TD Merchant PC

Merchant Guide

For Merchant PC

- with PINpad
- without PINpad

Copyright © September 2026

This publication is confidential and proprietary to The Toronto-Dominion Bank and is intended solely for the use of Merchant customers of TD Merchant Solutions. This publication may not be reproduced or distributed, in whole or in part, for any other purpose without the written permission of an authorized representative of The Toronto-Dominion Bank.

NOTICE

The Toronto-Dominion Bank reserves the right to make changes to specifications at any time and without notice. The Toronto-Dominion Bank assumes no responsibility for the use by the Merchant customers of the information furnished in this publication, including without limitation for infringements of intellectual property rights or other rights of third parties resulting from its use.

Table of Contents

Welcome to TD Merchant Solutions iii
The purpose of this guide iii

Overview iii
System requirements iii

Security iii
Protecting Cardholder Privacy iv
Protecting yourself from fraud iv
When to call for cardholder authorization iv
When to use your imprinter iv
Storing cardholder receipts v
Debit transaction disputes v

Using the Software v
User menu v
Logon v
Logoff vi
Your PC's main screen vi
Transaction buttons vi
Function buttons 1
The PINpad (optional) 2
The front view - iPP320 2

Financial Transactions 3
Purchase (credit) 3
Purchase (debit) 3
Mail / Phone order 4
Pre-authorization 4
Pre-auth completion 5
Refund 5
Void 5
Force purchase (if allowed) 6
Force mail / phone order (if allowed) 6
Balancing your transactions 7
Your balancing window 7
Balancing steps 7
Store close 8
Reports 8
User ID 8
Terminal details 9
Detailed report fields 10
Terminal detail report 10
User ID report 11

Continued on next page

Tender type *11*
Transaction type *12*
Batch selection window *12*
Terminal cashback *13*
User ID cashback *13*
Terminal tip total *14*
User ID tip total *14*
Terminal balancing *15*
User ID balancing *15*

Administrative Menu Options 16
Parameter download 16
Diagnostics 16
Editing existing settings 16

Software Messages 16

Agreement 19

Welcome to TD Merchant Solutions

We're glad you've decided on the TD Merchant Solutions Merchant PC Software. These merchant materials provide you helpful information about your equipment and TD Merchant Solutions (TDMS). Most importantly, they tell you how to contact us with any questions you may have.

The purpose of this guide

This guide provides instruction on the use and functionality of the TD Merchant PC software using credit card, debit card, as well as additional accepted card types. It also provides general administrative guidelines with respect to both credit and debit.

The provision of Visa® and/or Interac® Direct Payment and/or Mastercard® merchant services to you (the user) by TDMS is governed by the Merchant Services Agreement and any other agreement(s) that govern the services that we may provide to you. The use of the Merchant PC software with respect to the provision of merchant services by a third party is governed by any agreement(s) with such third party.

Overview

The TD Merchant PC Software provides automatic credit card and debit card authorizations and draft capture. Your printer will be used for providing cardholder receipts and printed reports for all balancing transactions. The PINpad issued by the cardholder during a debit card transaction to swipe their card, select their account and enter their PIN. It is also used during a credit card transaction to swipe the card.

Cardholder transactions are processed by selecting the appropriate card type, selecting the appropriate transaction type, entering the transaction information, swiping the card through the PINpad, or manually keying in a credit card,and clicking on a function button.

The first step in balancing is called a Software Balance Report which lists all transactions processed in the periods elected. The second step in balancing is called a **Store close** which sends all the transactions to the appropriate bank accounts and sets all totals to zero. For other balancing/ reporting options, make the appropriate menu choice.

System requirements

The following are the minimum requirements for the PC using the software:

1. Windows XP (with service pack 3) / Vista (with service pack 2) / Windows 7 / Windows 8.1 / Windows 10.
2. USB connector (for the PINpad).
3. DSL or other high speed Internet connection.
4. Certified PINpad (provided by TDMS) for debit and credit transactions.
5. Commercially available firewall software or commercially available firewall appliance.
6. Anti-virus software.

Security

To avoid unauthorized access to the cardholder information on your computer, you must have a firewall software or firewall appliance installed and properly configured on your computer. You must also have an anti-virus software installed and running with an up-to-date Virus Definition File. The TD Merchant PC software is capable of being used for unauthorized transactions including unauthorized debits to the merchant's account.

It is the merchant's responsibility to take whatever steps are necessary to keep the software and any user IDs or passwords secure and to prevent unauthorized use. In any event, the merchant will be liable for any unauthorized use of the terminal or any user IDs or passwords. Security can be placed on particular transaction types by request through the TDMS Help Desk.

Protecting Cardholder Privacy

Remember you have a responsibility to protect your customers from possible credit card fraud by maintaining the confidentiality of their personal information. Visa requires that merchants protect cardholders' account and transaction information including cardholder names, account numbers and information embossed, encoded or appearing on Visa cards ("information") in accordance with the Visa Account Information Security Standards.

You may not use Information for any purpose except to complete transactions authorized by the cardholder. Information must be stored in a secure area and only authorized staff should be given access to the Information. Information must be destroyed and rendered unreadable before it is discarded. If you make arrangements with any third party for the purpose of collecting, processing or storing information you must have a written contract with the third party which requires compliance with the Visa Account Information Security Standards.

You must allow TDMS or Visa to inspect your premises and ensure that we can inspect the premises of any third party to verify that Information is securely stored and processed. The Visa Account Information Security Standards Manual is available at www.visa.com or for further information please contact TDMS.

Protecting yourself from fraud

This software is designed to further protect us from cardholder fraud. The Merchant PC software can accept magnetic stripe and chip enabled credit cards. The PINpad provided by TDMS is equipped with a Smart Card Reader to read chip enabled cards and magnetic stripe reader to read magnetic stripe cards. When the credit card is inserted into the Smart Card Reader, the cardholder may be asked to enter a PIN (Personal Identification Number) or sign a receipt. For magnetic stripe transactions, please verify the credit card number and signature on the credit card against the merchant copy of the receipt. When the credit card is swiped in the PINpad, the cardholder number and expiry date automatically appear on the screen. The software will not proceed with the transaction until the user clicks on the **OK** key. This allows the merchant time to verify that the numbers on the screen match the numbers embossed on the card.

Take the time to do this verification. Always take the time to verify that the cardholder's signature on the receipt matches the signature on the reverse of the card.

When to call for cardholder authorization

- **Whenever the message CALL FOR AUTH is seen -** Do not attempt the transaction again. Click on **CLEAR** button and call for a voice authorization immediately.
- **When the card number on the screen does not match the number embossed on the card -** Click on **CANC** key and call for a voice authorization immediately. 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.
- **When the cardholder signature on the receipt does not match the signature on the reverse of the card -** Call for a voice authorization. Request a CODE 10 authorization. The financial institution will be able to advise whether or not the correct individual is using the card. They will also tell you how to proceed.
- **Whenever you have any doubts about the validity of a card or a transaction, do not hesitate to call for authorization.**

When to use your imprinter

You must use your imprinter in each of the following situations.

- **If you are unable to swipe the card through the PINpad due to a problem with the card's magstripe -** Key in the transaction manually, take an imprinted draft for the cardholder's signature, indicate the transaction details in the imprinted copy and staple the printer receipt to the signed copy.
- **If your printer is not working -** Take an imprinted draft for the cardholder's signature and indicate the transaction details on the imprinted copy.

- **If the system is down, the software does not ask for an authorization number and you receive a telephone authorization -** take an imprinted draft, note all transaction details on the draft. When the system becomes available, enter all manually imprinted transactions using the FORCE POST MENU OPTION, and staple all printed transactions to the imprinted sales drafts.

Storing cardholder receipts

Users are responsible for retaining all receipts to respond to cardholder inquiries. These steps should help to conveniently store receipts.

1. Keep receipts in a secure place for at least one year. Envelopes arranged by date in a secured filing cabinet can work well.
2. Transaction receipts should be stored in a dark (thermal receipts), secure area with limited access.
3. If you have several softwares use a separate envelope for each software.
4. For VISA transactions, file and store receipts for at least one year.
5. For Direct Payment transactions, store receipts as long as you retain cash register tapes.
6. If we need a receipt copy, send it to us within eight days. Retain a copy of the receipt for your records.

For further information on your responsibilities to secure Cardholders' information please see page 3. The required storage and response times apply for TDMS only and may vary by financial institution.

Debit transaction disputes

A customer, who complains regarding an alleged erroneous debit card transaction, must be referred to his/her own financial institution to correct the problem. Users will be responsible for any attempt to make debit card account corrections and will not be reimbursed if a cash refund is provided to the customer.

Using the Software

This section provides an introduction to the software's main user screen. It describes the landscape and provides instructions for using the buttons. Instructions for the most common customer and closing transactions are provided in the ***Quick Reference Guide***. Instructions for the transactions that you will use less frequently are provided in the section called Financial Transactions.

User menu

Logon

This window is only displayed if the merchant activates the option for **User Logon Required** in the Merchant Data Setup. All entries are case sensitive. Enter the user name, and the password for this user. If this is the first time the user is logging on, the password is ***temp***. Click on **OK**. First time users will see the ***Change Password*** window immediately after clicking on **OK**, otherwise the software's main screen will be displayed.

Click **Exit** to exit the software.

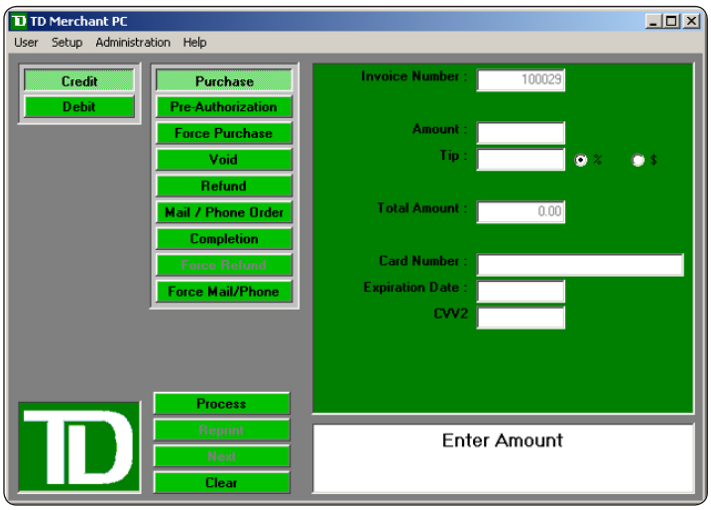
Logoff

This is only available if the merchant activates the option for User Logon Required in the Merchant Data Setup. Logs off the current user, and displays the ***User Logon*** window.

Your PC's main screen

Your screen has 4 main areas:

1. The transaction buttons on the upper-left side.
2. The function buttons on the lower-left side.
3. Information entry on the upper-right side.
4. Message display area on the lower-right side.



Transaction buttons

If an abbreviated description is displayed on the button, leave the cursor over the button for one second and a full button description will be displayed.

Transaction	Explanation
Credit	Process a transaction with a credit card.
Debit	Process a transaction with a debit card.
Purchase	Charge a customer's credit card or debit card for a regular purchase. Do not use this option for Mail/Phone Order transactions.
Pre-Authorization	Hold funds on a customer's credit card for completion at a later time.
Force Purchase	Process a voice authorized purchase on a customer's credit card.
Void	Void a transaction from a cardholder's account.
Refund	Return funds to a cardholder's account.
Mail/Phone Order	Charge a customer's credit card for mail/phone order.
Completion	Charge a customer's credit card based on a pre-authorized transaction.

Transaction	Explanation
Force Mail/Phone	Process a voice authorized mail/phone order on a customer's card.

If your business uses a PINpad, all manual credit card entries must be performed on it, not onscreen.

Function buttons

Button	Explanation
Process	Sends the transaction to the PINpad for card **Insert, Swipe**, **Tap** or **Manual Entry**.
Reprint	Reprints the last successful transaction. Only available on the current transaction until the **Clear** or **Next** button is clicked.
Next	Clears all fields on the screen and remains on the current transaction type (except for a completion transaction, which defaults to a Credit Purchase).
Clear	Clears all fields on the screen and defaults to Credit / Debit Purchase.

Information entry

Setting	Explanation
Invoice Number	The invoice number for this transaction. If this field is set to be automatically generated, the number will be displayed in a grey colour, and cannot be edited.
Amount	For the entry of the amount of the transaction.
Tip	For the entry of the percentage or dollar amount of the transactions (see ***Merchant Data*** window, to determine if allowed). The tip type must be chosen before entering the tip value, as the field is cleared after the type is chosen. **%** If chosen, indicates that the amount in the Tip box is a percentage of the Amount box to be added to the transaction amount. **$** If chosen, indicates that the amount in the Tip box is a dollar amount to be added to the transaction amount.
Cashback	A dollar amount (whole dollars only) to be given in cash to the customer at the end of the debit transaction (see ***Merchant Data*** window to determine if allowed).
Total Amount	The sum of the Amount, Tip and Cashback boxes. This amount is charged to the cardholder's account.
Authorization Number	For the entry of a voice authorization.
Card Number	For the manual entry of a credit card number.
Expiration Date	For the manual entry of a credit card expiry date. Entered as MMYY (as seen on the credit card).

The PINpad (optional)

The PINpad is used to process credit or debit cards via insert, swipe and tap or manually entry (if allowed) to meet requirements for protecting cardholder information. If you don't have a PINpad, you can only process credit cards manually.

The PINpad keys are described briefly below:

OK (Green key) The customer uses this key to authorize transactions.

CANC / ANNUL (Red Key) The customer uses this key to cancel a transaction (prior to pressing **OK**).

CHQ or SAV / EP The customer uses these keys to select the account they wish to access.

CORR (Yellow key) The customer uses this key to correct an entry when there is an error.

The front view - iPP320

1. **Function keys**

   The **F1** and **F4** keys can be used to select onscreen options.

2. **Navigation keys**

   Use the **F2** and **F3** arrow keys to navigate the screens and menus.

3. **Command keys**
   - Cancel
   - Correction
   - OK (or Enter)

4. **Card readers**
   - **a)** Insert chipped cards
   - **b)** Contactless cards
   - **c)** Swipe cards

Financial Transactions

Purchase (credit)

1. Click on **Credit**.
2. Click on **Purchase**.
3. Enter the **Invoice Number** (if allowed / required).
4. Enter the **Amount**.
5. Select the **Tip Type** and enter the **Tip Amount/Percentage** (if allowed / required).
6. Perform one of the following payment methods: **Insert, Swipe**, **Tap** or **Manual Entry**.

   Insert, Swipe or Tap (with PINpad)

   a) Follow the prompts on the PINpad. Go to step 7.

   Manual Entry (with PINpad)

   This is disabled by default. You must call TDMS Help Desk to activate manual entry on the PINpad.

   a) Enter the **account number** on the PINpad and press **OK**.

   b) Enter the **expiry date** on the PINpad and press **OK**.

   c) Enter the **CVD number** on the PINpad and press **OK**.
   This three or four digit number is generally located on the back of the credit card. Go to step 7.

   Manual Entry (without PINpad)

   a) Enter the **account number** on the screen.

   b) Enter the **expiry date** on the screen.

   c) Enter the **CVD number** on the screen. If the ***Card Number Check*** window pops up, compare the displayed card number with the embossed card number and verify that they are identical. Go to step 7.

   d) Click **Process**.
7. Click **Reprint** to reprint the receipt.
8. When the transaction is completed, click **Next** or **Clear**.

Purchase (debit)

1. Click on **Debit**.
2. Click on **Purchase**.
3. Enter the **Invoice Number** (if allowed / required) and press **OK**.
4. Enter the **Amount** and press **OK**.
5. Select the **Tip Type**, enter the **Tip Amount/Percentage**, and press **OK** (if allowed / required).
6. Perform one of the following payment methods: **Insert, Swipe**, or **Tap**. Follow the prompts on the PINpad.

7. Enter the **Cashback Amount** (if allowed / required) and press **OK**. Cashback is not allowed when the debit card is tapped.
8. Click **Reprint** to reprint the receipt.
9. When the transaction is completed, click on **Next** or **Clear**.

Mail / Phone order

1. Click on **Credit**.
2. Click on **Mail/Phone Order**.
3. Enter the **Invoice Number** (if allowed / required).
4. Enter the **Amount**.
5. Select **Mail Order** or **Telephone Order** or, if you use a PINpad, select **F1 - Mail Order** or **F4 - Telephone Order**. If your setup does not include both Mail Order and Telephone Order, you will not see step 5, but you will see the appropriate sub-steps for the transaction below.

   Mail Order

   a) Enter the **Card Number**

   b) Enter the **Expiration Date**.

   Telephone Order

   a) Enter the **Card Number**

   b) Enter the **Expiration Date**.

   c) Enter the Card Verification Data (CVD). This is the 3 or 4 digits printed on the front or back of the card.
6. Click **Process**.
7. Click **Reprint** to reprint the receipt.
8. When the transaction is completed, click on **Next** or **Clear**.

Pre-authorization

1. Click on **Credit**.
2. Click on **Pre-Authorization**.
3. Enter the **Invoice Number** (if allowed / required).
4. Enter the **Amount**.
5. Perform one of the following payment methods: **Insert, Swipe**, **Tap** or **Manual Entry**.

   Swipe (with PINpad)

   a) Follow the prompts on the PINpad. Go to step 6.

   Manual Entry (with PINpad)

   This is disabled by default. You must call TDMS Help Desk to activate manual entry on the PINpad.

   a) Enter the **account number** on the PINpad and press **OK**.

b) Enter the **expiry date** on the PINpad and press **OK**.

c) Enter the **CVD number** on the PINpad and press **OK**.

This three or four digit number is generally located on the back of the credit card. Go to step 6.

Manual Entry (without PINpad)

a) Enter the **account number** on the screen.

b) Enter the **expiry date** on the screen.

c) Enter the **CVD number** on the screen.

If the ***Card Number Check*** window pops up, compare the displayed card number with the embossed card number and verify that they are identical. Go to step 6.

d) Click **Process.**

6. Click **Reprint** to reprint the receipt.
7. When the transaction is completed, click on **Next** or **Clear**.

Pre-auth completion

1. Click on **Credit**.
2. Click on **Completion**.
3. Either click on the **Transaction** or choose a search criteria, **enter a value** and click on **Find Next** until the transaction is found.
4. Click on **Select**.
5. Enter the **Amount** if it is different from the pre-authorized amount.
6. Enter the **Tip**.
7. Click on **Process**.
8. Click on **Cancel** to exit when done.

Refund

1. Click on **Credit** or **Debit**.
2. Click on **Refund**.
3. Enter the **Invoice Number** (if allowed / required).
4. Enter the **Amount**.
5. Either click Pro**cess** and swipe the card, **OR** manually enter the **card number** and **expiry date**, and click **Process**.
6. When the transaction is completed, click on **Next** or **Clear**.

Void

1. Click on **Credit** or **Debit**.
2. Click on **Void**.
3. Choose the **Void Transaction Type**.

4. Either click on the **Transaction** or choose a search criteria, enter a **Value** and click on **Find Next** until the transaction is found.
5. Click on **Select**.
6. Debit Transaction - swipe the card at the PINpad.
7. Click on **Cancel** to exit when completed.

Force purchase (if allowed)

1. Click on **Credit**.
2. Click on **Force Purchase**.
3. Enter the **Amount**.
4. Select the **Tip Type** and enter the **Tip Amount/Percentage** (if allowed).
5. Enter the **authorization number**.
6. Manually enter the credit card information.

   Manual Entry (with PINpad)

   You must have both Force Purchase and Manual Entry enabled in order to use the PINpad.

   a) Enter the **account number** on the PINpad and press **OK**.

   b) Enter the **expiry date** on the PINpad and press **OK**.

   c) Enter the **CVD number** on the PINpad and press **OK**.

   This three or four digit number is generally located on the back of the credit card. Go to step 7.

   Manual Entry (without PINpad)

   a) Enter the **account number** on the screen.

   b) Enter the **expiry date** on the screen.

   c) Enter the **CVD number** on the screen.

   If the ***Card Number Check*** window pops up, compare the displayed card number with the embossed card number and verify that they are identical. Go to step 7.

   d) Click **Process**.
7. Click **Reprint** to reprint the receipt.
8. When the transaction is completed, click on **Next** or **Clear**.

Force mail / phone order (if allowed)

1. Click on **Credit**.
2. Click on **Force Mail/Phone Order**.
3. Enter the **Invoice Number** (if allowed / required).
4. Enter the **Amount**.
5. Select **Mail Order** or **Telephone Order** or, if you use a PINpad, select **F1 - Mail Order** or **F4 - Telephone Order**. If your setup does not include both Mail Order and Telephone Order, you will not see step 5, but you will see the appropriate sub-steps for the transaction below.

Mail Order

a) Enter the **Card Number**

b) Enter the **Expiration Date**.

Telephone Order

a) Enter the **Card Number**

b) Enter the **Expiration Date**.

c) Enter the Card Verification Data (CVD). This is the 3 or 4 digits printed on the front or back of the card.

6. Click on **Process**.
7. Click **Reprint** to reprint the receipt.
8. When the transaction is completed, click on **Next** or **Clear**.

Balancing your transactions

Your balancing window

Your balancing window is set into the system to reflect the time of the day you are most likely to do an End of Day. Depending on the time that has been chosen for your balancing window you will receive same or next business day deposit for Visa and debit card totals.

You are required to do an End of Day every day. If the End of Day is done after your balancing window all deposits to Visa, debit, and other card will be put forward to the next business day.

If an End of Day is not done, totals will remain in the terminal and are added to the following day's transactions. They will accumulate until an End of Day is done.

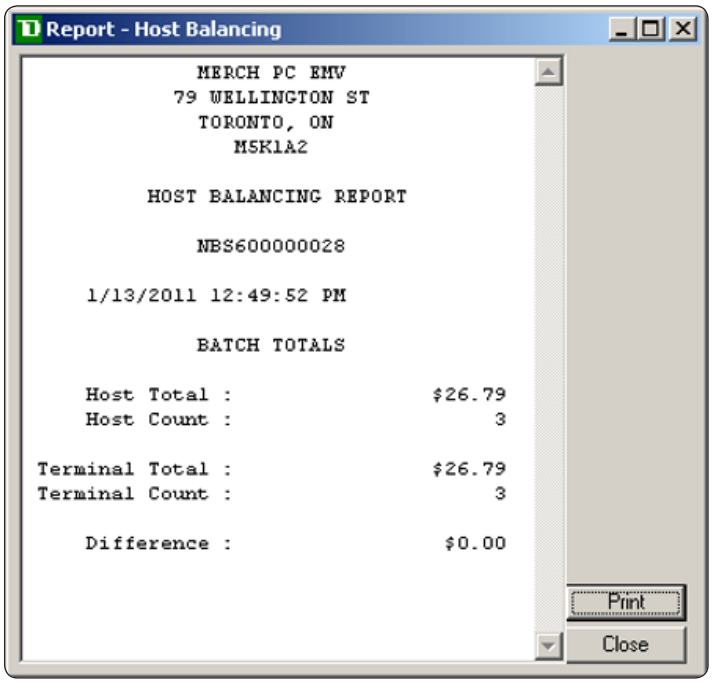
Balancing steps

There is one simple step to balancing your terminal, an End of Day transaction. The End of Day consists of the following steps:

1. Close the terminal to deposit all card totals to the appropriate accounts.
2. Print business day totals by card type.
3. Printing all reports specified for the End of Day Reports.

Store close

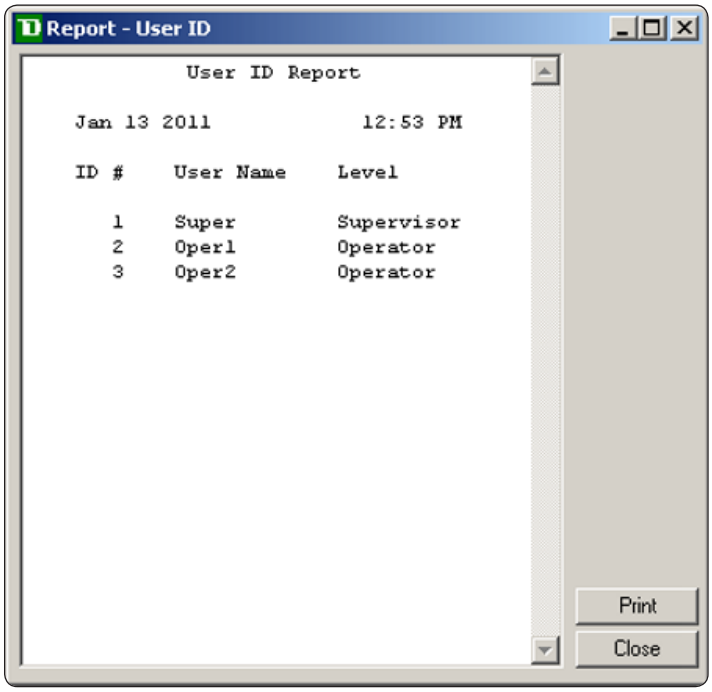
This report is automatically generated when a Store Close is completed.



Reports

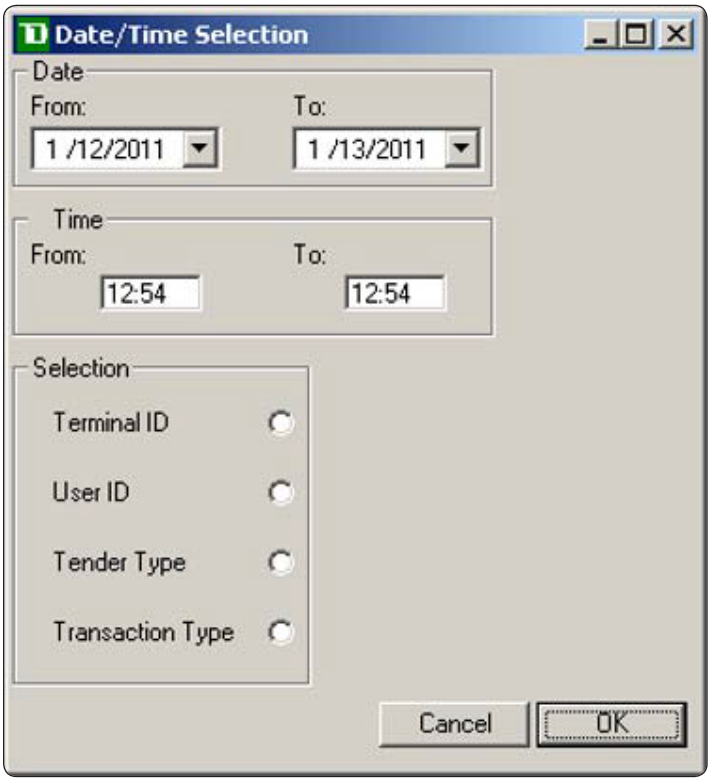
User ID

Provides a listing of all users and their levels.



Terminal details

This report allows you to print reports over multiple days, including the current open batch. The report is based on the selections available in the window.



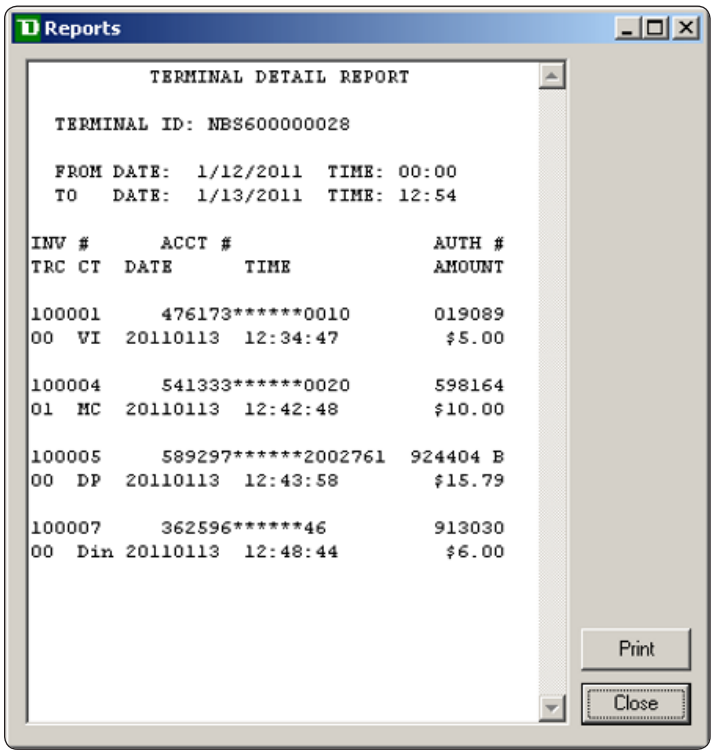
Setting	Explanation
Date	Start and end date for the reporting period. A drop down calendar is available for date selection. It is pre-filled with yesterday's date and today's date.
Time	Starting time on the start day and ending time on the end day of the reporting period. This is a 24 hour clock. Entry is done by entering the 4 digits of the time. It is pre-filled with the current time on the computer.
Selection	If no selection is made all transactions are listed in ascending order by date and time. If a selection is made the report is broken down by the item chosen. Note in the options, an All selection is available. If a person who has an Operator ID access selects the All option, they will only see their transactions. If a User ID, tender type or transaction type is not used within the time period selected, it will not be displayed.

Detailed report fields

Field	Explanation
Invoice #	Invoice number of the transaction
Acct #	Account / card number of the transaction
Auth #	Authorization number received for the transaction
TRC	Transaction code for the transaction type
CT	Card type used in the transaction
Date	Date of the transaction
Time	Time of the transaction
Amt	Amount of the transaction

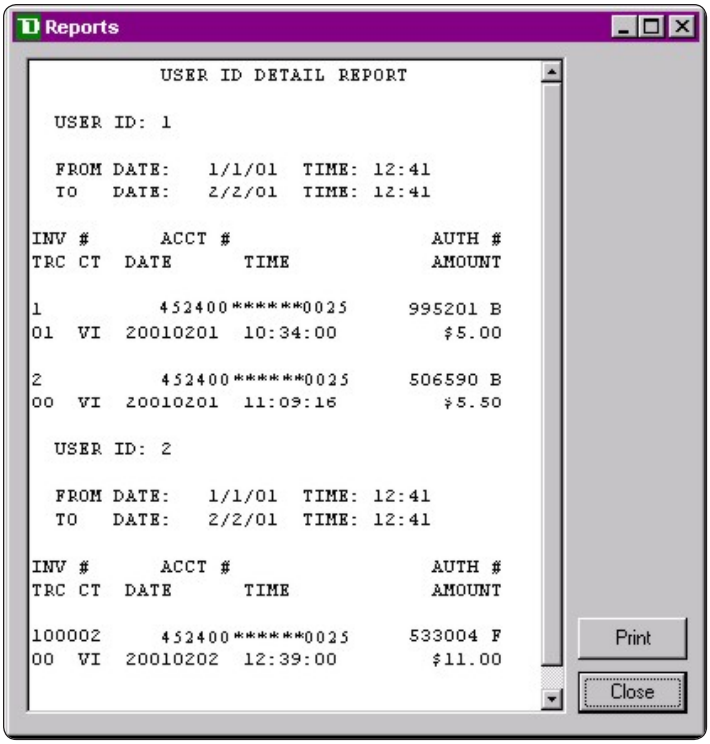
Terminal detail report

This report displays all terminal details for the terminal in ascending date and time order.



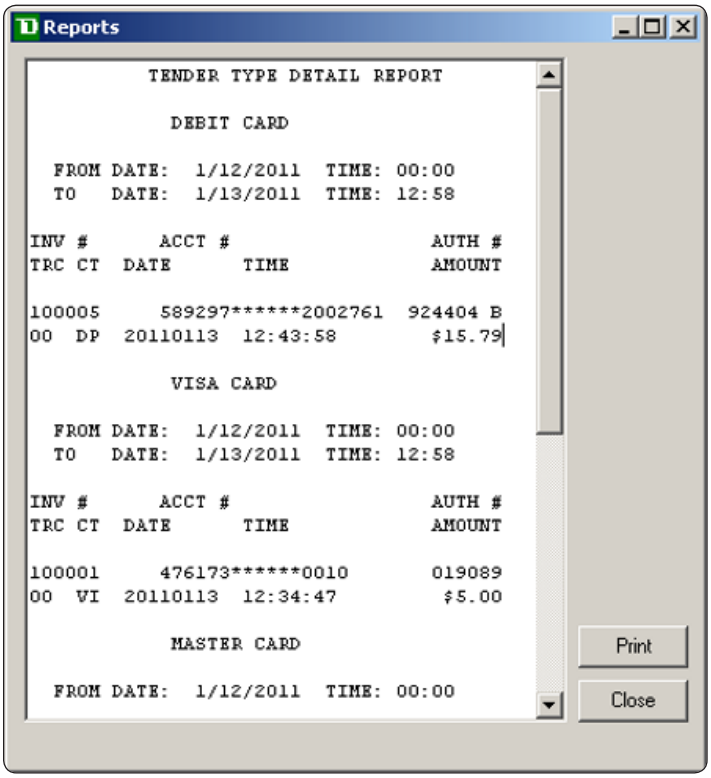
User ID report

This report displays all terminal details for the terminal by User ID, in ascending date and time order.



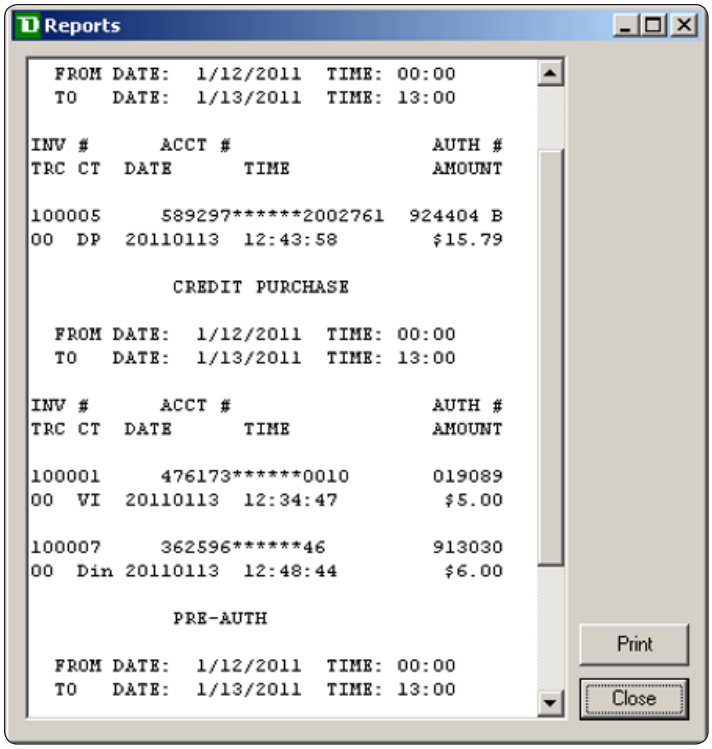
Tender type

This report displays all terminal details for the terminal by tender type, in ascending date and time order.



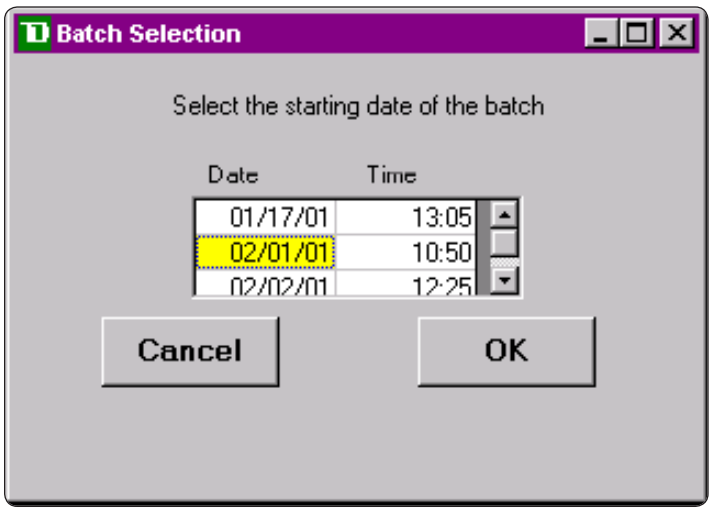
Transaction type

This report displays all terminal details for the terminal by transaction type in ascending date and time order.



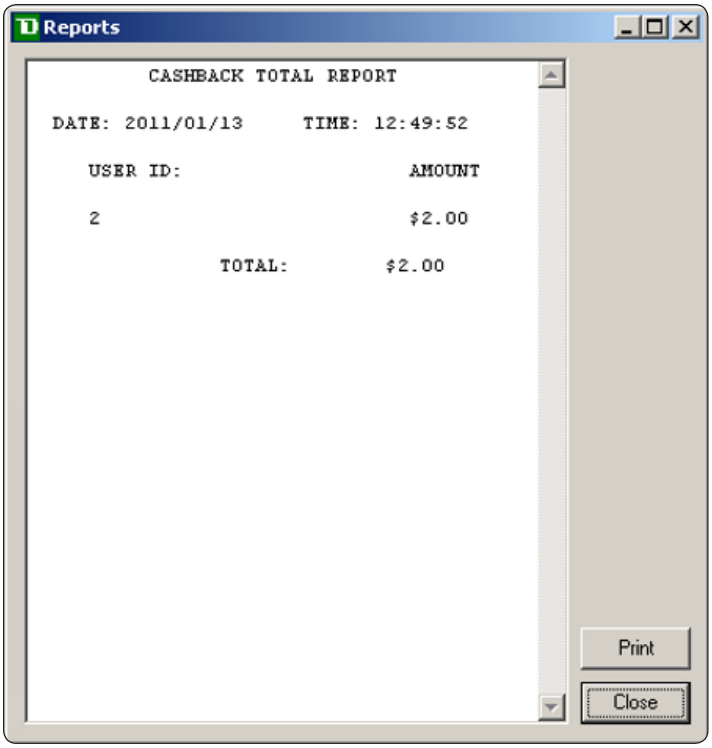
Batch selection window

This window displays the batches that are available for selection for the six reports below. It displays the date and time for the beginning of the batch. The last record displayed is the current open batch, and cannot be used for selection for these reports. When this window is opened, the last batch closed will be highlighted.



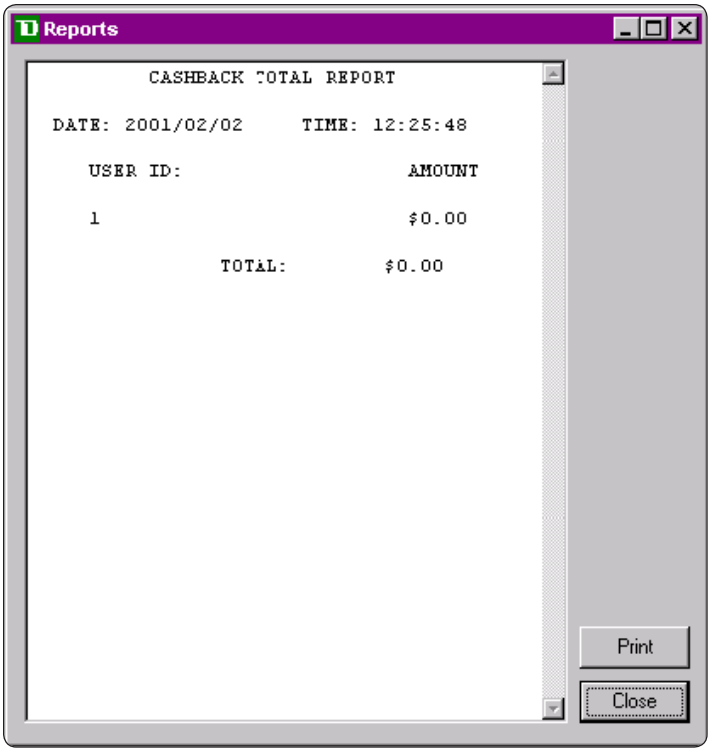
Terminal cashback

Displays / prints the total cashback amount processed for the terminal for the selected batch. This is only applicable if you use cachback.



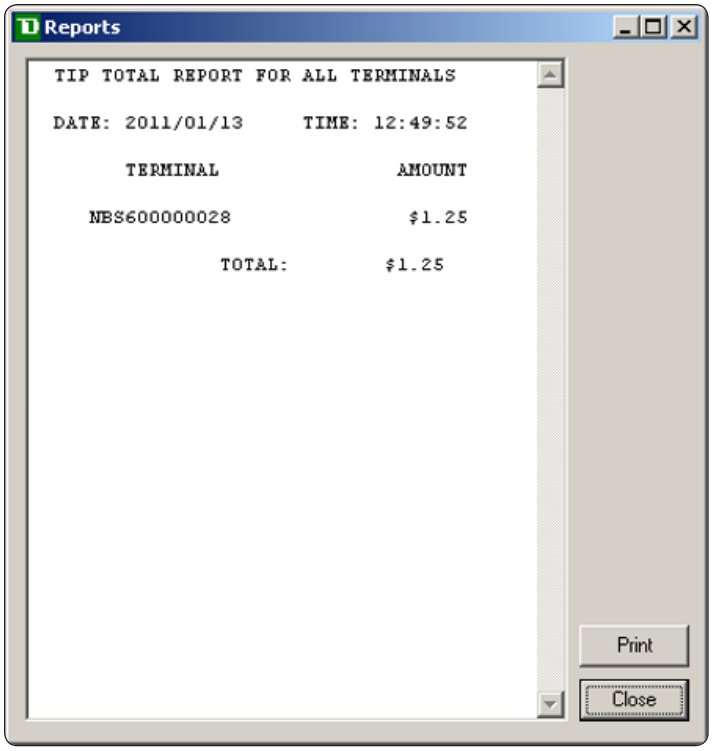
User ID cashback

Displays / prints the total cashback amount processed for the signed on user for the selected batch on the terminal (a Supervisor ID will display the amounts for all users). This is only applicable if you use cachback.



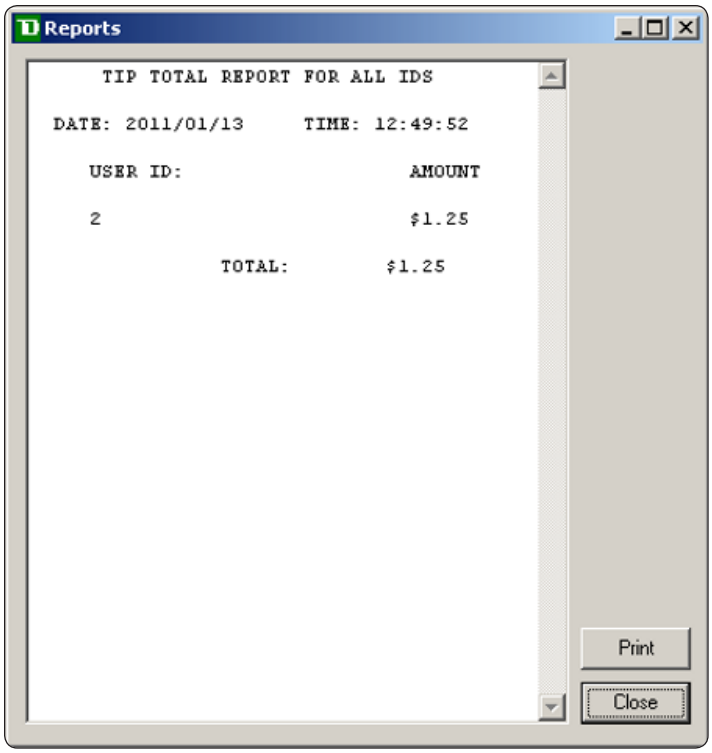
Terminal tip total

Displays / prints the tip totals processed for the terminal for the selected batch. This is only applicable if you use tips.



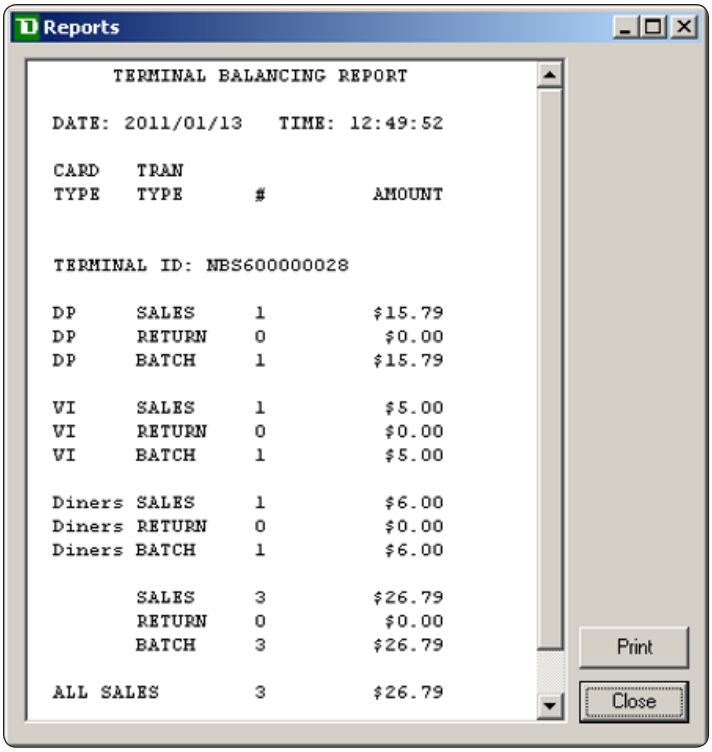
User ID tip total

Displays / prints the tip total processed for the signed on user for the selected batch on the terminal (a Supervisor ID will display the amounts for all users). This is only applicable if you use tips.



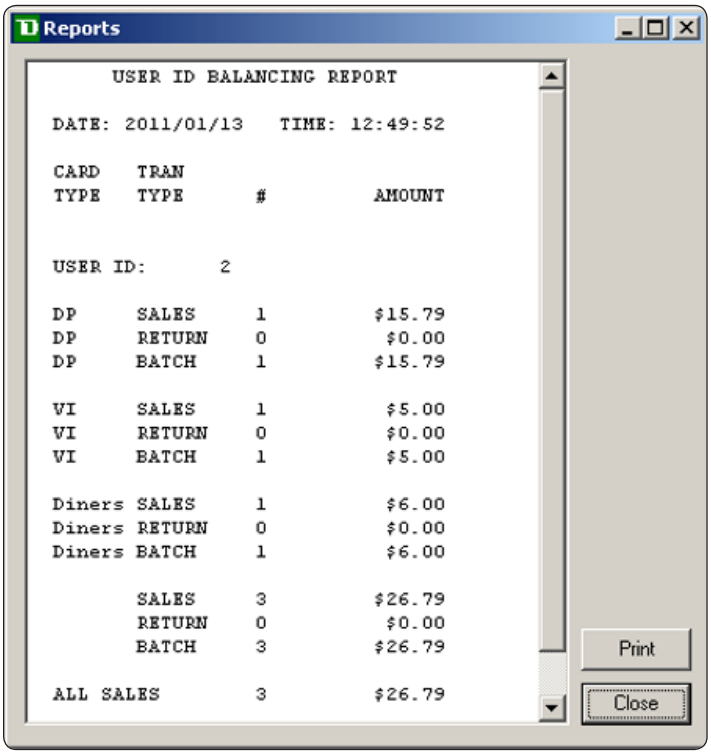
Terminal balancing

Displays / prints the terminal balance by card type for the selected batch.



User ID balancing

Displays / prints the terminal balance for the singed on user by card type for the selected batch (if the user logged on is a person with a supervisor ID access, the amounts for all users will display).



Administrative Menu Options

Parameter download

This function downloads the terminal's parameters from the host.

Diagnostics

This will be used by the help desk to assist in the collection of information to help diagnose any problems. A check mark will be displayed in the menu if it is enabled and the information is stored in a file.

Editing existing settings

The following are the two logins that can make changes to Merchant PC settings:

Supervisor ID: Created by another supervisor.

Supervisor Password: Created by another supervisor.

Support Login: Support and cannot be changed.

Support Password: Call TDMS Help Desk for the password of the day.

The following settings require a specific login to change them:

Supervisor Login	Support Login
Cashback (enable / disable)	User Login Required (enable / disable)
Invoice number (enable / disable)	Tip (enable / disable)
Printer changes	Any other security settings (enable / disable)
Create additional supervisor IDs	

Software Messages

Error Message	Explanation
Call For Auth	**1.** Call for a verbal authorization. **2.** Enter the authorization number received into the appropriate box. **3.** Click on **Process**.
Cannot Print to Receipt.txt	A change was made to the setup information and the program was not shut down. Close down the software completely and restart it.
Card Number Is Required	You are trying to process a transaction that requires a card number to be entered. Press **Enter**.

Error Message	Explanation
Check Printer	There is a problem with the printer. If the printer is out of paper, place a new roll in the printer. If not call TDMS Help Desk for assistance.
Could Not Read Configuration File	Contact the TDMS Help Desk.
Deletion Of This User Must Be Performed By A Supervisor	The Logon ID is not a person who has Supervisor ID access. A person who has Supervisor ID access must be logged on to delete an ID.
Driver Not Supported	Contact the TDMS Help Desk.
Error # . . .	Make a note of all steps leading up to the error and contact the TDMS Help Desk.
Expiration Date Invalid	The expiry date should be entered in the format MMYY (as seen on card).
Force Post Denied	Your Force Post request is rejected. Call the TDMS Help Desk.
Information Required To Perform Download Is Missing	Verify that the Terminal ID is filled in on the ***Merchant Data*** screen. Verify that the phone number / IP information, and the port numbers are correct on the Modem / PINpad screen.
Invalid Card Expiry Date	An invalid expiry date was entered manually. Please verify the expiry date and retry the transaction.
Must Be A Supervisor To Perform This Operation	The person who has an Operator ID access is trying to access a function reserved for a person with Supervisor ID access. Contact a supervisor.
New Password Must Be Different From Old	The old password cannot be used for the new password when changing a User ID password. Select a new password.
New Password Not Correct	The information in the **Confirm** box does not match the information in the **New Password** box. Please reenter the information in both boxes.
No Printer Has Been Setup	The software is unable to detect the printer. Check the connections, make sure it is turned on, verify that is displayed in the ***Setup Menu*** and then retry the transaction.
No Transactions Available For Completion	You have selected the **Completion** button, however there are no transactions in the Pre-Auth file. Select another transaction type.
No Transactions To Report	You have selected a report that has no information available for your request. Select another report.
Not Accepted Use Mag Stripe	You have tried to use a chip card that is not setup for the software. Swipe the card in the PINpad.

Error Message	Explanation
Password Invalid Please Reenter	You have entered an incorrect password for this user. Please reenter your password.
Password Length Too Short. Must Be A Minimum Of 4 Characters	You are trying to change your password with too few characters. Reenter the password with at least 4 characters.
Pin Pad Is Not Present	Check the connections on the PINpad and retry the transaction.
Pin Pad Is Not Ready	The PINpad should say ***Welcome/Bonjour***. Check the connections on the PINpad and retry the transaction.
Problem Initializing Modem Or Pin Pad	Make sure the modem or PINpad is connected correctly and turned on. If the problem still persists, call the TDMS Help Desk.
Problem With Store Close	Displays the transaction and file that the software had a problem with. Make sure the modem is connected and turned on, click **OK** and then continue. If the problem cannot be resolved, contact the TDMS Help Desk.
Processing Error	The chip card was removed from the terminal too soon. Please click on **Next** and retry the transaction. Do not remove the card until the transaction has been completed.
Sending Reversal	The transaction is being reversed. Retry the transaction.
Serv Not Allowed	This means the option is not available. Try again. If the problem persists, call the TDMS Help Desk.
Store Close Not Completed	The phone line was interrupted before the store close could be completed.
Swiped Data Does Not Match Card Number	The information entered for the credit card verification does not match the data read on the card's magnetic stripe. Try again or contact the Authorization Department for the card type.
Terminal Is Not Initialized	**1.** Go into the ***Setup Menu***. **2.** Verify that there is a **Terminal ID**. **3.** Download the phone number and modem setup. **4.** Perform a parameter download.
The Customer Requires $x Cashback	A cashback amount was entered on a debit transaction. The customer needs to be given the cash amount specified.

Error Message	Explanation
This Batch Has Not Yet Been Closed	You are trying to run a report on a batch that is currently open. Select a closed batch.
User Not Set Up. Please Contact Supervisor	The User ID entered does not exist on the system. Correct the information entered if a mistake was made on entry, or contact a supervisor to add the new user.

Agreement

This Agreement is between the merchant customer ("you", "your" and "yours") and The Toronto-Dominion Bank ("we", "us" and "our").

5. Carefully read all the provisions of this Agreement prior to opening software package, install software or using software. Opening, installing or using the software whether by you, by us on your behalf or by your employee or agent indicates:
   - **a)** your acknowledgement of receipt of and your agreement to the terms and conditions of this Agreement
   - **b)** your acknowledgement of receipt of and your agreement to the terms and conditions of the current form of our standard Merchant Solutions Agreement, and
   - **c)** your agreement to ensure that your employees and agents comply with this Agreement and to be responsible for their compliance with the provisions of this Agreement.
6. License. This software is licensed to you for your personal, revocable, non-transferable, non-exclusive use in machine-readable form under the terms and conditions of this Agreement. You may only use the software at one location, on one computer and with one terminal having one terminal identification number.

   You may not:
   - copy, reproduce, sell, transfer or make available any copies for resale of the software or transfer the software
   - electronically from one computer to another or make it available through timesharing service, network of
   - computers, retrieval system, other multiple user arrangements or any other form of transmission of the software
   - modify, translate, reverse engineer, decompile, disassemble or create derivative works based on the software
7. Title. All right, title, interest and intellectual property in and to the software and all documentation, code and logic which describes or comprises the software belong to us and/ or our supplier. You acknowledge that the software constitutes valuable property and trade secrets belonging to use and/ or our supplier and embodies substantial creative efforts and confidential information. You agree to take all measures necessary to keep the software confidential.
8. Software Copies. Any additional copies of the software must be purchased from us. You agree not to make any copies of the software.
9. Use of Software. You may use the software solely for the purpose of processing your own data. Data and reports generated by the software shall not be duplicated for the purpose of resale.
10. Your Systems. Your systems will remain your responsibility. It is your responsibility to maintain proper security and working conditions. It is your responsibility to ensure that your systems are and remain compatible with the software. We are not responsible if the software causes your systems to become obsolete, require modification or repair, or otherwise effect performance of your systems. If you are using

a TCP/IP connection, you must install a commercially available firewall software or commercially available appliance. The firewall must be configured to block internet access except to a limited number of known, trusted and reputable website required for use in the ordinary course of your business.

11. Fees. You agree to pay us a fee for the software which we may deduct from your bank account or amounts due to you pursuant to the Merchant Solutions Agreement.

12. Limited Warranty. We warrant to you the disks on which the software is recorded to be free of defects in material and workmanship under normal use for a period of ninety (90) days from the purchase date. Our only liability for any breach of this warranty shall be, in our sole discretion: (I) to replace your defective software; or (ii) to advise you how to achieve substantial functionality of the software through a different procedure; or (iii) if the above remedies are impracticable, to refund the fee you paid for the software. Repaired, corrected, or replaced software shall be covered by this limited warranty for the period remaining under this limited warranty. You must inform us of your problem with the software during the applicable warranty period. If any modifications are made to the software, except by us or our agents, during the warranty period, if the software is subjected to accident, abuse, or improper use, or if you violate the terms of this Agreement, then this warranty shall immediately terminate. This is a limited warranty, and it is the only warranty made by us or our suppliers.

13. DISCLAIMER AND EXCLUSION OF WARRANTIES. WE DISCLAIM AND EXCLUDE ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE, THE SERVICES ASSOCIATED WITH THE SOFTWARE, AND ANY MANUALS. THE SOFTWARE, THE SERVICES ASSOCIATED WITH THE SOFTWARE, AND ANY MANUALS ARE PROVIDED SOLELY ON AN "AS IS" BASIS. THE ENTIRE RISK ARISING OUT OF ANY USE OF THE SOFTWARE, THE SERVICES ASSOCIATED WITH THE SOFTWARE, AND ANY MANUALS REMAINS WITH YOU.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, TORT, CONTRACT, OR OTHERWISE, SHALL WE OR OUR SUPPLIERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES.

IN NO EVENT WILL WE OR OUR SUPPLIERS BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT WE RECEIVED FROM YOU AS A FEE FOR THE SOFTWARE, EVEN IF WE WERE INFORMED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM OF ANY THIRD PARTY.

THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

14. No Refund. No refund will be given for a software package that is already opened or installed.

15. Term and Termination. This Agreement is effective until terminated by either party at any time. This Agreement shall terminate immediately and automatically if the Merchant Solutions Agreement is terminated. Upon termination, you agree to cease using, return all original and destroy all copies of diskettes, software and manuals, including copies in computer memory or copies in any other form. You will not have any rights to seek any refund, claim or damages for termination.

16. Exclusivity. You agree to exclusively use our services, or our authorized agents, for any support, training, assistance or repair with respect to the software.

17. Software Revisions. We, or our suppliers, reserve the right to make changes or updates from time to time in the performance or contents of the software and any manuals without obligation to provide you or notify you of such changes.

18. Responsibility for Use of Software, Terminals and Passwords. You acknowledge that the software, terminals and/or passwords may result in loss or damage to you including by effecting debits to your bank account. You acknowledge that there may or may not be passwords to access the software and if there is a passwords feature you acknowledge that the passwords feature may not be activated. We are not responsible for any software passwords, if there is no software passwords feature or if any

software passwords feature is not activated or does not operate. You further acknowledge that the failure to balance your transactions daily by means of “Store Close” procedures required in the software manual increases the likelihood that you will not detect unauthorized use and you may thereby suffer further losses or damages. It is your responsibility to take such steps as are necessary or advisable in order to keep secure and prevent unauthorized uses of the software, terminals and/or passwords. In any event, you agree to be liable for the full amount of all authorized and unauthorized activity resulting from the use of the software, terminals and/or passwords.

19. Indemnification. You agree to indemnify and hold us harmless from and against all clams, suits, damages, losses, fines, penalties (including fines, penalties and other charges by a Card Association), costs and expenses (including legal fees) incurred directly or indirectly by us or a third party arising from (i) your failure to comply with this Agreement and (ii) any failure by you, your employees or your agents to use the software in accordance with the provisions of the Agreement, the Merchant Solutions Agreement, any manuals and procedures.

20. Procedures. We may, from time to time, issue directions in writing regarding the procedure to be followed in carrying out this Agreement and such directions shall be binding upon you unless you elect to give immediate notice of cancellation of this Agreement.

21. Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario and the laws of Canada applicable thereto. A suit may only be brought in the Province of Ontario, Canada.

22. Headings. All section headings are included solely for convenience and do not affect interpretation of this Agreement.

23. Assignment. We may assign this Agreement or any obligations under this Agreement. You agree that this Agreement will be binding on your heirs, successors and assigns, provided however that you may not assign this Agreement without our written consent.

24. Waiver. Any waiver by us of the provisions of this Agreement shall not constitute a waiver of any other provision (whether similar or not), nor shall such waiver constitute a continuing waiver of that particular provision unless we expressly provide a continuing waiver in writing.

25. Entire Agreement and Amendment. This Agreement and the Merchant Solutions Agreement constitute the entire agreement between you and us with respect to the subject matter hereof and cancels and supersedes any prior understandings and agreements with respect to the subject matter hereof. We may amend this Agreement by providing you with notice.

Call Centre Information

Please call the TD Merchant Solutions Help Desk 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

Documentation Portal

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/posresources.