

Card Skimming

Card skimming is costing Canadians over 400 million dollars annually. Credit and bank cards are usually skimmed when the legitimate card holder presents their card for retail transactions at businesses whose card reader equipment has been compromised. This happens when criminals have gained control of the card reader and have installed hardware designed to capture and store the data coded into the magnetic strip. The equipment is compromised by exchanging a real reader with a fake one. The stolen card readers have hardware installed to record the card holders PIN by installing a computer chip inside the reader and are then returned to the business. The criminals are then able to "read and write" these skimmed data onto counterfeit credit and bank cards, and use them make purchases or ATM withdrawals.

Until payment cards have more advanced security features you must make sure you are following the safety rules:

- a) Shield the PIN pad from view while entering the PIN
- b) Never share your PIN number with anyone else
- c) Review your account statements every month to verify all transactions

Contact your bank or Credit Card Company if you observe any problems on your account statement.

If you are a victim of card skimming, call Phone Busters. They are the central agency in Canada that collects information on scams including telemarketing, advance fee letters and identity theft complaints. Information collected by Phone Busters is forwarded to the appropriate agency.

Phone Busters
Box 686
North Bay, Ontario
P1B 8J9

1-888-495-8501
info@phonebusters.com

Please see www.ama.ab.ca for more information.