Blaney McMurtry LLP

PUBLICATION

Combatting Cryptocurrency Fraud

Date: March 16, 2026

Lawyers You Should Know: Nadav Amar, Olwen P.S. Alaminos

The rapid increase in popularity of cryptocurrency has been accompanied by an equally rapid rise in fraud and challenges to those seeking to lawfully trade in digital assets. The courts are seeing an increasing number of cryptocurrency fraud cases and recovery can be difficult.

Why has Cryptocurrency become a popular target of fraud?

Several characteristics of cryptocurrency make it uniquely attractive to fraudsters.

First, transactions may occur on decentralized platforms that operate outside traditional banking infrastructure. In such situations, there is no central authority to reverse fraudulent transfers or freeze suspicious accounts. Once cryptocurrency leaves a victim's wallet, fraudsters will often transfer money among several different wallets and liquidate the initial recipient wallet in an effort to make the funds untraceable.

Second, the nature of blockchain technology allows users to transact using only a wallet address. While blockchain transactions are publicly recorded, the identity behind each specific wallet is usually unknown unless additional steps are taken to retrieve that information.

Third, the global and borderless nature of cryptocurrency means that a fraudster operating in one jurisdiction can easily target individuals and businesses in another jurisdiction, meaning they may be beyond the reach of local courts.

Fourth, the speculative excitement surrounding digital assets has attracted investors eager to participate in perceived opportunities, making them vulnerable to scams.

How Cryptocurrency frauds operate and who they target

Investment fraud is a particularly prevalent form of cryptocurrency fraud. In these types of scams, the fraudsters will promise guaranteed returns and will often provide a small initial return in order to entice the investor to contribute more than their initial advance. For example, if an investor contributes $10,000, the fraudsters may well return $20,000, thereby producing a significant return on initial investment. This will lull investors into a false sense of security, incentivizing them to reach deeper into their pockets in the expectation of lucrative returns. By the time they have depleted all their savings, the unlucky investors discover that their money has been funneled to other wallets.

It should also be noted that elderly individuals and first-time investors are disproportionately targeted. Fraudsters exploit their lack of sophistication with digital assets and pressure them into converting savings into cryptocurrency and transferring funds to wallets controlled by the fraudsters.

However, businesses are not immune. Fraudulent schemes involving business emails have evolved to include cryptocurrency, with fraudsters impersonating executives or vendors and directing employees to make urgent payments in digital assets.

The Challenges

Victims of current cryptocurrency fraud face significant hurdles. The pseudonymity of wallet addresses means that the first step (identifying the wrongdoer) is often the most difficult. Further, if the fraudsters have disappeared, seeking relief against the cryptocurrency exchange is difficult. Such entities typically are protected by carefully crafted user terms and conditions.

Jurisdictional complexity presents a further obstacle. A victim in Ontario may find that the fraudsters operated through an exchange incorporated in Singapore. Determining which court has jurisdiction, which law applies, and how to effect service of legal process on the anonymous defendant or enforce a judgment once obtained creates significant legal complexities.

The Road to Recovery

Despite these challenges, victims still have tools available to them to aid their effort to recover from fraudsters in cryptocurrency scams.

Often, the first priority is to freeze the assets before they are dissipated further. A *Mareva* injunction is an interim order restraining a defendant from disposing or dealing with assets pending a trial. Ontario courts have granted *Mareva* relief over cryptocurrency holdings. For more information on *Mareva* injunctions, see our December 1, 2022 article breaking down the test to obtain this extraordinary relief in cryptocurrency disputes.

Where the identity of the fraudster is unknown, a *Norwich* order is also a helpful remedy to seek. This compels a third party who has become innocently mixed up in wrongdoing to disclose information that will assist the plaintiff in identifying the wrongdoer. In the cryptocurrency context, *Norwich* orders can be sought against exchanges to compel disclosure of account holder information.

One of the most important priorities is identifying where the funds are held. Victims of fraud will need to trace the misappropriated funds through various transactions to their current location. Cryptocurrency forensic firms have developed sophisticated tools capable of mapping the movement of cryptocurrency across wallets and exchanges, identifying patterns consistent with money laundering. Expert evidence from these firms is increasingly common and usually necessary in cryptocurrency fraud litigation.

Conclusion

Cryptocurrency fraud presents formidable challenges. A recent publication by the Ontario Securities Commission revealed that the government shut down more than 7,586 fraudulent investment platforms and cryptocurrency scam websites over just an eight-month period between June 2025 and February 2026, illustrating the ubiquity of online financial fraud. Fortunately, cryptocurrency fraud is not always beyond the reach of Ontario's courts. By deploying *Mareva* injunctions to freeze assets, *Norwich* orders to unmask wrongdoers, and blockchain tracing to follow the money, victims of digital asset fraud have a fighting chance to pursue meaningful remedies.

Nadav Amar is a member of Blaneys' Commercial Litigation Group and is currently handling cryptocurrency fraud matters. For assistance, you can contact Nadav at namar@blaney.com or 416.593.3903. Olwen Alaminos is also a member of Blaneys' Commercial Litigation Group and can be contacted at OAlaminos@blaney.com or 437.890.9283.