# ePayment Procedures for Collecting, Processing and Disposing Cardholder Data

**Revised January 2016**

## General

1. Collecting, processing and disposing of sensitive cardholder data is restricted to staff members whose roles place them in a position where a customer would expect them to collect such data.
2. Do not store cardholder data unless it’s absolutely necessary for business operations. Transient storage of cardholder data should be in a safe and secure area and access must be restricted to authorized staff only. The transient storage procedures documented below must be followed.
3. Do not transport cardholder data unless it’s absolutely necessary. Transport of cardholder data should be conducted in a safe and secure manner and restricted to authorized staff only. The transport procedures documented below must be followed.

## Collection

1. Only Authorized staff are permitted to collect cardholder data and only via the following methods:
* Post Mail
* Telephone: Merchant must not record phone calls and/or must not obtain sensitive credit card information via voicemail
* Regular Fax:
	+ Must be a regular, standalone machine using a dedicated line.
	+ Must not be network based; it cannot send to server or email out
	+ Appropriate access control must be in place to restrict access to the fax machine
* In person
1. Collection of cardholder data is not permitted through any other methods such as email, voicemail, instant messaging and so forth
2. Authorized staff:
* Must be authorized by Merchant account owner and ePayment
* Such staff must complete VT training to ensure safe and secure handling of cardholder data

## Designated Official Forms Only

1. Use designated official forms only to collect cardholder data.
2. If cardholder data is obtained over the phone or in person, authorized staff should process the payment immediately. Do not record cardholder data on forms unless it is absolutely necessary.
3. The authorized staff may only collect the minimum necessary data to process the payment. Do not collect 3-digit card verification code.
4. Forms must be clearly marked as confidential and numbered so it’s easy to detect if one or more are misplaced.

## Transient Storage and Access

1. Electronic storage of sensitive cardholder data is never permitted, for example, email, excel spreadsheet, word document, or other electronic software
2. If temporary storage is necessary, forms must be stored in a safe and secure storage at all times until they are ready for processing.
3. Access to the secure temporary storage must be restricted to authorized staff only.
4. Keep track of the number of forms stored at all times.
5. Forms must be in a folder/binder/envelope that is clearly labeled confidential.
6. The time between storage, access, retrieval and destruction must be kept to an operational minimum to reduce risk.
7. Always ensure that the storage is not broken and the forms are not stolen or misplaced.

## Transport of Forms

1. If transport of forms is necessary, it must be done in a safe and secure manner.
2. The transport process must be reviewed and authorized by Merchant account owner and ePayment.
3. Staff members need to keep track of the number of data cards/forms at all times.
4. The forms must be in a folder/binder/envelope that is clearly labeled confidential, and the folder/binder/envelope must be kept in a secure purse, briefcase, or backpack that is to remain with the authorized staff at all times during the transport.
5. The travel must be kept to an operational minimum to reduce risk.
6. A log sheet must be created to keep track of the following information and must be provided during spot audit request:
* # of data cards/forms prior to transport
* # of data cards/forms after arrival
* source and destination address
* departing and arrival time
* authorized staff member that is transporting the cards
* approval of Merchant management
* purpose of transportation

## Processing

1. Only authorized staff can process payments on behalf the customers.
2. All virtual terminal transactions must be processed on designated PCI-compliant Virtual Terminal computer only.
3. Processing of virtual terminal transactions on any other computers is not permitted, or your unit would be deemed non-compliant.
4. Designated PCI-compliant Virtual Terminal computer is required to be setup in a secure location, with access restricted to authorized staff only and identified with a sticker.

## Disposal

1. Cardholder data must be disposed immediately after payments have been processed. If the designated form also collects customer order information that need to be kept for future reference then must cut out the cardholder data portion of the form to destroy.
2. You must ensure that the disposed data cannot be recovered. For example, if you are shredding the forms, make sure you are using a cross cut shredder (straight cut shredders are not acceptable).

## Audit

1. ePayment may conduct a spot audit to verify if the procedures are followed consistently
2. Non-compliance of ePayment procedures may result in revocation of the use of the Virtual Terminal and/or closure of the ePayment account.