1 June 2020 | Reed Smith Client Alerts

Mitigating and investigating cryptocurrency and digital asset fraud in the Asia-Pacific region: some key considerations

The cryptocurrency and digital-asset ecosystem in the Asia-Pacific region has seen rapid growth over recent years and is generating opportunities for novel business models, but is also giving rise to various types of fraud. While fraud risk in this sector is being mitigated by service providers such as cryptocurrency exchanges and digital-wallet operators implementing practical safeguards for the protection and monitoring of assets and transactions, and while comprehensive regulatory frameworks are being introduced across the region to address operational risk, fraudulent actors remain able to exploit cybersecurity and control weaknesses. Consequently, it remains paramount for industry participants to put in place calibrated and risk-based fraud mitigation measures, and to have the capability to investigate fraud effectively where it does occur.

Authors: **Calvin Chan**, **Hagen Rooke**, **Nicholas Seng**, **Jun Yi Ho**

Global trading volumes in cryptocurrencies (e.g., Bitcoin, Ether and XRP) and other digital assets (e.g., stablecoins such as Tether and USD Coin) have been steadily increasing, as more traders and investors adopt these digital tokens as a means of investment, payment or value transfer.

The cryptocurrency and digital assets space is also attracting growing interest from hedge funds and other institutional investors, with some established financial institutions expanding their offerings to services such as crypto and digital asset custody and trade execution. In tandem with this rise in popularity, the cryptocurrency and digital assets space has attracted fraudulent activity.

Crypto and digital asset fraud in Asia-Pacific

The Asia-Pacific region is a hotbed for digital innovation, and has a significant cryptocurrency adoption rate among citizens. Cryptocurrency exchanges, which handle significant volumes of cryptocurrency, have been targets of fraud. As exchanges typically

enter into possession of their users' cryptocurrency, they present a centralized store of value for hackers to focus their attacks on. Exchanges in Japan, South Korea, Hong Kong and Singapore have been the targets of high-profile hacking attacks in recent times.

For owners of cryptocurrency or other digital assets, fraud risks are not limited to external risks such as hacking. They also include internal risks such as employees or other insiders exploiting flaws or gaps in internal security frameworks and controls to misappropriate cryptocurrency and digital assets. Such risks are more pronounced where access to private keys associated with these assets is entrusted to one or a few individuals.

Investors and crypto traders can also find themselves exposed to other types of fraud that are not unique to the cryptocurrency and digital asset space. In 2019, a purported South Korea-based crypto wallet and exchange solicited approximately US$2.9 billion worth of deposits in Bitcoin, Ether and other cryptocurrencies. This organization promised high rates of return (to be generated by exchange profit, mining income, and referral benefits), but was in fact a Ponzi scheme which resulted in the misappropriation of the deposited tokens. A comparable scam was perpetuated by a China-based organization, which resulted in the misappropriation of an estimated US$1 billion worth of cryptocurrency.

The manipulation of cryptocurrency prices is another category of fraud that affects the integrity of crypto markets. A concentrated campaign of manipulative trading activity conducted through a Hong Kong-headquartered exchange is alleged to have induced at least half of the increase in the price of Bitcoin and other major cryptocurrencies over the course of 2017. Another form of cryptocurrency price manipulation is "pump and dump", whereby messaging apps are used to rally investors to acquire cryptocurrencies in large volumes and drive up their price. The instigators then effect a sudden sell-off of those cryptocurrencies (which usually results in a subsequent and sharp price drop).

Other examples of manipulative practices include "spoofing", whereby orders for the sale or purchase of a cryptocurrency are placed but cancelled before they are executed, and "wash trading", where a person exploits an opaque trading structure to engage in purchase and sale transactions with themselves, thus artificially increasing demand and value.

READ MORE +

RELATED

Capabilities: **Data Protection, Privacy and Cybersecurity**, **Finance**, **FinTech**, **Regulatory & Investigations**

Offices: **Singapore**

YOU MAY BE INTERESTED

EDPB updates consent guidance to clarify its position on consent to the use of cookies

Technology Law Dispatch

Dutch court holds that a grandmother is in breach of the GDPR for failing to remove photos of her grandchildren from social media platforms

1 June 2020

Technology Law Dispatch

28 May 2020

When Unclear Retail Rent-To-Own Terms Draw FTC Ire

Law360

28 May 2020

ICO finalises guidance on explaining decisions made with AI

Technology Law Dispatch

27 May 2020