Article Information

Authors: Steven Pettigrove, Michael Bacina
Service: Blockchain
Sector: Financial Services, FinTech, IT & Telecommunications

Do you need a token dealing policy? Managing insider trading, fraud and conflicts risk

Michael Bacina and Steven Pettigrove of the Piper Alderman Blockchain group provide insight and commentary to token dealing policy and insider trading risks.

The past year has seen two high profile incidents involving buying or selling crypto-assets (tokens and NFTs) based on information obtained by employees of OpenSea and Coinbase during the course of their employment.

Despite uncertainties regarding the regulatory status of many crypto-assets, the potential consequences of trading of crypto-assets based on inside information are not limited, and wouldn't clearly be included in, insider dealing offences under the *Corporations Act 2001* (Cth) (**Corporations Act**).

Insider dealing type conduct can also engage general fraud offences and offend prohibitions on directors, officers and employees misusing their position or information for personal gain. In addition, trading by insiders and conflicts, or the perception of conflicts, can cause substantial reputational consequences for businesses and individuals involved, as was seen in the OpenSea and Coinbase incidents.

Piracy on the OpenSea

On 1 June 2022, a former product manager at OpenSea, Nate Chastain, was charged by the United States Department of Justice (**DOJ**) with wire fraud and money laundering in connection with an alleged scheme to commit insider trading in Non-Fungible Tokens (**NFTs**).[1] Chastain was accused of:

> using confidential information about what NFTs were going to be featured on OpenSea's homepage for his personal financial gain.[2]

Each of the charges against Chastain carry a maximum prison sentence of 20 years. Chastain has reportedly filed a motion seeking dismissal of the charges.[3]

Debasing the Coin(base)

On 21 July 2022, a former product manager at Coinbase (Ishan Wahi), his brother (Nikhil Wahi), and his friend (Sameer Ramani) were charged by the DOJ with wire fraud and wire fraud conspiracy in connection with a scheme to commit insider trading in crypto-assets.[4] They are also being pursued under insider trading laws by the US Securities and Exchange Commission (**SEC**) which is seeking civil penalties, disgorgement and permanent injunctive relief.[5]

Ishan Wahi is accused of tipping off his brother and friend to upcoming token listings on Coinbase, generating gains of around US$1.5M by front running listings in at least 25 tokens. The SEC claim that "at least 9" of the tokens traded were securities under US law, violating anti-fraud provisions under the US Securities Exchange Act 1934. If the SEC action proceeds to trial, the SEC would need to establish that one or more of those 9 tokens is a security under US law, a finding which would have wider implications for the token issuers and exchanges which have listed those tokens and presently have no path to comply with registration or licensing requirements under US law.

While it is understood that Coinbase cooperated with the SEC's investigation, Coinbase's Chief Legal Officer, Paul Grewal

criticised the SEC's decision to assert the tokens were securities:

> Coinbase has a rigorous process to analyze and review each digital asset before making it available on our exchange...we remain confident that Coinbase's rigorous review process keeps securities off Coinbase's platform.[6]

In September, Nikhil Wahi plead guilty to one count of conspiracy to commit wire fraud in connection with the charges brought by the Department of Justice.[7] Wahi is scheduled to be sentenced at a hearing on 13 December 2022. It is understood that the insider trading charges brought against each defendant by the SEC remain pending.

Damian Williams, United States Attorney for the Southern District of New York, said:

> Less than two months after he was charged, Nikhil Wahi admitted in court today that he traded in crypto assets based on Coinbase's confidential business information to which he was not entitled. For the first time ever, a defendant has admitted his guilt in an insider trading case involving the cryptocurrency markets. Today's guilty plea should serve as a reminder to those who participate in the cryptocurrency markets that the Southern District of New York will continue to steadfastly police frauds of all stripes and will adapt as technology evolves.[8]

After Chastain's trading in NFTs was revealed by online sleuths, OpenSea published a blog post indicating that it had commissioned a third party review of the incident and introduced new policies banning OpenSea employees from trading NFTs featured on its home page or otherwise trading on confidential information relating to NFTs.[9] That approach is a minimum level of compliance which should be observed.

At Coinbase, Ishan Wahi tipped his brother and friend to trade on confidential information despite express warnings to employees by Coinbase not to share such information or tip any person who might trade on that information.[10]

The OpenSea and Coinbase incidents highlight the need for cryptocurrency exchanges and NFT businesses, in particular, to have appropriate employee and contractor policies in place which mitigate the risks of employees and contractors dealing in tokens based on inside information, manage potential conflicts and avoid reputational harm. As digital assets become increasingly mainstream, we anticipate that a wide range of businesses will require such policies, including financial services businesses, venture capital firms, investment funds, and other commercial enterprises like sporting organisations which issue NFTs.

In Australia, insider trading in financial products is prohibited under the Corporations Act.[11] State laws include fraud related offences may be engaged even where the relevant dealing does not involve a security or financial product.[12] Directors, officers and employees also risk criminal and civil penalties under the Corporations Act where they use their position or information obtained because of their position to gain an advantage for themselves or someone else, or cause detriment to the company.[13]

To protect your business or project from reputational damage, a token dealing policy coupled with regular training and internal communications raising awareness of the policy (including from senior management) can be an effective way to reduce the risks.

While a token dealing policy will share similarities with securities dealing policies, token dealings can raise specific issues depending on the relevant business or project involved. For example:

1. It may be appropriate to include an exemption in a token dealing policy for airdrops where a transfer of tokens is received by an employee without notice to or further action by the recipient;
2. For a venture capital firm, it may be appropriate to grant permission to specified employees to deal in utility tokens on behalf of the firm up to a *de minimis* threshold for the purpose of conducting due diligence on a prospective investment; and
3. It will usually be important to include in a token dealing policy broader prohibitions around inappropriate token dealings to reduce the risk of false or misleading trading by employees which could engage market conduct laws or cause reputational damage.

In considering whether to implement a token dealing policy, it is important to instruct competent lawyers who are deeply familiar with both digital assets, corporate and financial services laws and the unique issues which arise involving digital assets.

[1] https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme

[2] Ibid.

[3] https://blockworks.co/opensea-ex-employee-asks-court-to-dismiss-insider-trading-case/

[4] https://www.justice.gov/usao-sdny/pr/three-charged-first-ever-cryptocurrency-insider-trading-tipping-scheme

[5] https://www.sec.gov/news/press-release/2022-127#:~:text=The%20SEC%27s%20complaint%2C%20filed%20in,prejudgment%20interest%2C%20and%20civil%20penalties.

[6] https://www.coinbase.com/blog/coinbase-does-not-list-securities-end-of-story

[7] https://www.justice.gov/usao-sdny/pr/tippee-pleads-guilty-first-ever-cryptocurrency-insider-trading-case

[8] https://www.justice.gov/usao-sdny/pr/tippee-pleads-guilty-first-ever-cryptocurrency-insider-trading-case

[9] https://opensea.io/blog/announcements/employee-information-use-at-opensea/

[10] https://www.sec.gov/news/press-release/2022-127#:~:text=The%20SEC%27s%20complaint%2C%20filed%20in,prejudgment%20interest%2C%20and%20civil%20penalties.

[11] *Corporations Act 2001* (Cth), s 1043A.

[12] e.g. *Crimes Act 1958* (Vic), s 82 (obtaining financial advantage by deception); *Crimes Act 1900* (NSW), s 192E (fraud).

[13] *Corporations Act 2001* (Cth), ss 182 to 184.