

CANADIAN ANTI-FRAUD CENTRE BULLETIN

Telephone Extortion : CBSA/SIN Scams

2021-10-20

FRAUD: RECOGNIZE, REJECT, REPORT

The Canadian Anti-Fraud Centre continues to see reports of telephone extortion scams. You may receive a fraudulent automated phone call pretending to be from a government agency, police or a business asking you to dial 1 to speak with an officer or an agent. Here are some variations to look out for:

New Variation Fraudsters may call claiming to be Canada Border Services Agency (CBSA). They try to make you believe that a package addressed to you was intercepted by Canada Post containing illegal substances. After asking you to dial 1 on the automated phone call, the scam is similar to previously reported Service Canada, Canada Revenue Agency (CRA) and RCMP telephone extortion scams described below.

- Fraudsters may call and tell you that your Social Insurance Number (SIN) is linked to fraudulent or criminal activity. In these cases:
 - Fraudsters will ask for personal information including your: SIN, DOB, name, address, and account balances. By providing your personal information to fraudsters you are at risk of identity fraud.
 - Fraudsters may also direct you to withdraw money from your bank accounts. Then ask 0 you to deposit it into a "safe account". In rare cases, suspects pose as police officers and present themselves at your house to pick up the money.
- Fraudsters pretend to be calling from government agencies, such as Service Canada, Department of Justice, Canada Revenue Agency, Government of Canada, and RCMP. They will ask you to provide or confirm your SIN or other personal information, resulting in identity theft.

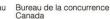
What you should know

- Fraudsters manipulate caller ID to display phone numbers starting with your area code. They • may also display the legitimate phone number of these agencies. This is called "Call-spoofing" and this technology is easily available.
- No government agency will contact you and tell you that your SIN is blocked. •
- Police officers will never present themselves at your residence to demand a payment.

How to protect yourself

- Never provide personal information over the phone to an unknown caller.
- Do not assume that phone numbers appearing on your call display are accurate.
- If you provide personal information, contact Equifax and Trans Union to place fraud alerts on your accounts.







- Be wary of automated calls asking you to dial 1 to speak with an officer.
- 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 <u>online reporting system</u> or by phone at 1-888-495-8501. If not a victim, report it to the CAFC anyway.