

FRAUD PREVENTION

MORE PREVENTION. LESS FRAUD.

TWO WAYS TO MAKE POINT-OF-SALE EQUIPMENT SECURE

The point-of-sale terminal should be secured by using the support or the steel wire cable or better yet, a combination of the two. Merchants are encouraged to equip every place of business with at least one terminal that is adapted for use by individuals with limited mobility.

1 SECURE SUPPORT

The secure support helps prevent PIN-pad and terminal theft and also reduces the risk of other types of fraud at the point of sale. By using this type of device, you will also provide customers with a secure environment in which to process transactions.

A quick look at the benefits!

- The support is equipped with a side-plate to conceal PIN entry, thus providing customers with an added security feature. The rotating support base or top lets your customers turn the terminal as needed.
- The support is made up of robust, durable and non-flammable materials, thereby providing an added level of safety. The fastening mechanism ensures that the equipment is held solidly in place and protects it from being stolen.
- Thanks to the security device, you may remove the terminal from its support for any technical service call. Make sure to properly check the technician's identity before allowing him to handle the equipment.

2 STEEL WIRE SECURITY CABLE

This locking system also offers good protection and may be custom made. The cable gives added handling flexibility for customers while also serving as a very efficient deterrent for potential fraudsters.

A quick look at the benefits!

- The aviation-type cable is very sturdy and highly resistant.
- The cable is secured under the counter via a strong, fixed latch that can be used on any type of surface.

 For a list of security accessories providers, call Business Customer Service at **514-397-4450** or **1-888-285-0015**.



Payment and Financing Solutions

Desjardins Card Services



Desjardins

ADOPT BEST PRACTICES FOR FRAUD PREVENTION

RECOGNIZE SUSPICIOUS BEHAVIOUR

- Compare the signature on the receipt with the one on the credit card.
- If you have doubts about the transaction (large purchase or unusually large quantity of goods), ask to see two pieces of identity, including one with a photograph.
- Compare the signature on the identity cards with signature on the credit card and receipt.
- Be especially vigilant when a customer tries to distract you or pressures you to complete the transaction.

STEPS TO TAKE WHEN SUSPECTING A FRAUDULENT SITUATION

- If you can do so safely, hold on to the customer's card.
- Call your authorization center at 1-800-361-8120 and ask for a "Code 10" authorization.

BE WARY OF UNUSUALLY HIGH WITHDRAWAL AMOUNTS (PURCHASE-WITHDRAWAL)

- Set a maximum withdrawal amount on debit card transactions. Only debit cards can be used for this type of transaction, as cash withdrawal is not permitted with credit card purchases.
- Take note of situations where a customer purchases an inexpensive item and wishes to withdraw a significant amount of cash. This is often a fraud tactic.

WATCH OUT FOR PURCHASES MADE USING PREPAID CARDS*

- The ultimate safeguard is to cross-check the number on the receipt generated by the transaction with the corresponding part of the prepaid card number. This should be done for every transaction.
- For all purchases that exceed \$200, the legitimacy of the card must be confirmed by contacting the issuing financial institution.

REMEMBER TO CHANGE THE ADMINISTRATIVE PIN

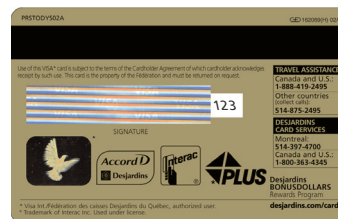
- On a quarterly basis, change the administrative PIN for the store's payment solution that processes sensitive transactions such as refunds, and restrict use of the PIN only to those in charge. The administrative PIN must be changed immediately every time there is an employee termination, and the code must be kept confidential.

DETECT COUNTERFEIT CARDS BEFORE ANY TRANSACTION BY IDENTIFYING THE MAIN SECURITY FEATURES



The card must contain the embossed account number, expiration date, VISA or MasterCard

brand mark and hologram as well as the four digits printed below the card number that must match the first four digits of the embossed number. Check for signs of chip tampering.



The back of the card must have a signature panel with no signs of tampering such as scratching, white tape or

white correction fluid applied over the panel. The repeated word "void" appears if the panel has been erased or compromised. Finally a 3-digit Card Verification Value 2 (CV2) appears on the signature panel or to the right of it in a white box.

Thanks to your vigilance, you can protect your business from fraud and offer your customers a more secure shopping experience!

*Prepaid card issued by a financial institution, using the international payment network identified on the card.

For more information, call Business Customer Service at 514-397-4450 or 1-888-285-0015.