Administrative Policy

1 Policy

1.1 This policy applies to all OPTIONS employees. The policy also pertains to all departments that process credit cards, including: transmitting or handling cardholder information. The cardholder information may be in a physical or an electronic format.

1.2 All transactions that OPTIONS processes must meet the standards outlined in the policy.

1.2.1 Electronic credit card numbers should not be transmitted or stored on a personal computer or e-mail account. Electronic lists of customer's credit card numbers should not be retained. Credit card information should only be accepted by telephone, mail, or in person. This information should not be accepted via e-mail and departments should not e-mail credit card information.

1.2.2 Physical cardholder data must be locked in a secure area. Access should be limited to individuals that require the use of the data. Access should also be restricted on a 'need to know' basis.

1.2.3 Only essential information should be stored. The Card Validation Code (also known as the Security Digits, V Code, or CID); users PINs or the full data from a cards magnetic strip are not to be stored.

1.2.4 Credit card information is to be retained for the time needed to process, or if retained for reconciliation, for a maximum of 3 months.

1.2.5 Credit card information, if it does not need to be retained, should be destroyed. Information should be destroyed by shredding immediately after processing, or immediately after it no longer needs to be retained.

1.2.6 Credit card receipts may only show the last four digits of the credit card number. If receipts show more than the last five digits, the receipts must be shredded or retained in a secure area.

1.2.7 Exceptions to the policy may be granted by the CEO or CFO.

1.2.8 External scans by an approved PCI scan vendor are required to be run on a regular basis.

1.2.9 Employees who handle credit card accounts are to be made aware of security policy and cardholder information practices upon hire and at least once a year thereafter.

1.2.10 Upon discovery of a cardholder information breach, OPTIONS will immediately contact NPC/Retriever Systems and First Data to report the incident.

1.2.11 The CFO has been designated as the Security Administrator has been assigned to ensure that the policy and security practices of OPTIONS are enforced and updated, as needed.

General Precautions:

- Do not disclose or acquire any cardholder information without the cardholder's consent.
- Keep all cardholder numbers and information secure and confidential and limit access to the minimum number of employees.
- Cardholder data cannot be stored in any fashion on computers, networks or related media.
- Payment card numbers must not be transmitted via email.
- All documentation containing card account numbers must be destroyed in a manner that will render them unreadable after their useful life (12 months) has expired.
- Procedures should be reviewed by the Department Manager on an annual basis and submitted to the CFO along with other required PCI compliance documentation.
- Annual update of Merchant Information including current contacts is required.

Over the Counter Transactions

- Verify signature of cardholder at the time of the transaction.
- Obtain the signature of the cardholder on the receipt and provide the duplicate copy to the cardholder.
- Be sure only the last four digits of the card number are printed on the

receipt.

- Store the merchant copy of the receipt safely until it is needed for end of day balancing.

- Keep all receipts for each day together. Compare them to daily totals and then group them with the daily batch settlement tape for storage/reference purposes.

- If for any reason the terminal does not work, use the sales drafts. Get an imprint of the card, write a description of the transaction, the transaction date, and the dollar amount on the draft. Also write the merchant name on the sales draft. Be sure to have the cardholder sign and give him/her a copy of the draft. Hand enter the information when the terminal is up and running again. Keep the original copy of the sales draft in case a retrieval request is received.

Mail-in, Fax and Phone Orders

- Maintain a payment listing for balancing and accounting purposes but this listing should not contain the cardholder data –the last four digits of the card number may be listed.

- Fax machines should be located in a nonpublic area where access is limited to trained employees.

- Documents with the card number and other cardholder data should be processed promptly and then safely stored until needed for balancing the day's transactions.

- Keep all receipts for each day together. Compare them to daily totals and then group them with the daily batch settlement tape for storage/reference purposes.

- Record the batch total and batch number for each day in the monthly summary report.

POLICY DATE: March 2008
REVISED: May 2012
REVISED: April 2014
REVISED: October 2015
REVIEWED: October 2018
REVIEWED: November 2019
REVISED: November 2020

REVIEWED: January 2022
March 2023