVV/CVV2/CID and AVS for recurring billing or installment purchases.
7. Insert, swipe, or obtain a manual imprint whenever the Card is present. If the card cannot be inserted or swiped, manually key enter the Card account number.
8. For those transactions not authorized by a PIN entry, collect a Cardholder signature and compare it to the signature on the back of the card for EVERY Card-Present Transaction.
9. Retain original or legible copies of sales slips for at least three years.
10. Identify suspicious behavior and take the necessary precautions, such as ordering a "Code 10" Authorization. Please see Code 10 on page 3.
11. Do not enter the same Transaction more than once. Know the proper procedures for canceling or voiding Transactions.
12. Do not ship merchandise to an address other than the Cardholder's billing address. If a Card-Not-Present or Internet Transaction, request a delivery signature or other identification if you are not shipping to the same billing address. This practice may not protect you from certain types of chargebacks for authorized purchases even with a valid AVS response. It is your responsibility to know your customer.
13. As of the time of this publication, your business may set a minimum Transaction amount to accept a credit Card, as long as the minimum Transaction amount does not exceed $10 (or any higher amount established by the Federal Reserve Board by regulation) and does not differentiate between Card issuers or between Card networks. Your business may impose a maximum on credit card transactions if you are a federal agency or institution of higher education. Your business **may not** impose a minimum or maximum on a debit or prepaid Card.
14. As of January 2013, MasterCard, Visa, Discover and American Express began allowing surcharges on certain credit and Commercial Card Transactions. For more information on whether you may assess a surcharge:
    - MasterCard®
      https://www.mastercard.us/en-us/merchants/get-support/merchant-surcharge-rules.html
    - Visa®
      https://usa.visa.com/support/small-business/regulations-fees.html#2
    - Discover®
      https://www.discoversurcharge.com/
    - American Express®
      http://about.americanexpress.com/news/pr/2013/amex-agrees-to-settle-class-action.aspx
15. Regardless of whether the Card Associations permit surcharging, some states have laws that prohibit surcharging. Before assessing a surcharge on any Transaction, be sure to check whether the state in which you do business permits surcharging.
16. Collection of Service Fees or Convenience Fees is allowable with certain restrictions. Please call an **M&T Bank Merchant Services Specialist at: 1-800-724-7031 from 8am to 5pm (ET)** to determine if your business type is eligible; or you may review qualification criteria on the card association websites.
17. Do not process the prohibited transactions as outlined in Prohibited Transactions section. Doing so may result in termination, requirement of a reserve account or funding holds in accordance with your Merchant Agreement.
18. If you do not feel comfortable accepting the Transaction, you can ask for another form of payment.

# PROHIBITED TRANSACTIONS

A prohibited Transaction is one that is not in compliance with the Rules. Businesses that accept Cards should be aware of the types of Transactions that are prohibited and the penalties that can be imposed if a prohibited Transaction is completed. Below are some of the more common prohibited Transactions. For a complete list please visit the Association websites.

***Note:*** *If deposited, sale slips involving prohibited Transactions will be subject to chargeback and may lead to termination of your Merchant Services Agreement.*

## YOU ARE PROHIBITED FROM PROCESSING (FOR A COMPLETE LIST VISIT EACH ASSOCIATION WEBSITE):

- Cash advances to your business, yourself or your employees
- Transactions to cover previously incurred debts, such as bounced checks or payment for returned merchandise not purchased with a Card
- Pre-authorized Transactions for goods or services after you receive notice of cancellation by the Cardholder
- Transactions declined by the Authorization Center
- Transactions using a Card with an invalid effective date or expired date
- Transactions where the signature on the Card and the sales slip are not the same
- Transactions that separate taxes from the purchase amount
- Knowingly making cash refunds to Cardholders for any returned merchandise or canceled service originally purchased with a Card. Your sales staff should complete a credit slip for adjustments
- Taxes paid separately via cash. Include taxes in the original Transaction amount

## YOU ARE PROHIBITED FROM ENGAGING:

In factoring (laundering) or depositing sales slips from other businesses, which you may own or purchase, but are not explicitly listed in your current Merchant Services Application on file with us. Be wary of the "fellow business person" who offers to pay you a fee or commission to deposit their MasterCard, Visa, Discover Network or American Express sales slips in your account or third-party intermediaries who offer payment plans to cardholders for merchandise or services purchased at your place business. Ask yourself, "Why can't this business or business person get an agreement on their own?" These transactions are often questionable or even fraudulent.

## ADDITIONALLY, YOU ARE PROHIBITED FROM THE FOLLOWING:

- Minimum transaction dollar amounts on debit card Transactions, as a condition for honoring a Card. Cardholders are permitted to use their debit Cards for any dollar amount
- Maximum transaction dollar amounts, as a condition for honoring a Card
- Resubmitting a Sale on a previously charged back Transaction
- Sales deposited at another financial institution before or after you deposit it with M&T Bank
- Transactions into multiple Transactions to avoid Authorization requirements

# CARD ACCEPTANCE SECURITY

You should be aware of the basic elements and security features of MasterCard®, Visa®, Discover® and American Express® Cards. These elements and features can help your staff avoid inadvertently accepting a counterfeit Card or processing a fraudulent transaction. Consider the following:

## SIGNS OF POSSIBLE CARDHOLDER FRAUD:

- First time shopper
- Larger than normal orders
- Orders consisting of several of the same item
- Orders made up of "big" ticket items
- Orders shipped "rush" or "overnight"
- Orders shipped to an international address
- Transactions with similar account numbers
- Shipping to a single address when Transactions take place on multiple Cards
- Multiple transactions on one Card over a short period of time

Be alert for Transactions with several of these characteristics. Keep in mind that a Transaction with one of these characteristics does not mean you are being scammed, but a few or several of them together might. Remember, never ship an order unless you receive a valid Authorization.

In addition, taking the time to look at the Card is critical. Encourage your sales staff to **STOP** at the beginning of the Transaction, **LOOK** at the Card, and **LISTEN** for any warning signals from the Cardholder that might indicate a suspicious Transaction. Do not be hesitant to ask for a different form of payment or call for a Code 10 Authorization.

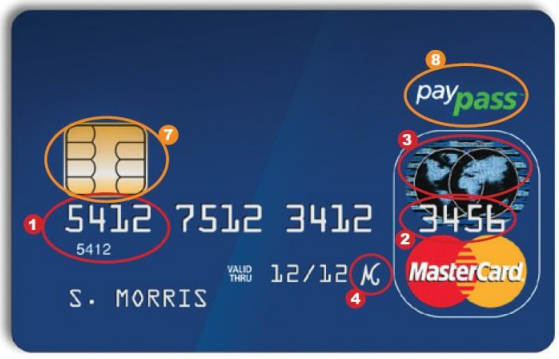
# SECURITY FEATURES TO REVIEW AT THE POINT-OF-SALE BY CARD BRAND

The basic elements and security features of MasterCard, Visa, Discover and American Express Cards are as follows:

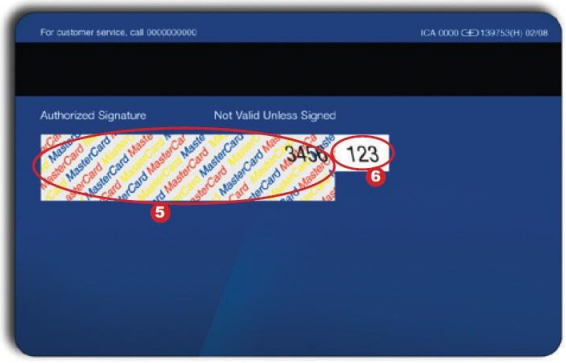
## Use these tips for verifying Traditional MasterCard® Cards:

### MasterCard Card Security Features and Optional Card Features

Card Front




Card Back




1. The first 4 digits of the account number must match the 4 digit preprinted BIN. Remember, all MasterCard account numbers start with the number 5 or 2.
2. The last 4 digits of the account number must match the 4 digits that appear on the Cardholder receipt.
3. The global hologram is three dimensional with a repeat "MasterCard" printed in the background. When rotated, the hologram will reflect light and appear to move.
4. The stylized "MC" security feature has been discontinued, but may continue to appear on cards through June 01, 2010.
5. The signature panel is tamper evident with the word "MasterCard" printed in multiple colors at a 45º angle. For magnetic swiped transactions, remember to compare the signature on the back of the card with the Cardholder's signature on the receipt.
6. The 4 digits printed on the signature panel must match the last 4 digits of the account number, followed by the 3 digit indent printed CVC2 number.

**Optional Card Feature (see Card Front).**

7. A Chip may be present on the Card. The Cardholder may be prompted to enter a unique personal identification number or PIN when the card is inserted into a chip capable payment terminal.
8. PayPass® contactless payment technology may be present on card. A signature is not required for PayPass® "tapped" transactions below a specified limit.

**If you are ever suspicious about the validity of a MasterCard card, call your Voice Authorization Center and request a Code 10.**

## Use these tips for verifying Alternative Design MasterCard® Cards:

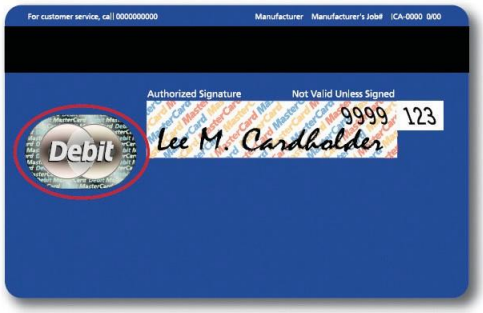
### Alternative MasterCard Card Features and Designs

**Alternative Card Front**


Card design and MasterCard Brand Mark may be oriented vertically.

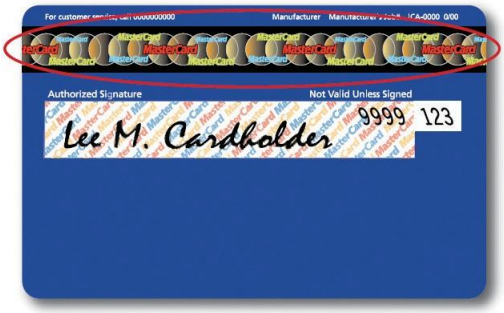
**Alternative Card Back**


Global hologram on the back of a chip card design. The signature panel has been shortened to accommodate the chip.




Debit Hologram on the back of a magnetic stripe card design.

**Note:** In some countries, it is a mandatory for Debit MasterCard cards to bear the Debit Hologram.




Holographic magnetic tape may be used in lieu of the hologram or in conjunction with the hologram. A longer signature panel is used on traditional magnetic stripe cards.

**If you are ever suspicious about the validity of a MasterCard card, call your Voice Authorization Center and request a Code 10.**

## Use these tips for verifying Traditional Visa® Cards:

### Visa Brand Mark Card Security Features

Every Visa card contains a set of unique design features and security elements developed by Visa to help merchants verify a card's legitimacy. By knowing what to look for on a Visa card, your sales associates can avoid inadvertently accepting a counterfeit card or processing a fraudulent transaction.

Train your sales staff to take a few seconds to look at the card's basic features and security elements after they swipe, insert, or wave the card and are waiting for authorization. Checking card features and security elements helps to ensure that the card is valid and has not been altered in any way.

## What to Look For On All Visa Cards

### Visa Brand Mark Card Security Features


Embossed/Unembossed or Printed Account Number on valid cards begins with "4." All digits must be even, straight, and the same size.

Chip may appear on the card front

Dove Hologram may appear on the front or back of the card

Visa Brand mark may be placed in the upper left, upper right, or lower right corner of the card

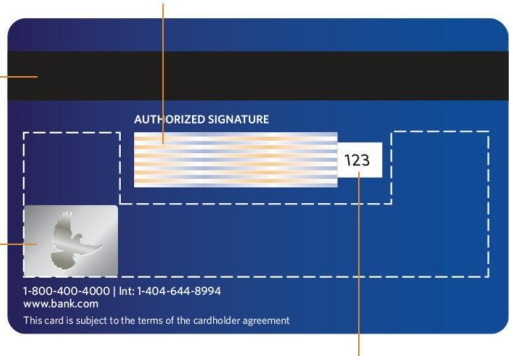
Ultraviolet V is viable over the Visa logo when the card is placed under an ultraviolet light

Four to Six Digit Bank Identification Number (BIN) must be printed directly below the account number and must match exactly with the first four digits of the account number

Expiration or "Good Thru" dates should appear below the account number

The Signature Panel must appear on the back of the card and be signed

Magnetic Stripe is encoded with the card's identifying information




The Mini-Dove Design Hologram may appear on the back anywhere within the outlined areas shown here. The three-dimensional dove hologram should appear to move as you tilt the card.

The Mini-Dove Design Hologram may appear on the back anywhere within the outlined areas shown here. The three-dimensional dove hologram should appear to move as you tilt the card.

Card Verification Value (CVV)* is a unique three-digit code on the magnetic-stripe of all valid cards

* In certain markets, CVV2 is required to be present for all card-absent transactions. Also, U.S. merchants who work in the face-to-face sales environment may include (CVV2) in the authorization request for U.S. domestic key-entered transactions in lieu of taking a manual card imprint.

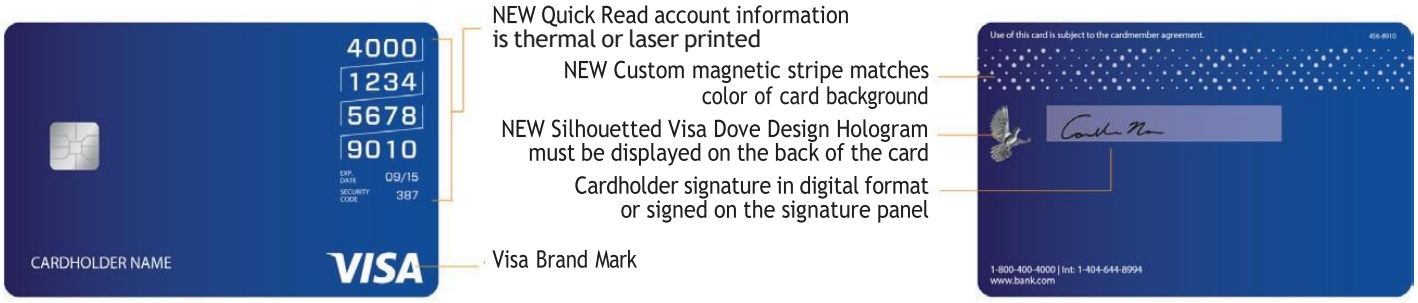
Card Acceptance Guidelines for Visa Merchants

## Use these tips for verifying Alternative Design Visa® Cards:

### Visa Brand Mark Card Security Features

**Unembossed Visa Card Acceptance**

The unembossed Visa card (e.g., prepaid card) may look and feel different, but it is a valid card that can be accepted at any Visa merchant location that has an electronic terminal. Unlike an embossed Visa card with raised numbers, letters, and symbols, the unembossed card has a smooth, flat surface. From a merchant perspective, the processing of an unembossed card at the point-of-sale should be seamless. There's no need for new software, special hardware, or modified terminal procedures. You simply swipe, insert, or wave the unembossed card just as you would an embossed card, then wait for an authorization and obtain the cardholder's signature. Because of the unembossed card's flat surface, it cannot be used for transactions that require a manual card imprint. A merchant should not attempt to hand-write receipts or key-enter the account number for unembossed cards.




### Visa Mini Card


A Visa Mini Card is a miniature version of a standard size Visa Card.

### Visa Vertical Card


This card has a vertical orientation and account information is laser printed on the card, not embossed. It includes a magnetic-stripe just like its embossed counterpart, and a card verification code on the back.

## When Something Doesn't Look Right

If any of the Visa card security features are missing or look altered, adhere to your merchant store procedures and respond accordingly.

## Use these tips for verifying Discover® Cards:

### Discover Card Identification Features


Many cards display a three-dimensional holomagnetic stripe which, when tilted, shifts color and appears to move.

### Standard Security Features Common to Discover Cards

- "DISCOVER" or "DISCOVER NETWORK" will appear under an ultraviolet light
- All Discover card numbers start with "6." Embossed card numbers should be uniform in size and spacing. Unembossed cards may display the card number and expiration date printed flat on the front
- "Valid Thru" indicates the last month in which the Card is valid
- A business name may be embossed below the Cardholder name
- Embossed security character appears as a stylized "D." No stylized "D" appears on unembossed cards
- Many cards display a three-dimensional holographic magnetic stripe which, when tilted, shifts color and appears to move
- Some cards display a three-dimensional hologram on the card front with a globe pierced by an arrow
- "DISCOVER" or "DISCOVER NETWORK" appears on a tamper-evident signature panel. Some cards contain an ultraviolet image that repeats the word "DISCOVER" in the signature panel
- Embossed cards display the last four digits of the Card number on the signature panel in reverse-indent printing
- A three-digit CID (Card Identification Data) is printed in a separate box to the right of the signature panel on the card back. You may choose to verify the CID during any authorization request for keyed or swiped transactions
- The Discover Acceptance Mark will appear on the front AND/OR back of the Card
- Chip may appear on the Card front

## Use these tips for verifying American Express® Cards:

### American Express Cards Security Features

1. All American Express account numbers are embossed and start with “37” or “34”.
2. Check account numbers are embossed (15 digits) with no alterations and spaced in 4, 6 and 5 digits.
3. Check 4 digit Card Identification Number (CID) is printed above embossed account number on right or left of card and cannot be scratched off.
4. Compare name embossed with presenter. Cards are not transferable.
5. Check member since date is embossed and compare age of presenter.
6. Check expiry date is embossed and card is valid.
7. Check clarity of Centurion similar to U.S. currency. Phosphorescence of Centurion portrait and words “AMEX” visible under UV light.
8. Some cards have a hologram of the American Express image embedded Into the magnetic stripe.
9. Check printed account number matches embossed number on front of card and sales receipt.
10. Compare signature with the sales receipt. If card presented is unsigned, request for photo ID with signature and request customer to sign card and sales receipt while you hold the ID.

## MORE SIGNS OF POSSIBLE CARDHOLDER FRAUD

- The signature on the sales slip does not reasonably compare with the signature on the back of the Card
- If the Card is not signed, ask the Cardholder for valid government-issued identification
- There are signs of erasure on the signature panel of the Card
- Fraud typically occurs within hours of the loss or theft of a Card. This is before most victims have called to report the loss. Checking the signature becomes very important in these first few hours of loss. Also keep in mind that the thief may have altered the signature panel
- The Card account number does not match the printed Card account number on the Transaction receipt/sales slip. This may indicate an altered magnetic stripe

If your sales staff knows a Card is invalid, they should not accept it. If they suspect a Card has been altered or is counterfeit, they should call the following Authorization Center and request a "Code 10" Authorization:

### MASTERCARD, VISA, DISCOVER AND AMERICAN EXPRESS: 1-800-228-1122

The Authorization Operator will ask you a series of "Yes" or "No" questions to prevent arousing the customer's suspicion. If the identity of the customer as the Cardholder can be verified, you will receive a valid Authorization number, which then must be manually keyed into the Device.
If the identity of the customer cannot be verified, the Authorization Operator will instruct you to keep or return the Card. You should only keep the Card if you can do so by peaceful means. If the Cardholder becomes threatening in any way, your staff should give back the Card. Your safety comes first!

## EUROPAY, MASTERCARD, VISA ("EMV") CHIP CARDS AND CONTACTLESS CARD PAYMENTS

As of **October 1, 2015**, merchants may be liable for card-present fraud if they are presented with a chip card and cannot read the chip data based on their point-of-sale technology. Although not a mandatory initiative, merchants are urged to use upgraded terminals or software to solutions that can support chip technology to avoid receiving disputes with no rebuttal rights. M&T Bank is not liable for merchant's failure to upgrade devices.


Chip technology is an evolution in our payment system that is meant to help increase security, reduce fraud and enable the use of future value-added applications. Chip cards are standard bank cards that are embedded with a micro computer chip. Some will require a PIN instead of a signature to complete the transaction process.

Point-of-sale software applications are currently available which to support this chip card technology as well as contactless payments. Look for more information at:

- MasterCard®
  https://www.mastercard.us/en-us/merchants/safety-security/emv-chip.html
- Visa®
  https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/index.jsp
- Discover®
  https://www.discovernetwork.com/en-us/business-resources/chip-cards-emv/business-owners
- American Express®
  https://network.americanexpress.com/globalnetwork/products-and-services/security/emv-chip-card-payments/

# RETRIEVAL AND DISPUTE REQUESTS

A retrieval or dispute request, which are both initiated by a Cardholder, is essentially a communication sent back and forth between a Cardholder's issuing bank and M&T Bank, when a Cardholder questions a Transaction. Retrieval and dispute requests are usually initiated because a Cardholder does not recognize your business name, there is incomplete information on a Cardholder statement, the Cardholder suspects fraud, or the Cardholder is dissatisfied with their purchase. It is important for you to understand: **WHAT** they are, **WHY** they occur, and **WHAT** to do when you receive one.

## RETRIEVAL REQUESTS ("12 B LETTERS")

A retrieval request is simply a Cardholder requesting more information from the business regarding a Transaction in question. It is not a reversal of transaction. It typically occurs because a Cardholder does not recognize your legal business name on a statement. You typically have a limited number of days from receipt of the request to deliver to your acquiring bank a copy of the sales slip and any other documentation pertinent to the Transaction. Your acquiring bank then delivers your response to the Cardholder's issuing bank for review with the Cardholder. Often times, the initial question is resolved by this means.

## DISPUTE REQUESTS

Unlike retrieval requests, a dispute is an actual reversal of the Transaction. This means that the dollar amount of the original Transaction is debited from your Merchant Deposit Account. The debit may or may not be reversed depending on the documentation pertinent to the Transaction that you provide to us. You have a limited number of days from receipt of the request to respond to your acquiring bank. You may be able to "remedy" a dispute by providing additional information about the Transaction in question.

Disputes are often generated as a result of an issue arising about a particular Transaction because:

- A Transaction is fraudulent
- A credit has not been processed when the Cardholder expected
- A Transaction was processed more than once
- A Transaction was processed without an Authorization code
- An incorrect Card account number was key-entered into the Device
- The merchandise ordered was never received
- The service was not performed as expected

It is possible that Associations may assess fines to merchants who exceed their established thresholds of dispute volume. If such a fine is levied, you will be responsible for payment.

Please contact **M&T Bank Merchant Service Team at 1-800-724-7031** regarding any retrieval or dispute issues. Also feel free to fax retrieval or dispute responses directly to M&T Bank within the allotted time frame to expedite the dispute process at **1-866-419-8335 to avoid losing rebuttal rights**. Be sure to fax the request with the documentation as well.

## MINIMIZE RETRIEVAL AND DISPUTE EXPOSURE

You can be your own best defense against most retrieval or dispute request situations. Although you cannot avoid retrievals or disputes completely, you have considerable control. The more you know about proper procedures, the less likely you will be to inadvertently do or fail to do something that might result in a dispute. Below are steps you can take to minimize the reoccurrence of retrieval and dispute requests.

- Do not complete a Transaction if the Authorization request was declined
- Do not repeat the Authorization request after receiving a decline
- Insert, swipe, or wave (if contactless payment) the Card through the Device every time if you are a Card-Present business
- If your Device is not working, make an imprint of the front of the Card using the manual imprinter. Key-enter the Card account information if you are a Card-Present business. If the sales slip does not have an imprint of the front of the Card even though the Transaction is Authorized and the Cardholder signs the sales slip, it may be returned for "no imprint" if the Cardholder denies participating in the Transaction

- Obtain the Cardholder's signature on the sales slip for every Card-Present Transaction which is not accompanied by a PIN entry
- Compare the Cardholder's signature on the sales slip to the signature on the back of the Card before returning the Card to the Cardholder. The signature should appear to be the same and the names should be spelled the same. Signatures that are clearly not the same may be indicators of potential fraud
- Ensure that the Transaction information on the sales slip is complete, accurate, and legible before completing the Transaction. An illegible original or copy of the sales slip may be returned
- Disclose your return or refund policy clearly to the Cardholder at the time of the Transaction. Your policy should be printed on your sales slips near the Cardholder signature line; if not, write or stamp your policy on the sales slip
- Ensure that Transactions are settled only once
- Settle Transactions the same day as Authorized
- Process the Transaction when the merchandise is shipped or services performed
- Verify the billing address of the Cardholder
- Obtain a document signed by Cardholder authorizing you to process the Transaction on a specific date, if the service will be provided over time
- Respond to the request immediately by sending a sales slip and any documentation pertinent to the Transaction to your acquiring bank, within the specified time frame
- Keep copies of sales slips and pertinent documentation for at least thirty six months (3 years), in a safe and secure place, so you can respond to requests quickly

## CARDHOLDER PRIVACY

The Card Association Rules and applicable federal and state law prohibit listing the Cardholder's personal information on the Card sales slip. You can expose your customers to unnecessary danger or fraud by listing personal information about a Cardholder on a sales slip, such as: phone number, driver's license or social security number. In fact, you are prohibited from refusing to complete an otherwise valid Transaction just because a Cardholder refuses to provide personal information.

However, you may obtain personal information if you need it to complete the Transaction because:

- You need the address and telephone number to deliver merchandise for a Card-Not-Present Transaction
- The Authorization operator specifically requests additional information for the Card issuer record

If you do obtain additional personal information, you may not write it on the sales slip.

Unless you obtain the expressed written consent of the Cardholder, you cannot sell, purchase, provide, or exchange Card account numbers in the form of imprinted sales slips, carbon copies of imprinted sales slips, mailing lists, tapes or any other media or communication obtained by reason of a Card sale, to any third party other than to your agents for the purpose of assisting you in your business, to M&T Bank and the appropriate Card Association for any Card, or in response to a government request or otherwise specifically permitted by law.

All systems and media containing Card account numbers, Cardholder Information, and Transaction information (physical or electronic, including but not limited to Card account numbers, imprints, and terminal ids) must be stored in an area in a secure manner to prevent access by or disclosure to anyone other than the business' authorized personnel, M&T Bank, or its designated sub-contractors until destroyed. It must be destroyed in a manner that will render the data unreadable.

If unauthorized individuals can access Card account numbers electronically, the data must be stored in an encrypted form behind a secure "firewall." If data is compromised, you must provide M&T Bank with complete information about the Card account number compromise, including the contributing circumstances and may be required to employ a data security firm selected by the Card Associations to assess the vulnerability of your systems.

# PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)

There is a fast growing, worldwide problem involving data theft. As such, it is of paramount importance to protect sensitive Cardholder Information. At M&T Bank, we understand the importance of data security and want to help protect your business from suffering a data security breach involving Cardholder Information. All merchants must be PCI Compliant regardless of who their merchant services provider is. For M&T Merchants, it's a requirement of your Merchant Agreement.

## WHAT IS THE PCI-DSS?

The PCI-DSS represents a common set of industry tools and measurements to help ensure the safe handling of sensitive Cardholder Information. The standard provides an actionable framework for developing a data security process – including helping to prevent, detect, and react to security incidents.

## WHAT ARE THE BASIC 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

## WHAT TYPES OF BUSINESS NEED TO COMPLY WITH THE PCI-DSS?

The PCI-DSS requires all businesses that store, process, or transmit Cardholder Information are required to comply with the standard. That is, all businesses that accept Cards must comply, even those using dial-up terminals to process Cards, to reduce the risk of a compromise and mitigate its impacts, if it does occur.

## WHAT ARE THE BENEFITS OF COMPLYING WITH THE PCI-DSS?

- Increased protection for you Cardholders' Personal Information
- Enhanced Cardholder confidence through improved data security
- Reduced risk of non-compliance fines imposed by MasterCard®, Visa®, Discover®, and American Express®

## WHAT DOES MY BUSINESS NEED TO DO TO COMPLY WITH THE PCI-DSS?

The PCI-DSS requires businesses to validate compliance by annually completing a self-assessment questionnaire and network scan, if applicable, with a verified Qualified Security Assessor ("QSA").

M&T Bank wants to help you achieve PCI-DSS compliance at a reasonable expense and with expert guidance. Working with SecurityMetrics, a PCI Council approved Qualified Security Assessor, our merchants are enrolled in our PCI program, which affords your business a $100,000 liability waiver in the event of a security breach as well as tools for registering your business as a PCI Compliant merchant. To learn more about PCI Compliance, visit the PCI Data Security Council at www.PCISecurityStandards.com or SecurityMetrics at www.SecurityMetrics.com.

Your attention to Cardholder data security is more important

than ever and we appreciate your time and assistance. Please act as soon as possible to protect both your business and your Cardholders!

# IMPORTANT TELEPHONE NUMBERS

| M&T BANK | Phone Numbers |
|---|---|
| **Merchant Service Team** | **1-800-724-7031** |
| Chargeback Department | 1-800-724-7031 |
| Chargeback Department Fax | 1-800-724-7031 |
| **Terminal Help Desks** | |
| TSYS | 1-800-552-8227 |
| **Other Help Desks** | |
| e-Processing Network | 1-800-971-0997 |
| SIGIS (Pharmacy & Medical Professional Registration) | 1-925-855-3228 |
| PCI - SecurityMetrics | 1-801-705-5700 |
| **Supplies** | |
| POS Portal | 1-800-264-1105 |
| **Card Associations** | |
| American Express (if not OptBlue) | 1-800-528-5200 |
| Discover Network (if receiving statement from Discover directly) | 1-800-347-2000 |
| **Authorizations** | |
| Voice Authorization or Code 10 Authorization Requests | 1-888-602-0323 |

RETURN TO MAIN MENU

M&T Bank