

Paypoint® Verifone Tranz330 Terminal
Users Guide (cont.)

Fraud Prevention

Debit

Here are two steps merchants can take to prevent debit fraud:

- 1.) Advise your customers to keep their PIN (secret code) a secret. Never let your cashier enter a customer's PIN number.

- 2.) Always give customers their debit receipt, or dispose of it safely so that unauthorized use cannot occur.

Credit

On the PayPoint system, merchants can do credit card on-line authorizations for any amount. Off-line authorization is handled by calling the credit card center, then keying in the transaction when back on-line with PayPoint. Merchants should try to key in the transaction the same day as authorization is obtained. This is the recommended procedure to avoid chargebacks to merchants.

Here are some steps merchants can take to reduce the possibility of credit card fraud and chargebacks:

- 1.) Ask for a second piece of photo I.D. (recommended by PayPoint).

- 2.) Compare printed account number on receipt to embossed number on card (required by credit card company) [Note: Counterfeit cards represent one of the most common types of credit card fraud. Counterfeiters re-encode the magnetic stripe so the "encoded" account number is different from the "embossed" account number that appears on the front of the card. Using the VeriFone 250 printer will show the account number encoded on the card's magnetic strip, which can be matched with the number on the receipt with the embossed number on the card. You can also match the card number on the Tranz 330 terminal display with the embossed number on the card.]

- 3.) Compare signature on card to signature on receipt (required by credit card company).

- 4.) Check expiration date on card. Do not accept expired cards.

- 5.) Check for the hologram on the face of the card. Do not accept cards without holograms.

- 6.) Keep tight security on manager's code number.

- 7.) Carefully maintain receipts so that they can be produced when requested (banks request the original copy of receipt).

- 8.) Replace printer ribbons often, so that the receipts are easily read and copied.

- 9.) Carefully tear off receipts, so that all required sales information appears on each receipt.
- 10.) Depositing credit card receipts for any business but your own is called "factoring" and is against the law. This can result in chargebacks, the loss of your credit card business and even criminal penalties.
- 11.) Watch customers for signs of potential credit card fraud, such as:
- a.) Credit card is pulled out of a pocket rather than a wallet.
 - b.) Credit card is not presented because merchandise was previously ordered by telephone. Tell customers ordering by phone to bring their credit card when they pick up their merchandise.
 - c.) Customer distracts the salesperson during the transaction.
 - d.) Rapid purchases are made without regard for price, size, color or style.
 - e.) Many small purchases are made instead of one large purchase to avoid the floor limit rule.
 - f.) Customers may ask salesperson to split up their purchases into two sales drafts in order to get around the floor limit rule. This is a violation of credit card regulations and your Merchant Agreement and could result in a chargeback. The merchant is always liable if these split sales are investigated.
- 12.) If you suspect fraud, call the credit card Authorization Center and say that you have a "Code 10" authorization request, then follow the operator's instructions. Do not keep a customer's card if it means putting yourself in danger.