Proper Card Acceptance procedures must be followed at all times to avoid or mitigate the risk of potential fraud-related chargebacks

- IF – Terminal is Chip & PIN ready and the cardholder has a Chip & PIN preferring card, merchants must insert the card and obtain a ‘Verified by PIN’ transaction that is fully authorized (no decline or refer response).

- IF – Chip & PIN technology fails, merchants must swipe the card. The merchant must obtain a valid authorization and the cardholder’s signature, or he or she will be liable for fraud-related chargebacks if the transaction is disputed.

- IF – Chip & PIN technology fails AND card swipe fails, key in the card number and obtain a valid authorization. A manual imprint of the credit card and the cardholder’s signature are required, or the merchant will be liable for fraud-related chargebacks if the transaction is disputed.

- IF – Terminal is Chip & PIN ready and the card is a Chip & Signature card, merchants must insert the card and obtain a valid authorization and the cardholder’s signature on the transaction receipt.

- IF – Terminal is Chip & PIN ready and the card is a non–chip card (magnetic-stripe only), merchants must swipe the card and obtain a valid authorization and the cardholder’s signature on the transaction receipt.

- IF – Terminal is Chip & PIN ready and the cardholder has a Chip & PIN preferring card but forgets the PIN or PIN is locked and the PIN attempt fails, merchants must advise the cardholder to contact their Card Issuer, or ask for another form or payment.

- IF – Chip card is removed from the device before the transaction is finished, merchants must re-insert the card and obtain a “Verified by PIN” transaction that is fully authorized.

- IF – Terminal is NOT Chip & PIN ready and the card is Chip & PIN preferring, merchants will be liable for fraud-related chargebacks, even if proper card acceptance procedures were followed.

- IF – Merchant is experiencing system failure, downtime procedure for credit cards MUST be followed. Debit cards cannot be accepted during downtime.

For any questions or concerns, call 1-866-319-7450, available 24/7
Chip & PIN Transactions
- The card is inserted into a Chip & PIN ready terminal, instead of being swiped.
- The card remains inserted in the terminal throughout the transaction.
- The terminal will display the purchase amount and request the cardholder’s PIN.
- The cardholder will enter his or her PIN on a keypad.
- If the PIN is confirmed and the purchase approved, a receipt will be printed.

Magnetic-Stripe Transactions
- For all non-chip, card present transactions, the card must be swiped.
- Swipe the card once and in one direction only.
- Enter the correct amount to be authorized and verify the authorization response.
- Obtain the cardholder’s signature.

For merchants who are not Chip & PIN ready, swiping a chip card does not provide protection from fraud-related chargebacks under liability shift rules

Key-Entered Transactions
The chip and magnetic stripe are active components of the card’s security that makes manual processing appropriate ONLY when a card’s chip or magnetic stripe cannot be read. Key-entered transactions are considered high-risk and may result in chargebacks.

- At the POS terminal you must:
  - Manually key enter the card number.
  - Enter the sales amount and valid expiry date.
  - Verify the authorization response.
- On the POS terminal receipt you must:
  - Print “PROOF COPY” on the signature line.
  - Record the pre-printed reference number as it appears on the manual sales draft.
- A manual sales draft that includes all of the following must also be completed:
  - Date
  - An imprint of the card
  - Details of the transaction
  - Dollar amount
  - Customer signature
  - Authorization Number/Code
  - Merchant name, address and merchant number
  - Do not write “void” or “copy” on the face of the manual sales draft.

For merchants who are not Chip & PIN ready, an imprint of a chip card does not provide protection from fraud-related chargebacks under liability shift rules.

Downtime Procedures (Credit Card Only)
- If amount is greater than your assigned floor limit, call Moneris for a voice authorization: 1-866-802-2637.
- Take a manual imprint of the credit card and obtain the cardholder’s signature on the manual sales draft.
- When system/service is restored, force post the transaction on the electronic POS terminal using the assigned authorization number.
- Ensure that all of the information is clearly visible on the manual sales draft.