August 2021

OON & BAZUL

ASIAN EXPERTISE·GLOBAL REACH

WITH THE RISE OF CRYPTOCURRENCY FRAUD, LEGAL REMEDIES ARE AVAILABLE TO RECOVER STOLEN ASSETS

In June 2016, Dr Ruja Ignatova walked onto the Wembley Arena stage to cheers from thousands of adoring fans. Also known as the "Cryptoqueen", she was there to promote her very own cryptocurrency – OneCoin, which she touted as the next Bitcoin. Between her charming persona and impressive credentials, people from all over the world were sold on the OneCoin dream – it is estimated that investors poured over US$4 billion into OneCoin purchases between August 2014 and March 2017.[1]

The scheme, however, eventually unravelled. OneCoin was revealed to be nothing more but a Ponzi scheme. Dr Ignatova went missing in October 2017, and has not been found to date.[2] The OneCoin scam was one of the world's first, and possibly largest, cryptocurrency-related scams. Since then, cryptocurrency fraud has only been on the rise, targeting both retail and institutional investors alike.

Surge in Cryptocurrency-related fraud

As the value of cryptocurrencies leapt and skyrocketed over the past year or so, a report by fraud prevention company Bolster revealed a corresponding increase in cryptocurrency-related fraud, and predicts that this trend is likely to grow as the prices of cryptocurrencies continues to rise. Data shows a direct correlation between the value of bitcoin and the incidences of bitcoin scams.[3] True enough, 2020 saw more than 400,000 cryptocurrency-related scams globally, a 40 per cent increase from 2019.[4]

Global market capitalisation for cryptocurrencies hit US$1.7 trillion in January 2021, an 800 per cent increase from January 2020. As of now, the global cryptocurrency market capitalisation is well over US$2 trillion.[5] Based on current levels of suspicious activity, researchers have predicted a 75 per cent increase in cryptocurrency-related crimes in 2021. With cryptocurrency becoming more accessible to the general public, the days of "Nigerian prince" scams are over – as investors become more sophisticated, fraudsters too have had to update their approach to find a way to help themselves to a slice of the pie.

But why Cryptocurrency?

Cryptocurrency transactions provide a greater degree of autonomy and confidentiality than regular fiat currency transactions. Under traditional cash or credit systems, banks act as the "middle man" and every transaction is recorded. With cryptocurrency however, each transaction is a unique exchange on terms agreed upon between the parties involved, with a unique anonymous address generated for each transaction that makes it difficult to track a specific user's transaction history. The independent nature of decentralised transactions also renders cryptocurrency-based transactions much more convenient as the "middle man" is eliminated, saving on transaction fees, exchange rates, tax, etc.[6][7][8]

However, it is these very same conditions that allow fraudsters to thrive. Due to the difficulties in regulating cryptocurrency transactions and the anonymity afforded by decentralisation,

[1] https://www.bbc.com/news/stories-50435014
[2] https://thenextweb.com/news/onecoin-cryptocurrency-scam-need-to-know
[3] https://securityboulevard.com/2021/03/cryptocurrency-is-going-mainstream-so-are-the-scams/
[4] https://www.businesswire.com/news/home/20210325005317/en/Bolster-Research-Shows-Cryptocurrency-Scams-Nearly-Doubled-in-2020-and-Forecasts-More-This-Year%C2%A0
[5] https://coinmarketcap.com/ as at 12 April 2021
[6] https://blog.finjan.com/advantages-of-cryptocurrency/
[7] https://www.europeanbusinessreview.com/advantages-of-cryptocurrency-all-you-need-to-know/
[8] https://www.investopedia.com/ask/answers/100314/what-are-advantages-paying-bitcoin.asp

fraudsters can easily mask their true identities with aliases and pseudonyms, essentially conducting transactions anonymously.[9] Further, in the absence of transaction records, it can often be near impossible to track them down.

Most Common Types of Cryptocurrency-related Fraud[10][11]

Ponzi schemes

Crypto Ponzi schemes, such as the OneCoin scheme, typically promise unusually high returns and may actually seem to deliver on these promises at first, but the payouts are really from new deposits rather than actual returns on investments.

Fake exchanges and wallets

As the title suggests, fake exchanges and wallets disguised as legitimate cryptocurrency exchanges and wallets dupe victims into thinking they are making legitimate transactions and investments. Some fake wallets even double as phishing scams – when victims key in their account details, the fraudsters are able to access the victims' accounts and steal funds from the victims' accounts.

Fraudulent ICOs

Fraudulent ICOs are probably the most common type of cryptocurrency fraud. According to a study conducted by Bloomberg, 80 per cent of ICOs conducted in 2017 turned out to be scams.[12] But even if the ICO is genuine, chances of stumbling upon "the next Bitcoin" are low.

Identifying and Avoiding Cryptocurrency Scams

Stick to established, reputable organisations

If it sounds too good to be true, it probably is. Do not fall for get-rich-quick schemes as they are most likely multi-level marketing or Ponzi schemes. Instead, only use well-known and reputable trading platforms and wallet apps. For new cryptocurrency users, start off with big-name cryptocurrencies.

Look for signs of scams

Before committing to any cryptocurrency investments and revealing any account information, always double check if a website is legitimate, as fraudsters may create almost identical interface copies of legitimate sites. For instance, check if the site is secure by looking for the image of a padlock or the word "Secure" in the address bar. Spelling and grammatical errors, minor differences in the logos from those of the legitimate organisations that the websites seek to represent, as well as exaggerated claims may also be dead giveaways.

Research thoroughly

Most importantly, always conduct thorough research before investing. The crypto community is a tight-knit group – a simple google search of any given trading platform, app, wallet, or cryptocurrency, will likely uncover reviews and/or warnings from other crypto enthusiasts.

Legal Remedies

Earlier this year, a North-American company, successfully secured a US$3.9 million Mareva injunction to freeze the assets of a Hong Kong-incorporated company which was used as a vehicle for a Bitcoin fraud. In this elaborate global scheme involving parties from Canada, USA, UK, Malaysia, Singapore and Hong Kong, the fraudsters used fictitious identities to convince victims to invest in large amounts of Bitcoin which they did not actually have. As they engaged a law firm to act early, they were able to act swiftly and trace and freeze the fraudsters' assets before they could be dissipated.

In another case, an individual had his cryptocurrency-wallet hacked after he was tricked into clicking on a pop-up window which had prompted a "software update". The client's losses exceed US$70 million and since he engaged a law firm to act for him, steps have

[9] https://digitalcommons.lasalle.edu/cgi/viewcontent.cgi?article=1041&context=ecf_capstones
[10] https://www.thebalance.com/beware-of-these-bitcoin-scams-4158112
[11] https://www.finder.com/sg/bitcoin-scams
[12] https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

been taken in the Courts to trace and recover the stolen cryptocurrency.

So not all hope is lost if you've been defrauded – there are various legal remedies which may enable you to recover your assets. We set out in the following sections, some legal remedies that may assist you in an attempt to recover stolen crypto assets.

Disclosure Orders

To ascertain the identity of potential defendants with a view to commencing legal proceedings, a Norwich Pharmacal Order (a disclosure order made by the Court against non-parties) may be sought. This is especially useful in cryptocurrency fraud cases since fraudsters can hide behind a wall of anonymity provided by decentralised systems. This Order compels the production of documents and relevant information which may assist in revealing the identity of the fraudster. A Bankers Trust Order (a specific disclosure order made by the Court against non-parties, including banks and cryptocurrency exchanges, to aid in the tracing of funds) may also be sought to compel the disclosure of relevant information which may assist in tracing your assets to aid in their recovery.

Freezing Orders

If the fraudster has been identified and assets traced, a freezing order (also called a Mareva injunction order) may be obtained to freeze the fraudster's assets to aid a prospective Judgment. This way, the fraudster will not be allowed to move his funds out of reach, so that there will most likely be sufficient amounts to restore your losses. Unfortunately, the COVID-19 pandemic has increased the reach of fraudsters with the prevalence of use of technology. The availability of this very practical and effective remedy when utilised timely increases the chances of recovery and also leads to a quick settlement. Law firms have obtained several injunctive orders including one for a worldwide freezing order co-ordinated over several jurisdictions for a claim valued at US$5 billion.

A Leap of Faith

Navigating the cryptocurrency world is still a challenge for both regulators and investors alike as it is difficult to govern the exchange of cryptocurrency without curtailing the very features which differentiate it from fiat currency. That being said, if proper due diligence is done before buying or investing in any cryptocurrency-related products, and/or if the appropriate legal remedies are embarked upon promptly after the fraud having taken place, the risks associated with navigating the treachery of trading in cryptocurrencies can be substantially mitigated.

If you require assistance in cryptocurrency fraud or any other fraud matters, please do not hesitate to get in touch with:

Bazul Ashhab
Managing Partner
Head of Dispute Resolution

bazul@oonbazul.com
DID + 65 9757 1479

Lionel Chan
Partner

lionel.chan@oonbazul.com
DID + 65 9759 2037

www.oonbazul.com

Oon & Bazul LLP
36 Robinson Road,
#08-01/06 City House,
Singapore 068877
Tel (65) 6223 3893
Fax (65) 6223 6491

In Association with
TS Oon & Partners,
Malaysia