



CANADIAN ANTI-FRAUD CENTRE BULLETIN

Money Mules

2022-06-06

FRAUD: RECOGNIZE, REJECT, REPORT

Increasingly, fraud networks are recruiting unsuspecting fraud victims to receive and transfer money from other victims. When this happens, the victim becomes a money mule. With the sharp increase in reported frauds and the noticeable prevalence of money mules, the Canadian Anti-Fraud Centre (CAFC) wants to educate Canadians on the various frauds that utilize money mules, in addition to providing general awareness to prevent victimization.

What is a Money Mule?

A money mule is an individual who is recruited by fraudsters to serve as a middle person to transfer proceeds of crime funds. The mule may, or may not, be aware that they are a pawn in a larger network. When a mule moves money, it becomes difficult to identify the fraudsters from the victims.

The money is often transferred using bank wire transfers, email money transfers, money services businesses and virtual currencies. Typically, mules get paid for their services; receiving a small percentage of the money transferred. A money mule is used in the money laundering process, which is an offense under the [Criminal Code of Canada \(Section 462.31\)](#).

Variations of Money Mule Scams

Most reported scams to CAFC involve Money Mules at one point. The following scams are examples of how they work:

Job Scams

Victims are approached by suspects, most commonly, after posting their resume on a website. Job titles offered are often “payment processor” and “administrative assistant” among many others. Suspects will advise that your job duties include accepting payments from clients which are most commonly e-transfers or cheques. In most cases, victims will then be asked to keep a small percentage of the payment and send the remaining amount via Bitcoin. In many cases, payments received are from other victims and by transferring these funds to criminals you become a money mule.

Prize Scams

Consumers are solicited over the phone, via email, text message, social media and regular mail and are advised they are the winner of a large lottery or sweepstakes. Prior to receiving any winnings, the consumers will be asked to pay an upfront fee. Consumers often send the payments to victims of other scams who are found to be money mules.



Royal Canadian Mounted Police
Gendarmerie royale du Canada



Competition Bureau
Canada

Bureau de la concurrence
Canada



Ontario Provincial Police

Canada

Romance Scams

Victims often use various payment methods (Bitcoin ATM, wire transfers, money service businesses, cryptocurrency, gift cards, etc.) to send funds to the romance fraudsters. Victims don't realize that, in most cases, these funds are actually being sent to money mules. The suspect will gain the trust and affection of the victims over a lengthy period of time (months). The suspect will convince the victims they are an investor, engineer, in the military or someone prestigious. The suspect will use the goodwill of the victims to accept and send money using one or more of the various payment methods listed above. Often, the suspect will provide victims with a cell phone to communicate with them. The suspect will request that the victims open a bank account and to send the suspect a bank card. All of these steps are used to turn the victim into a money mule and involve them in the money laundering process.

Warning Signs - How to Protect Yourself

- If you receive funds for any reason from an unknown individual or company, and you are asked to forward it elsewhere - DON'T!
- Be aware of offers for employment from what appears to be a legitimate employer looking for a "Financial Officer". The duties usually involve: collecting payments for the new employer, accepting funds into your personal bank account, and forwarding the money to a different country.
- Victims of romance scams have been used as money mules as their "loved one" is working in a foreign country and needs help to collect funds.
- Consumers that have won a fake lottery receive advance payments on their winnings. They are then asked to forward it to a "financial office" to cover fees or taxes.
- **Any request to conduct unusual or questionable transactions on behalf of a third party should be questioned.**
- Learn [more tips and tricks for protecting yourself from fraud.](#)

Anyone who suspects they have been the victim of cybercrime or fraud should report it to their local police and to the CAFC's [online reporting system](#) or by phone at 1-888-495-8501. If not a victim, report it to the CAFC anyway.