Fraud Prevention Guide

TD Merchant Solutions Terminals

Table of Contents

How Secure is Your Business?

No matter what type of business you're in, the risk of fraud is present and always evolving.

Fraud facts

- Weaknesses in internal controls are responsible for nearly half of all employee thefts/frauds[1].
- Over 80% of businesses reported being targets of payment fraud in 2018[2].
- While cheques remain the most frequent source of payment fraud, Business Email Compromise (BEC) scams are on the rise. The percentage of organizations being targeted by such scams has increased from 64% in 2014 to 80% in 2018[2].

Stay vigilant and guard your information!

Do not share your confidential login credentials with anyone. TD Bank will never ask you to provide personal information or login information such as Connect IDs, passwords, authentication token codes or account numbers either by phone or by email.

Employee training

Your first line of defense is your employees. Ensure that you train them to recognize suspicious behaviour or transactions. Immediately report any suspicious activity to TD Merchant Solutions at **1-800-363-1163**.

Suspicious behaviour

There are a number of common Fraudster behaviours that you need to be aware of:

- the number of times that they enter their PIN number incorrectly,
- if they insert their chip card incorrectly so that the device requests you to swipe their card,
- they appear nervous,
- they select products to buy randomly, and/or
- they want to purchase a single large, expensive item.

Please note that the above is not an exhaustive list. Your vigilance and awareness of when something is not right are also strong fraud prevention tools.

1 2018 Report to the Nations. Association of Certified Fraud Examiners.

2 2019 AFP Payments Fraud and Control Survey, Association for Financial Professionals.

Terminal Security

You are responsible for the security of your terminal. **We strongly suggest** that you:

- keep your terminal close to where you work during business hours,
- securely store your terminal out of sight when it is not in use (during and after business hours),
- limit third-party access to your terminal (contractors or delivery personnel accessing your business), and
- routinely inspect your terminal for tampering.

Routinely inspect your terminal

During your inspection process, you must determine whether devices have been substituted or tampered with. To determine whether a device has been substituted, you should collect the following information when you receive your terminal to compare against future information.

- Device manufacturer (front of the device)
- Make and model of terminal (back of the device on the label)
- Serial number of the terminal, (back of the device on the label)

We have provided a checklist (***Appendix A - Terminal Inspection Checklist***) that you may find useful when inspecting your terminal. If you find any discrepancies, immediately unplug the affected terminal and call the TDMS Contact Centre at **1-800-363-1163** to report this and receive instructions on your next steps.

Things to look for:

- Missing/damaged/altered tamper seals
- Missing/mismatched screws
- Incorrect keyboard overlay
- Exposed wires on the outside of the terminal
- Holes drilled/cut into the terminal
- New labels/paint/coverings that could mask tampering
- A ***skimmer*** device has been added to the terminal — skimmers are devices used by unauthorized personnel trying to capture cardholder data prior to reading the card

Secure your business' WiFi network

If you use a terminal that uses WiFi communications:

- **Never use a public, or an unsecured, WiFi network!**
- Always change the default password supplied with your router/modem to a strong, complex password that include letters, numbers, ***and*** symbols.
- Do not share the password with customers or employees.
- Frequently change the password.
- Install firewalls and antivirus software to protect your WiFi network.

User management

By utilizing user types, you can help secure your terminal by limiting access to certain terminal functionality. Listed below are the generally available user types.

- Administrator (highest),
- Manager/Supervisor, and
- Clerk (lowest).

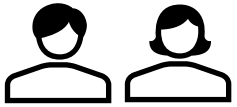
Role	Description
Administrator[3]	• Can access all features and functions, including financial transaction processing, reports, and all menus • Can set up manager, supervisor, and clerk IDs
Manager/ Supervisor	• Some terminals have one or both roles (Manager and/or Supervisor) available • Can access features and functions (including transaction processing), all reports, and all menus • Can perform financial transactions • Can set up clerk IDs
Clerk	• Can perform financial transactions

Example

You have a business with four employees: you the business owner, an assistant manager, and two cashiers. You could set up the roles as follows:

Business Owner
Administrator

Asst. Manager
Manager/ Supervisor



Cashiers
Clerks

3 The administrator passcode is also referred to as the Terminal Access Number.

When an employee leaves your business:

- immediately remove their ID and password from all of your terminals,
- change any passwords that they had access to, and
- remove any access they may have to bank accounts or sign authority.

Business Owner as Administrator

This role is created at terminal installation as you, the business owner, must have access to everything on the terminal to run your business.

Asst. Manager as Manager/ Supervisor

The Manager/Supervisor performs your role for day-to-day business activities. You can select what access they have to sensitive terminal functionality.

Cashiers as Clerks

Clerks facilitate customers performing financial transactions for your business.

To learn how to manage users, refer to the online ***Merchant Guide*** or the ***Configuration/Troubleshooting Guide***.

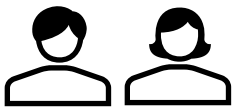
Protecting terminal functionality

There are different ways to help protect your terminal by password including using passwords and the user level functionality (administrator, manager/supervisor, or clerk). These settings are useful to block specific transactions/functions from general users such as force sale, day end settlement, and administrative functions on the terminal.

Note: You must call the TD Merchant Solutions Contact Centre to enable the protected settings.

Example

It is best to work your way up from the lower user roles in deciding what functionality you want to grant to them. Using the same business example:



Cashiers
Clerks

If the cashiers at your business only perform sales, you could call the TDMS Contact Centre and password protect refunds, voids, force sales, etc. As you have password protected these transactions, you must now decide who can use their password to access these transactions.

Asst. Manager
Manager or Supervisor

If your Asst. Manager is your representative when you're not at your business, they should have to have the authority to perform the password protected transactions.

If they are only responsible for managing users (add, edit, delete) then they do not need this functionality and the responsibility would fall to you, the business owner/administrator.

Activity log

Some terminals have an activity log that displays/prints a report log showing all protected activity accessed on the terminal. The activity captures the user ID against the password protected function that was performed.

Only the administrator has access to this report.

To learn how to retrieve the activity log, refer to your terminal's the online ***Merchant Guide*** or ***Configuration/Troubleshooting Guide***.

What functionality can I protect?

- Initiating sale, return, void, force sale, and manually-keyed credit card transactions
- Initiating and completing pre-authorization transactions
- Performing settlement/day close
- Reprinting receipts
- Printing reports
- Changing between semi-integrated to standalone modes (semi-integrated terminals only)
- Accessing various menus

How is it protected?

- Terminal functionality is protected by user type (administrator, manager/supervisor or clerk), not by user ID.
- To use a protected function, the user must log in with their ID. If their user type is insufficient, they will be denied access.

Transaction Security

No matter what type of business you're in, fraudulent transactions can impact you. Knowing how to recognize and reduce this risk is possible. While there is not one specific thing that you can do to eliminate fraud, below are some tips on how you can help prevent it.

Card present transactions

- Using chip technology (e.g. chip and pin, tap/contactless) to process Card Present transactions is one of the most important and effective ways to help protect your business from losses.
- Manually keying credit card information into your terminal when the Cardholder is present significantly increases your risk of fraudulent transactions and incurring losses from Chargebacks. For more information, visit Risks of Manually Keying Credit Card Information.
- Merchants are responsible for the care and control of their terminals at all times. This includes being present for the duration of time that the device is in operation by your customer. Fraudsters will try a variety of different ways to perform fraudulent transactions. Common methods that they will use include:
    - They damage their credit card's magnetic stripe and insert their card incorrectly to force the transaction to default to manual entry.
    - Change the mode of acceptance initially programmed by the Merchant (e.g. from Chip and PIN to manual entry) exposing Merchants to potential fraud with Chargebacks.

Manually entered transactions have a high risk of fraud

If you do manually enter a credit card transaction which is deemed fraudulent, you will be held responsible for any Chargebacks associated with it. Manually entered credit card transactions include mail order and telephone order transactions.

Card checks

Ensure that you train employees to recognize suspicious behaviour or transactions. Immediately report any suspicious activity to TD Merchant Solutions at **1-800-363-1163**. Also, ensure you are compliant with the Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/merchants/.

What do I check for?

- Verify the card is signed.
- If a signature is required for the receipt, verify that signature matches the back of the card.

- Verify that the expiry date has not passed.
- Remember: Only **you** may manually enter the card information on the terminal.

The above checks do not eliminate the risk of fraud.

Manually entered credit card transactions

If you are uncomfortable performing a force sale, it is within your right as a business owner to request another form of payment (debit, cash, etc.).

If you do process a manually entered credit card transaction, please refer to the available card checks on the previous page. These transactions can be password protected to ensure it is not performed by unauthorized employees.

Please see ***Protecting terminal functionality*** for more information.

Manually entered transactions have a high risk of fraud

If you do manually enter a credit card transaction which is deemed fraudulent, you will be held responsible for any Chargebacks associated with it. Manually entered credit card transactions include mail order and telephone order transactions.

Force sale/Force post transactions

The Force sale/Force post function allows prior authorization numbers to be manually keyed in. For your protection, this capability is disabled by default on your terminal.

If you wish to process force sale transactions, please call the TD Merchant Solutions Contact Centre at **1-800-363-1163** to enable the capability after being authenticated. We strongly recommend that you password protect force sale functionality.

Please see ***Protecting terminal functionality*** for more information.

Force sale transactions have a high risk of fraud

If you receive an authorization for a force sale, it does not eliminate the risk of fraud.

Refunds (Credit and Debit)

If you are concerned about the risk of inappropriate refunds (whether due to errors, employee fraud, etc.) you should consider adding a supervisor password to these transactions.

To have a supervisor password requirement added to refund transactions, please contact the TD Merchant Solutions Contact Centre at **1-800-363-1163**.

Please see ***Protecting terminal functionality*** for more information.

Card not present transactions

- Capturing the Card Verification Value (CVC) is mandatory when processing Card Not Present transactions. The CVC is usually the 3 or 4-digit security code on the back of the card.
- The Address Verification Service (AVS) is a tool offered to ecommerce Merchants to support the detection of suspicious credit card transactions and compares the billing address submitted by the purchaser with the cardholder's billing address on record at the issuing bank.

AVS checks **do not** eliminate the risk of fraud.

Call for authorization

Sometimes, due to a communication or security issue, a transaction cannot or should not be completed. See the list of messages and events below that will require you to call for authorization.

Authorizations **do not** eliminate the risk of fraud. If you manually enter a fraudulent credit card transaction you will be held responsible for any chargebacks associated with it.

Whenever...

- you perform a force sale or force pre-authorization transaction.

  OR

- the card number on the screen does not match the embossed number on the card.

  OR

- the cardholder signature on the receipt does not match the signature on the reverse of the card.

  OR

- you have any doubts about the validity of a card or a transaction.

You must...

1. Call for a voice authorization immediately.
2. Request a **CODE 10** authorization. In this situation, you may be dealing with a fraudulent card and **CODE 10** will alert the financial institution to this possibility.

Storing cardholder receipts

Merchants are responsible for retaining all receipts to respond to cardholder inquiries such as challenges or chargebacks. The following are storage guidelines to ensure their integrity. Please store your receipts:

- ***In a dark, cool, secure area for at least 18 months***
- ***For as long as you retain cash register tapes for direct payment transactions***
    - If TD needs a receipt copy, please send it within eight (8) days and retain a copy for your records.
    - The required storage and response times are for TD Merchant Solutions only and may vary by financial institution.
    - Your receipts could become unreadable if they are stored in plastic coated containers or exposed to direct heat or cold sources.
- ***File receipts in envelopes, arranged by date, in a secured/locked filing cabinet***
    - If you have several terminals use a different envelope for each terminal.

Cardholder information

Fraudsters may use receipts to piece together card information.

The above also includes any reports that you may print with cardholder information. These should be stored securely or destroyed.

Payment Card Industry Data Security Standard (PCI DSS)

The efforts of PCI DSS are designed to help you prevent the theft of confidential consumer cardholder data by assessing whether that data is secure within your organization and, if necessary, improving your level of security to meet or exceed industry standards.

PCI DSS requires any organization that collects, processes, transmits or stores cardholder data, to uphold and maintain the data security standards that are set by the payment industry worldwide, and which are managed by the PCI Security Standards Council (PCI SSC).

All merchants who handle cardholder data must comply with PCI DSS and the Payment Card Networks' Compliance Programs. Merchants that don't comply may be subject to fines, fees or assessments and/or termination of their processing services.

Please visit https://www.td.com/ca/en/business-banking/how-to/merchant-solutions/fraud-prevention-pci-data-security-standard and https://www.pcisecuritystandards.org/merchants/ for more information.

Appendix A - Terminal Inspection Checklist

Print this checklist for each terminal and inspect them to verify that they have not been tampered with.[4]

Date of Inspection: _____

Device Manufacturer: _____(front of the terminal)

Make and Model: _____(back of the terminal on the label)

Serial Number: _____(back of the terminal on the label)

Does your terminal have any of the following?

Condition	Yes	No
Missing, damaged, or altered tamper seals	☐	☐
Missing or mismatched screws	☐	☐
Mismatched keys	☐	☐
Incorrect keyboard overlay	☐	☐
Exposed wires on the outside the terminal	☐	☐
Holes drilled or cut into the terminal	☐	☐
New labels/paint/coverings have been added that could mask tampering	☐	☐
A ***skimmer*** device has been added to the terminal[5]	☐	☐
Something not covered in the points above that looks unusual or out of place	☐	☐

If you checked **Yes** to any of the above boxes:

- Immediately unplug the affected terminal, and
- call the TDMS Contact Centre at **1-800-363-1163** to report this and receive instructions on your next steps.

4 We strongly suggest that you inspect your terminals thoroughly and frequently.

5 Skimmers are devices used by unauthorized personnel trying to capture cardholder data prior to reading the card. Skimmers may be inserted into the Magnetic Stripe Reader, Chip Reader, or overlaid on the device itself.

Appendix B - Computer Fraud Prevention Tips

- Install a firewall to protect your computer.
- Use only legally licensed software and keep it current with the latest updates.
- Use the most up-to-date commercially available antivirus software. Free software may not protect against the latest threats.
- Choose unique passwords that include a combination of letters, numbers and symbols.
- Do not use the same passwords for personal and business applications.
- Ensure that auto-complete password functions on your browser are disabled.
- Never save passwords on your computer, the internet, or on any software.

Appendix C - Email Fraud Prevention Tips

- Do not include banking information in an email to TD or anyone else unless it is encrypted.
- Do not open file attachments in emails from unknown senders.
- Do not use links in an email to go to any web page. If you suspect the message might not be authentic, call to verify it or type in the web address directly in your browser.
- Be suspicious of emails that appear to be from a trusted sender (such as a bank or government agency) that instruct you to provide account information or verification, or banking access credentials such as Connect ID, password and authentication token codes via a hyperlink. Report any suspicious emails immediately to TD at phishing@TD.com.
- If you believe you've responded to a suspicious email and have shared your online banking login credentials, please report the incident immediately:
    - For Web Business Banking call the CMS Support Desk at 1-800-668-7328
    - For EasyWeb call EasyLine at 1-866-222-3456
- Always verify payment instructions by phone or in person even if they appear to be from a known source. Do not act on email instructions as the email could have been fraudulently created.

Contact Information

Please call the TD Merchant Solutions Contact Centre at **1-800-363-1163**. We would be happy to answer any questions you may have.

Authorization:

24 hours a day, seven days a week

Terminal Inquiries:

24 hours a day, seven days a week

General Merchant Inquiries:

Monday – Friday, 8 a.m. – 8 p.m. ET

Printer / Stationery Supplies:

Monday – Friday, 8 a.m. – 5 p.m. ET

Resource Centre

This guide covers the most commonly used information in order to get you started. Your terminal has more features and functionality to explore on our documentation portal which you can find at www.tdmerchantsolutions.com/resourcecentre.

Resource Centre