CANADIAN ANTI-FRAUD CENTRE BULLETIN

Bank Investigator 2025-06-27

FRAUD: RECOGNIZE, REJECT, REPORT

The Canadian Anti-Fraud Centre would like to warn Canadians about an increase in reporting related to the “bank investigator” scam. Fraudsters are impersonating financial institutions, law enforcement, Amazon and credit reporting agencies claiming that the victim’s bank account has been compromised.

In some cases, suspects provide some of the victim’s personal information which might include name, date of birth, phone number, address, Social Insurance Number (SIN) and debit card number to make the call seem legitimate. Additionally, suspects are spoofing financial institutions, law enforcement and credit reporting agencies’ phone numbers or are providing fraudulent call-back phone numbers which impersonate the institutions.

<u>Current variations of the bank investigator scam:</u>

1.) Victims receive an automated phone call claiming to be their financial institution, law enforcement, credit reporting agency (Equifax® Canada or Transunion) or, in some cases, Amazon advising that there have been fraudulent transactions in their account. Fraudsters will request access to the victims’ computer or device to continue the “investigation”. Victims are then shown a fraudulent transaction on their online bank account. The suspects state that they want the victims' help in an ongoing “investigation” against the criminals who stole their money and request that the victims send funds as part of the “investigation”.

    In some cases, fraudsters will add the victim as a “payee” with a fraudulent email address and advise that the victim must transfer a large amount of money in order to protect their account. The fraudsters will convince the victim that they have added funds to the victim’s account but, in reality, the funds were transferred from their line of credit or savings account.

2.) Suspects may have the victim’s debit card number and password but cannot access the victim’s account due to multi-factor authentication protection on their account. Suspects then proceed to contact the victim claiming to be their financial institution and will advise the victim that they must provide a code they receive via text message or email in order to confirm their identity. The code the victim provides is the multi-factor authentication code which gives the suspects full access to their bank account.

3.) Suspects will advise that they are required to retrieve the victim's debit or credit card from their residence as part of the investigation. Suspects will attend the victim's residence to pick up the card and they may even ask the victim to cut the card in half without damaging the card chip to make the call seem more legitimate. They may also threaten victims that they may be arrested if they do not cooperate.

Warning Signs – How to Protect Yourself

- Criminals use Call-Spoofing to mislead victims. Do not assume that phone numbers appearing on your call display are accurate.
- If you get an incoming call claiming to be from your financial institution, advise the caller that you will call them back. End the call and dial the number on the back of your bank debit card from a different phone if possible or wait 10 minutes before making the outgoing call.
- Credit bureaus will not randomly call you, unless it is a requested call back. If you receive an incoming call claiming to be from a credit bureau, advise the caller that you will call them back. Visit the credit bureau's website and contact the official phone number provided.
- These institutions or law enforcement will never threaten you over the phone.
- Don't share codes received via text message or email with anyone. In most cases, these are multi-factor authentication codes that will give fraudsters access to your account.
- Fraudsters will often provide the first 4 to 6 numbers of your debit or credit card. Remember that these numbers are used to identify the card issuer and are known as the Bank Identifier Number (BIN). Most debit and credit card numbers issued by specific financial institutions begin with the same 4 to 6 numbers.
- If your personal information has been compromised in the past through a breach or a phishing message, remember that the information can be used as a tool to make the communication appear legitimate.
- Never provide remote access to your computer.
- Institutions or online merchants will never request transferring funds to an external account for security reasons.
- Institutions or police will **never** request you to turn over your bank card nor attend your residence to pick up your bank card.
- Enabling Auto-Deposits for Interac e-transfers provides an additional layer of security.
- Learn more tips and tricks for protecting yourself.

Anyone who suspects they have been the victim of cybercrime or fraud should report it to their local police and to the Canadian Anti-Fraud Centre's online reporting system or by phone at 1-888-495-8501. If not a victim, you should still report the incident to the CAFC.