PCI COMPLIANCE AT THE POINT OF SALE

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements created to protect sensitive cardholder data wherever it is processed, stored, or transmitted.

As someone who handles cardholder payments, you play a significant role in the security of that data. Here are some tips to help you manage your part in securing PCI DSS compliance:

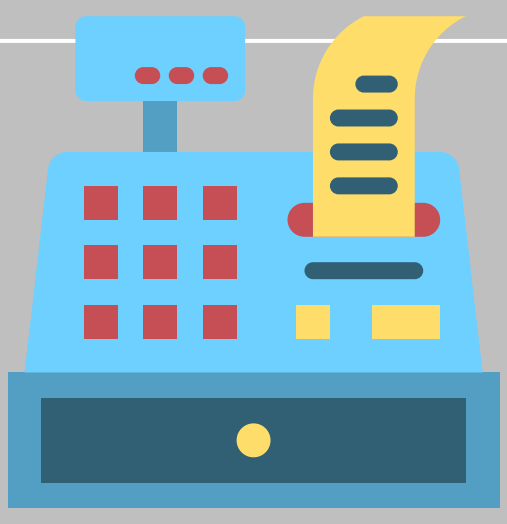
1) EXAMINE PAYMENT CARDS

Each time you are given a payment card, take the time to ensure the card is not stolen or forged. Never accept a card if:

- The cardholder name is different than the customer's ID
- The card looks warped or blurry, or the text is slanted
- The spacing of embossed numbers is uneven

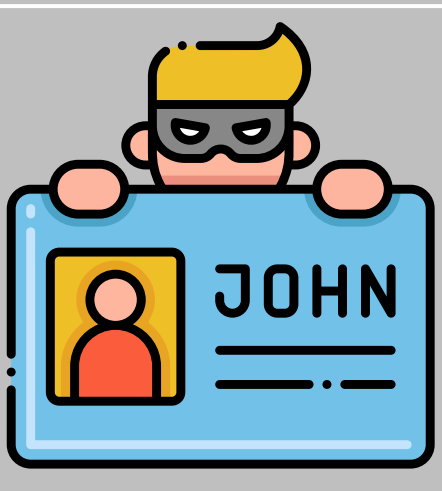
2) PROTECT EQUIPMENT

- Do not allow non-employees behind the Point- of-Sale (POS) or into secure rooms.
- Never connect the POS system to an alternative network without receiving authorization.
- Check POS terminals for signs of tampering.



3) REMOVE SENSITIVE DATA FROM RECEIPTS

- Receipts should always mask a payment card number except for the last four digits.
- Never write down a cardholder's information.
- Confirm that any documents with full card numbers are destroyed.



4) PREVENT INSIDER THEFT

Keep an eye out for any suspicious behavior, such as:

- The unauthorized use of a device
- Writing down cardholder information
- Accessing protected areas without authorization
- Installing unauthorized software

5) REPORT INCIDENTS

If you are unsure whether or not to report an incident, report it. Leadership and your organization are only able to act once they are alerted to any issues. Quick action can help to mitigate negative impacts.