Protection for Cardholders

Offering Protection -- To protect Providence and our customers who offer bankcards as payment, all workforce members who have access to credit card information are responsible for protecting that information.

Cardholder information includes:

- Primary Account Number (PAN)
- Cardholder name
- Expiration date
- Service code (the 3 or 4 digit number on the back of the card used for authentication)

Credit card information is confidential. To protect this information follow these three cardinal rules:

1. When you are working with a customer never leave the card unattended.
2. Do NOT store cardholder information.
3. Never send or request Primary Account Numbers (PAN) by email.

Make your point of sale area secure by following these precautions:

- **When not in use lock any point of sale device** such as a laptop, mobile payment device or tablet.

- **Secure files and equipment** before leaving a work area by signing off of a computer or POS system, and physically securing files and hand held payment devices in locked drawers or cupboards.

- **Do not record** a cardholder’s security code on paper or store it on the computer.

- **Check for criminal activity** -- Criminals are illegally accessing POS devices to steal cardholder data.
  
  - Regularly check swipe devices for damage.
  
  - Check for signs of altered or damaged cords or cables, additional stickers or labels, or new pieces of hardware plugged into the device. These could be signs of tampering.
  
  - Carefully check your area for hidden cameras or recording devices.

- **Limit access to POS equipment.** Unauthorized individuals are never allowed access to the POS equipment. Contact your manager if you have an unexpected request.
Fight Fraud at Every Transaction

Processing cards at point of sale
Swipe the card stripe for payment authorization and hold on to the card during the transaction to check the card security features.

Card Security Features
- The first digit should always match the designated card brand
  American Express – 3, Visa – 4, MasterCard – 5, Discover - 6
- The four digit number printed below the first four digits embossed on the card should be identical
- Check the expiration date
- Check the signature panel. The words “Authorized Signature” or “Not Valid Unless Signed” appears above, below, or beside the signature panel.
- If the card doesn’t read when swiped there could be a problem with the magnetic stripe. If the card appears authentic, use the terminal’s manual override feature to key-enter transaction data for authorization.
- Match the signature on the card with the customer’s signature on the receipt. If the card is not signed ask for ID with a signature (e.g. driver’s license) and check against that signature.

Approval of the transaction
**Declined** -- Never accept a transaction on a card that has been declined. Return the card and instruct the cardholder to contact the card issuer for more information.

**Need more information** -- If the card issuer needs more information call the authorization center and follow the instructions given.

**Pick up Card** -- If the card issuer message is to ‘Pick up Card’ say the card has been declined and return the card to the cardholder.

If you think there may have been a breach in the security of credit card information, regardless of whether or not you are directly involved, **alert your supervisor immediately as well as the Providence Operations Center**. Examples of stolen or lost materials include credit cards, daily credit card terminal tapes, and computer files containing cardholder data.

Signed______________________________________   Date__________________