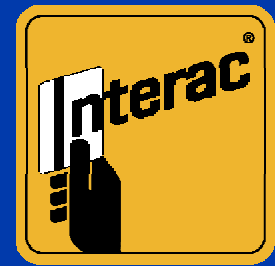




Project PROTECT

Debit & Credit Card Fraud For Owners and Managers of Retail



Police officers will meet with your employees in an effort to make them more aware of the problems related to payment card fraud and to elicit their co-operation in efforts to stop this type of fraud.

The police are seeking your assistance and active participation in this project through supervision of your employees. We also ask your help in ensuring that your customers are comfortable following the necessary steps for a debit or credit card payment.

INTEGRITY CHECKS

Please conduct regular and thorough integrity checks of the point of sale PIN Pad and other vulnerable areas within your premises. These checks will help detect any unauthorized equipment or tampering and will reduce the potential installation of card skimming equipment. Integrity checks must be recorded. A checklist will be provided.

SUPERVISION OF EMPLOYEES

Please ensure that all of your employees, present and future, are familiar with "Project Protect". This will ensure they are aware of the consequences of debit/credit card fraud and the various approaches a fraudster may take.

- Verify at the end of every day/shift

the serial number of your PIN Pad (located at the back of the device) to ensure it corresponds to the original number. Fraudsters will often come at the end of the day/shift to "switch" the PIN Pad with a fraudulent one.

- In the event that your PIN Pad has been "switched", tampered, stolen or is not functioning, immediately advise your manager and Service Provider.
- If you notice unusual amounts of cash during a shift, as compared with credit and debit transactions, this may signal a dummy terminal has been installed at your station.
- If you have any doubts, review your surveillance tapes to detect any unusual activity. You may discover that a new employee is skimming cards. Additionally, it may reveal if this new employee had the intention of skimming cards.
- Ensure that you receive proper identification from all persons applying for work. Take necessary

steps to verify the identification. Ask for and thoroughly verify references. Many fraud artists use false identities and provide no references upon being hired. After skimming customer cards, they quit employment. You can discourage most fraud artists by verifying their identity, address and other legitimate information.

Your co-operation and participation in this project is very important. So is the trust in both customers and employees. Rewards can be given to employees who report information concerning the location of skimming equipment or information on persons engaged in this activity (e.g., Crime Stoppers). Information on this activity is welcomed by the police. Please contact the police service in your area and ask for the criminal investigation unit responsible for fraud occurrences.

*Thank you
for your co-operation!*

FOR MORE INFORMATION ON PROJECT PROTECT PLEASE CONTACT WINNIPEG POLICE SERVICE AT 986-6322

OR CALL CRIME STOPPERS AT 1-800-222-TIPS.

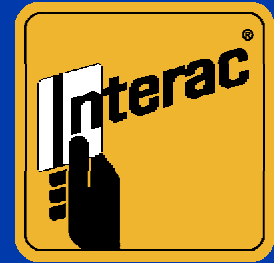
www.winnipegcrimestoppers.org





Project PROTECT

Debit & Credit Card Fraud For Employees of Retail Outlets



Police officers will meet with you and other employees in an effort to make you more aware of the problems related to payment card fraud and to elicit your co-operation in efforts to stop this type of crime.

WHY THIS MAY CONCERN YOU

If you are a clerk or cashier working in a place where purchases can be paid for by debit or credit card, YOU may be approached by people who will attempt to convince you to participate in a fraud scheme by:

- Providing you with a device used to record data on debit/credit cards; and/or
- Allowing them to install a device to record debit/credit card data.

THE FRAUDSTER'S APPROACH

The fraudster will:

- Conceal their true identity;
- Try to become your friend;
- Ask you to help them with their scam. They may even insist, if you refuse;
- Offer/promise you large amounts of money. Remember – false promises are NEVER kept;
- Tell you there is no risk involved, as no one will ever know what you have done. This is FALSE. Police and financial institution investigators will investigate and discover the roles of all involved persons in the scam; and/or

- Tell you that you will never be accused of fraud. This is FALSE. This activity includes offences of Fraud and Credit Card Forgery and Conspiracy to Defraud the Public. All are indictable criminal offences. A conviction for these offences can result in a fine and jail, can hurt your present and future employment, and can restrict your freedom to travel to other countries.

WHAT YOU NEED TO KNOW

- You take all the risks and the consequences. (Court, jail, criminal record.)
- Your honesty and integrity are essential to maintain the respect of your family, friends, and peers, as well as the trust of your present and future employers.

WHAT YOU SHOULD DO

- REFUSE to become involved in such a scheme;
- RECORD as much information as you can remember about the persons (e.g. physical description, licence plate number of vehicles);
- STAY within view of the security cameras. Fraud artists may try to speak to you in areas where they

think they cannot be recorded;

- NEVER give out your phone number, last name or home address;
- DO NOT be tempted by offers of large sums of money or bragging about easy cash;
- NEVER tolerate any personal threats;
- NOTIFY your employer; and
- NOTIFY police.

Your co-operation and participation in this project is very important. So is the trust in both customers and employees. Rewards can be given to persons who report information concerning skimming, location of skimming equipment, or information on persons engaged in this activity.

Information on this activity is welcomed by the police. Please contact Winnipeg Police Service and ask for the criminal investigation unit responsible for fraud occurrences – OR – call Crime Stoppers at 1 - 8 0 0 - 2 2 2 - T I P S . www.winnipegcrimestoppers.org