# PAYMENT CARD SKIMMING

The Commercial Crime and Fraud Sections with the Saskatoon Police Service, Regina Police Service, Saskatchewan Financial Services Commission, and the RCMP “F” Division have joined forces to promote March as Fraud Awareness Month to Saskatchewan residents and consumers.

During this third week of Fraud Awareness Month, the fraudulent activity to be profiled is payment Card Skimming.

Payment card skimming also referred to as skimming is the illegal copying of data contained on the magnetic strip of a credit or debit card. This is often done surreptitiously using Automated Teller Machines or Point of Sale (POS) terminals that fraudsters have compromised. With this information counterfeit cards can be produced. The fraudsters then use these cards to withdraw money from your account and/or make unauthorized debit or credit card purchases. Skimming has been and continues to be a problem around the globe and we are not immune. With the introduction of “chip cards” we are hoping skimming incidents will be reduced. However, until there is complete “chip” conversion the threat remains.

To help reduce your risk we advise people to always protect their PIN (personal identification number). Never lose sight of your card if providing it to a merchant to swipe. It takes only a moment for a fraudster, working embedded as an employee, to slide your card through a concealed skimming device. Do not use any ATM or POS terminal that appears tampered or altered. Check your financial statements carefully. It is helpful to have on-line banking which allows you to regularly check your account information. Any unusual or unauthorized transactions should immediately be reported to your financial institution. If a fraud is confirmed, report it to the police.

Fraudsters often target POS terminals as their first step in the skimming process. POS terminals that are easily accessible and not secured by the merchant in some manner are vulnerable. Typically, fraudsters need to remove a POS terminal for a period of time in order to insert the technology which allows the skimming to take place. Merchants should always try and use a supplementary method to secure their terminals. This can be achieved by attaching it to a platform, securing it with a cable, etc. This will eliminate or at least reduce the possibility of a fraudster being able to gain the control needed to compromise it. The importance of maintaining the security and integrity of these devices can not be overstated.

These are just a few tips to help prevent you from becoming a victim of skimming. Additional information on this and many other types of fraud can be found on various banking, police and Government websites. Be informed and reduce your chances of becoming a fraud victim.

For more information contact:

Detective /Sergeant Trent Emigh
Saskatoon Police Service
(306) 975-8243