# Fraud Prevention at your Point-of-Sale

Best practices to help protect your business against fraud.

While chip technology provides your business with enhanced security, fraud resulting from skimming can still occur. Skimming refers to the fraudulent practice of capturing account information from the magnetic stripe of a credit or debit card in order to make a counterfeit payment card.

While fraud can occur in different forms, it can be prevented by implementing appropriate best practices.

- Know and educate your employees You and your employees are the first line of defense against fraud. Be sure to implement strict hiring procedures to thoroughly screen potential candidates as fraudsters may attempt to join your organization. Fraudsters may also approach your employees to assist them with illegal activity. Train employees how to recognize the signs of possible fraud, and provide them periodic reminders to stay alert to potential threats. In addition, restrict access to your point-of-sale device(s) to authorized employees only.
- Avoid manual payment card entry Fraudulent payment cards often cannot be inserted or swiped at the point-of-sale device. Your customer may ask (or your employee may offer) to key in the payment card number manually. Doing this may bypass the payment card anti-fraud and security features. Always use the point-of-sale device to insert or swipe the payment card. If the payment card cannot be read, ask the customer for another form of payment.
- Do not accept letters of authorization Fraudsters may present a letter claiming to be from the cardholder authorizing use of the payment card by another person. Because only a cardholder — the owner of the payment card — is the authorized user, letters of authorization should be declined as a form of verification.
- Contact the payment card issuer When in doubt, do not hesitate to contact the payment card issuer. You may do so by using the contact information listed on the back of the payment card and request an authorization number. Contacting the payment card issuer protects both you as the merchant and the cardholder. Please note that obtaining the authorization number may only confirm that the funds are available on the payment card - this does not validate the cardholder authorized the transaction or prevent a future chargeback.
- Know and protect the point-of-sale device Skimming is the process fraudsters use to access information on the magnetic stripe of a credit or debit card when it is swiped at the point-of-sale. Usually this requires an attachment to the point-of-sale device to skim the payment card. To prevent this, ensure you are familiar with the point-of-sale device and its operation. Keep


PIN pads out of sight when not in use and inspect and secure standalone point-of-sale devices at the end of the business day. If you suspect the point-of-sale device has been tampered with, please contact RBC Royal Bank and your local law enforcement immediately prior to resuming accepting credit or debit cards.

- Keep accurate records of your transactions Some legitimate cardholders make authorized purchases, only to dispute the charges later in an attempt to defraud the business. To help prevent this type of fraud, keep accurate records of your transactions. At a minimum, you will need to keep copies of transaction receipts as evidence you received the authorized approval.
- Look out for payment card security features Ensure that the payment card presented by the customer bears the standard symbols and marks by carefully reviewing the security features of the payment card. In the event the payment does not process by inserting or swiping the payment card at the point-of-sale device, you may choose to enter the payment card information manually on the device. To minimize your risk, you must ensure to obtain a manual imprint of the payment card as evidence that it was presented. The imprint needs to be clear and legible on all copies of sales drafts with a record of the date, authorization number, the amount and the customer signature.
- Be aware of customer purchases Fraudsters have been known to purchase multiples of the same expensive items, often by selecting them quickly, without consideration as to sizes, colours or price. Another potential sign of fraud may be if the customer wants an expensive rush delivery to a new address not connected with their payment card.

**To sign up for RBC Merchant Services today, contact our team at 1 888 847-5803 or visit your nearest RBC Royal Bank branch.**

## Disclaimer