



M&T COMMERCIAL CARD

BEST PRACTICES TO HELP MITIGATE COMMERCIAL CARD FRAUD

M&T Bank understands how important it is to help protect cardholders from fraudulent activity on their cards, as well as employee misuse.

M&T Bank

BEST PRACTICES TO HELP MITIGATE COMMERCIAL CARD FRAUD

This document describes some of the most common types of unauthorized card use, the tools M&T makes available to assist in detecting unauthorized use, some of the industry's proactive best practices to help protect your organization from fraudulent transactions, and where to call if fraud does happen.

WHAT IS UNAUTHORIZED USE?

There are two basic types of unauthorized use:

- **Employee Misuse** – unauthorized use by the cardholder which is outside of the company's spend policy or doesn't benefit the company. In the event of cardholder misuse, the Visa® Liability Waiver Program provides M&T Commercial Card clients with up to \$100,000 coverage, provided certain criteria are met¹
- **Fraudulent Activity** – unauthorized use of the card account by someone who is not the cardholder. Common fraudulent transactions usually occur as a result of the following:
 - **Lost / Stolen Cards** – card plastic is lost by a cardholder or stolen from them and used to make unauthorized purchases before the cardholder can duly report the card missing and have it closed
 - **Unauthorized Internet Transactions** – card account and expiration date information is stolen and used by criminals to make unauthorized purchases in a card-not-present environment
 - **Counterfeit** – card account and magnetic stripe information is stolen and used to create a duplicate plastic for fraudulent card present use

MEASURES TO DETECT FRAUD

M&T takes cardholder fraud very seriously, implementing multiple measures to monitor transactions for its clients and cardholders. These measures aim at either preventing certain transactions at the point of sale or by flagging suspect transactions that are outside learned fraud behavior for follow-up with the cardholder.

M&T Bank offers every Commercial Card customer both the Card Guard Fraud Detection Service as well as Visa® Advanced Authorization scoring. These fraud detection systems use neural network technology in conjunction with spending history and other factors to isolate fraudulent activity. Suspicious transactions are scored, prioritized, and analyzed, and the M&T Financial Crimes unit places calls to Program Administrators and Cardholders.

Additionally, there are a number of controls that companies can institute themselves through the Card Management tool, CentreSuite, to help prevent fraudulent use of their cards.

M&T Bank now issues all Commercial Cards as EMV Chip and PIN cards. EMV Chip cards use dynamic data on each transaction which renders stolen card information virtually useless for creating counterfeit cards. Your customized PIN adds to the security of your card.

Enjoy worldwide acceptance and enhanced security with chip technology on all M&T Commercial Cards. Visit www.mtb.com/commercialchip for more information.

¹ The Visa® Liability Waiver Program is offered by Visa® USA, Inc. subject to all the terms and conditions described in the Visa® document. Please refer to such document for full details, conditions and restrictions.

BEST PRACTICES FOR FRAUD PREVENTION

Fraud prevention is an ongoing battle in the payments world. While fraud will likely never be completely eliminated, the following are some “best practices” that organizations can employ to help reduce the window of opportunity for fraud.

1. ESTABLISH A COMPANY POLICY

- A Company card spend policy should be developed and distributed to cardholders, which clearly outlines the types of acceptable and prohibited purchases
- Companies should instruct employees on proper storage and safeguarding of card and account numbers and what to do if their card is lost or stolen
- Provide each cardholder with a Cardholder Agreement (require signature and keep original) outlining acceptable card uses
- Visa® Liability Waiver – become familiar with the requirements for claims under this program

2. PHYSICALLY CONTROL CARDS

- Determine which employees require a card. Limit the window of opportunity for unauthorized use by only providing cards to employees who need a card. Don't simply give a card to everyone in the company if only certain employees need them
- One User per Card – do not share use of a card or card information with others
- When a User leaves the company – immediately close the card issued to that employee; do not pass it on to another employee
- Limit physical access to cards prior to distributing them to employees

3. CREDIT LIMITS ON THE CARD

- Keep credit limits on individual cards as low as appropriate to allow required transactions to be conducted, but to prevent large dollar fraudulent usage
- Know which cardholders require larger limits and keep lower limits on all other cardholders
- Adjust credit limits in real-time through CentreSuite

4. MERCHANT CATEGORY CODE (MCC) RESTRICTIONS

- MCC restrictions are a critical tool to prevent transactions at known risky business types
- Set MCC restrictions to limit card use to acceptable, business-related industries
- Block transactions at any known MCC's that would never be used
- Adjust MCC restrictions in real-time through CentreSuite

5. VELOCITY LIMITS

- M&T's Commercial Card products have the ability to set velocity limits around daily, cycle, monthly, quarterly, and yearly authorizations and dollar amounts allowed on a card
- Single Purchase Amount Limits can be enabled to prevent large dollar fraudulent transactions
- Many velocity restrictions can be adjusted in real-time through CentreSuite

6. RESTRICT TRANSACTIONS TO US ONLY

- Restrictions should be considered for most cards to allow domestic (US) transactions only
- Allow international transactions for only those who travel or purchase internationally

7. DO NOT ALLOW CASH ACCESS ON YOUR CARDS UNLESS NECESSARY (IF APPLICABLE)

8. IMMEDIATELY REPORT LOSS OR THEFT OF CARD

- Immediately contact M&T's Commercial Card Service Team at **1-800-443-8671** to report the card lost or stolen. In addition, please contact your Program Administrator after reporting the incident to the Bank
- To dispute any suspicious transactions, **you must call M&T at 1-800-443-8671**

9. REVIEW STATEMENTS

- Cardholders and Program Administrators should actively and timely review their statements to identify suspicious card activity
- If printed, hard-copy statements should be stored securely to prevent card number exposure

10. MONITOR TRANSACTION ACTIVITY THROUGH REPORTING TOOLS

- Program Administrators should monitor transaction activity within CentreSuite through the following:

Transaction Reports

Authorizations/Declines

Program Change Requests (Audit of CentreSuite access)

Unassigned Transaction Reports



TOOLS TO HELP

M&T can provide the following:

- Sample Policies and Procedures
- Sample Cardholder Agreement
- Visa® Liability Waiver Outline and Brochure
- Merchant Category Code Lists

WHAT TO DO IF YOU SUFFER FRAUD OR SUSPECT FRAUD

- Immediately contact M&T's Commercial Card Service Team at **1-800-443-8671** to report the card lost or stolen, or if you become aware of suspicious activity on your card account. In addition, please contact your Program Administrator after reporting the incident to the bank
- To dispute any transactions, **you must call M&T at 1-800-443-8671**

DISPUTE PROCESS

M&T is committed to researching and resolving issues as quickly as possible and processes card transaction disputes within established Visa® procedures. Below please find some helpful tips on disputing a transaction:²

- Based on the present Visa® procedures for disputing transactions, all charges must be disputed within 60 days of receipt of the paper or electronic version of your billing statement
- Disputed items are not removed from your statement and are still due and payable upon receipt of your monthly invoice
- Your organization or your organization's cardholder must contact the M&T Commercial Card Service Team at 1-800-443-8671 to close and reissue the card and identify the transactions that need to be disputed

² The information is correct as of July 2016. For the most up to date information on dispute procedures, please read the Visa® rules on disputing transactions at www.visa.com.

- If you are contacted by the M&T fraud monitoring team and the suspicious transactions are deemed fraudulent, the card is typically closed and reissued at that time. When contacting the Commercial Card Service Team, you will only need to initiate the dispute
- Authorizations that appear fraudulent cannot be disputed until they are posted as transactions on the card account. We encourage you to monitor the authorizations in question and contact M&T when they post so that they can be disputed as well
- In certain instances, M&T may send a Dispute Letter to you to complete, sign, and return, as instructed on the form
 - If you receive a Dispute Letter, it must be signed by you and your Program Administrator, and it must be returned to the indicated address at the Bank within 10 business days. If the form is not received on time, the claim will be closed
- Once all information is received (including the signed Dispute Letter, if necessary), the dispute process begins
- The length of time to complete the process varies and may take up to 120 days to complete. In rare instances, the process can take up to 6 months
- Your Program Administrator will be notified upon resolution of the dispute in writing



To learn more, contact your local
M&T Bank Relationship Manager or visit
www.mtb.com/corporate.