# What Members Need to Know About e-Transfer Autodeposit Fraud

- March 8, 2023
- Fraud Management

In honour of Fraud Prevention Month this March, PPJV wants to share insights with credit unions about e-Transfer Autodeposit fraud.

Recently, there was a **CBC article** related to an *Interac* e-Transfer Autodeposit scam – below find some additional details to help educate your members.

## What is Autodeposit?

*Interac* e-Transfer's Autodeposit function is a feature that you can enable through your financial institution. Once you have set it up and defined which account you want to use to receive your transfers, all e-Transfers you receive will be automatically deposited into your account following routine fraud checks by your financial institution, without any additional steps such as receiving and email or text or answering a security question.

## How does Autodeposit work?

When someone sends money using the *Interac* e-Transfer service, the money never actually travels by email or text message – only notifications and deposit instructions do. As with most money transfers, the sender's financial institution and the recipient's financial institution transfer the funds using established and secure banking procedures.

The Autodeposit feature works by allowing the consumer or "recipient" of the funds to register and connect their email address or phone number to a specific bank account in advance, providing an added layer of validation between the sender and the receiver.

Once Autodeposit is enabled, the sender of an *Interac* e-Transfer knows who is receiving the funds (and the account they are going to be deposited in) prior to sending. Autodeposit transactions are considered **near real-time** as they go through this pre-authentication step by both the sender's financial institution and the recipient's financial institution in advance of the transfer.

Autodeposit eliminates the security question and answer step for every transaction. However, as with all transfers, there are additional fraud checks that occur in the background by both the sending and receiving financial institutions as part of their standard processes. In some cases, a

transaction may be completed faster due to the previous history of transactions between a sender and the recipient, or other parameters set up by the financial institution.

It is the financial institution that sets the dollar amount and fraud delay thresholds on all transactions being sent by their customers to mitigate fraud risk. These are determined by a financial institution's risk tolerance or by previously established history between the sender and recipient.

**Only when an Interac e-Transfer Autodeposit notification is received by the recipient of the funds should a e-Transfer transaction be considered complete.**

# Does Autodeposit protect against fraud?

Autodeposit can help protect you from **email fraud**, which is a very common type of fraud where criminals gain access to email accounts in order to collect personal information and intercept messages such as e-Transfer emails.

Fraudsters often try to exploit weaknesses in email security to gain access to your email account and attempt phishing scams or other cyber attacks. If the criminal does gain access to your email, they may be able to intercept your e-Transfer message, guess (or find) the answer to your security questions and redirect the funds. If you use Autodeposit to bypass the email step of a transfer, fraudsters who gain access to your email account can't intercept the message and therefore can't intercept the funds, as transfers will be automatically deposited in your account following routine fraud checks by your financial institution, without any additional steps.

However, e-Transfer fraud is not completely prevented with Autodeposit.

When buying or selling anything, especially from a person you don't know, the receiver of the funds should always confirm that they have received an *Interac* e-Transfer Autodeposit notification that funds have been successfully deposited into their account before parting with the goods they are selling. This will ensure the funds have been deposited. For example, a fraudster could pretend to transfer funds and show a fake confirmation screen, or could immediately cancel the transfer or not complete the transaction, and claim the funds have been sent. A confirmation to the recipient that the funds have been deposited from *Interac* or their financial institution is the only proof that the funds have been legitimately transferred.

For many different security reasons, consumers should avoid entering personal information into a device that is not their own.