BCSI Investigations

March 2022, Issue No. 1

The Investigator Newsletter

A Pandemic of Cybercrime!

by Denis Gagnon LPI - President

Over the past 2 years, parallel to the Covid-19 pandemic, we have seen a surge of fraudulent activities online. In addition, we have seen many variants of the modus operandi (M.O.) and the development of new ways to target victims.

Jurisdiction is always a problem with cybercrime if often layered and protected by “VIRTUAL PRIVATE NETWORKS” (VPN).

The focus must always be to recover the funds with a secondary focus of identifying the suspect (s) and proceeding to civil litigation and/or criminal charges.

Criminals focus on creative ways to scam their targets. One of the most recent creative ways is based on Covid-19 fraud and other approach focusing on seniors.

The Canadian antifraud centre states the impact of Covid-19 fraud between March 6, 2020, and February 28, 2022, as follows:

- 31,556 reports of Covid-19 fraud
- 28,813 victims of Covid 19 fraud
- $8.15 millions of loss

This is only a small portion of the financial impact of cyber fraud, as most cases remain unreported.

The most common scam of 2021-2022: cryptocurrencies fraud

Cryptocurrencies fraud has now reached the top of the online fraudulent scams. The scammers are sending phishing emails with fraudulent links for fake Instagram login pages; this allows scammers to steal account credentials. Once the account is taken over, the suspects blackmail victims to record videos of themselves promoting fake cryptocurrency platforms.

Top scams in Canada identified by the Competition Bureau

1.Investment scams
These scams have become more sophisticated and are multi-faceted. This includes but is not limited to cryptocurrencies, stocks pump and dump, Ponzi schemes, franchise/business opportunities. Therefore, any unsolicited offers require in-depth due diligence.

2.Identity theft
Scanners collect or reproduce personal information to commit fraud.

3.Health and medical scams
The three most common types of health scams are miracle cures, weight loss programs, and fake online pharmacies.

4.Romance scams
A fraudster on an online dating site convinces someone into sending large amounts of money in the name of love.

5.Phishing and smishing scams
The scam arrives via email (phishing) or text (smishing) and attempts to gain personal and financial information.

6.Employment scams
A scammer offers a (non-existent) job, but you first must pay a fee or provide your banking or personal information.

Cybercrime has bypassed the legal system

The legal system has been unable to keep up with the sophistication of cybercrime and the constant change of modus operandi (M.O)

How can I protect myself?

The best way to protect yourself is through prevention. However, with scams increasingly hard to identify, documentation is important when there is suspicion of any such crime. We will address ways to protect yourself in our next newsletter.

What can I do when I have been scammed?

The first step is to document all relevant information, including timelines, wire information, individual names who requested the investment, email addresses, and any information the investigation agency may require.

BCSI can help you investigate cryptocurrency fraud and recover your investment. Our investigative strategy and model have been developed over the past two (2) years and are unique to our Firm.

We will be happy to provide you with a complimentary consultation. Please contact our offices at 604-922-6572.