New York Law Journal
White-Collar Crime
WWW.NYLJ.COM
An ALM Publication
VOLUME 266—NO. 108
MONDAY, DECEMBER 6, 2021

Crypto Insider Trading: What Exchanges Should Know

BY NOLA B. HELLER
AND SAMSON ENZER

Imagine the following. An employee of the proprietary trading arm of a digital asset trading exchange learns confidential information from a colleague in another division that their employer will soon be publicly listing a new cryptocurrency token for trading on the exchange. The trading employee buys units of the token for the exchange's benefit and for his own account before the public learns of the upcoming listing, the units' market price skyrockets when the listing is announced, and the employee sells the units at a profit.

The risks that can arise from such insider trading are not merely hypothetical in the cryptocurrency industry. For example, several news outlets recently reported that criminal and regulatory authorities have opened investigations into potential insider trading in digital assets at one of the largest digital asset exchanges in the world.

In this article, we discuss the potential criminal and civil penalties that such exchanges can face if their employees engage in insider trading in digital assets. We also suggest several measures that exchanges can take to reduce their exposure from such risks.

Potential Liabilities of Exchanges for Employee Insider Trading In Digital Assets

When an employee of a digital asset exchange engages in insider trading in digital assets, the exchange may be at risk of being held vicariously liable for financial penalties in a civil enforcement action by the Securities and Exchange Commission (SEC) or Commodity Futures Trading Commission (CFTC) or for criminal penalties in a prosecution by the Department of Justice (DOJ).

SEC Enforcement. Under §10(b) of the Securities Exchange Act (SEA) and SEC Rule 10b-5 thereunder, it is illegal to engage in fraud in connection with the purchase or sale of any "security,"

ADOBE

including the form of securities fraud known as insider trading. Rule 10b-5 prohibits corporate insiders and their agents from trading company-issued securities based on material, nonpublic information about the company in breach of a duty of trust or confidence owed to the source of such inside information. See 17 C.F.R. §240.10b-5-1(a). The SEC has multiple statutory tools under which it can hold an employer vicariously liable for an employee's insider trading violation. See, e.g., 15 U.S.C. §§78t, 78u-1. For example, the SEC can sue an employer for civil penalties under SEA §21A for failing to take appropriate steps to prevent an employee's insider trading violation in certain situations (see 15 U.S.C. §78u-1), including in circumstances where the employee did such trading for the employer's benefit. See, e.g., *SEC v. CR*

NOLA B. HELLER *is a partner and* SAMSON ENZER *is a counsel at Cahill Gordon & Reindel, and both are former federal prosecutors in the Southern District of New York who now defend companies and individuals in white-collar criminal and regulatory matters, including those relating to cryptocurrency.*

Intrinsic Investors, 12 Civ. 8466 (VM) (S.D.N.Y.).

The SEC has jurisdiction to enforce Rule 10b-5 against anyone engaged in or vicariously liable for insider trading in digital assets, but only if the assets qualify as "securities" under the SEA. The SEA defines "security" to include a variety of traditional investment instruments such as stocks and bonds, and also to include any "investment contract." 15 U.S.C. §78c(a)(10). An "investment contract" is any contract, transaction, or scheme "whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of a promoter or a third party." *SEC v. W.J. Howey Co.*, 328 U.S. 293, 298-99 (1946). Whether a particular digital asset qualifies as an "investment contract" under *Howey*, and thus as a "security," turns on the characteristics of the asset and the manner in which it was sold. See SEC Corporation Finance Director William Hinman, Remarks at the Yahoo Finance All Markets Summit (June 14, 2018). For example, publicly traded digital assets that were initially sold to investors by businesses raising startup capital will frequently qualify as "securities" under the *Howey* test. See SEC FinHub, *Framework for "Investment Contract" Analysis of Digital Assets* (April 3, 2019). SEC Chair Gary Gensler has stated that in his view, "we have a crypto market now where many tokens may be unregistered securities," including many digital assets that were sold to the public through initial coin offerings, and initiatives "to offer crypto tokens or other products that are priced off of the value of securities and operate like derivatives." Remarks Before the Aspen Security Forum (April 3, 2021). A variety of digital asset offerings have been deemed securities offerings by courts. See, e.g., *SEC v. Telegram Group*, 448 F. Supp. 3d 352, 379 (S.D.N.Y. 2020).

CFTC Enforcement. Section 6(c)(1) of the Commodity Exchange Act (CEA) and CFTC Rule 180.1 thereunder, the latter of which was modeled on SEC Rule 10b-5, provide an analogous prohibition against fraud in connection with any contract of sale of any "commodity" as that term is defined by the CEA, including insider trading in commodities. Like the SEC, the CFTC can hold an employer vicariously liable for civil penalties based on an employee's insider trading violation in certain situations, including under CEA §2(a)(1)(B) where the employee was trading for the employer's benefit (see *CFTC v. Byrnes*, 13 Civ. 1174 (VSB), Dkt. 226 (Aug. 3, 2020)). But to do so in a case involving digital asset trading, the asset at issue must qualify as a "commodity" under the CEA. The CEA defines "commodity" to include all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in. See 7 U.S.C. §1a(9). The CFTC maintains that Bitcoin and other virtual currencies are commodities within that definition (see *In the Matter of: Coinflip*, CFTC Dkt. 15-29 (Sep. 17, 2015)), and several courts have agreed (see, e.g., *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 228 (E.D.N.Y. 2018)).

The SEC has jurisdiction to enforce Rule 10b-5 against anyone engaged in or vicariously liable for insider trading in digital assets, but only if the assets qualify as "securities" under the SEA.

DOJ Enforcement. The DOJ has authority to seek incarceratory and financial penalties to punish willful insider trading violations of the SEA and CEA. See 15 U.S.C. §78ff; 7 U.S.C. §13. Accordingly, insider trading in a digital asset that qualifies as a "security" or "commodity" can result in a DOJ prosecution for criminal SEA or CEA violations. The DOJ can also prosecute criminal insider trading in digital assets—regardless of whether they qualify as securities or commodities—under the far-reaching wire fraud statute (see 18 U.S.C. §1343), which makes almost every variant of fraudulent conduct a federal crime, as long as the conduct involved an interstate or international wire communication (such as an email communication, electronic transfer of funds via the Internet, or telephonic communication). Courts have sustained wire fraud convictions for insider trading in many types of assets. See, e.g., *United States v. Dial*, 757 F.2d 163, 164-69 (7th Cir. 1985) (affirming wire and mail fraud convictions for insider trading in silver futures, as the "federal mail and wire fraud statutes have often been used to plug loopholes in statutes prohibiting specific frauds"). The DOJ has also prosecuted a variety of cryptocurrency-related frauds under the wire fraud statute. See, e.g., *United*

States v. Sharma, 18 Cr. 340 (LGS) (S.D.N.Y.); *United States v. McAfee*, 21 Cr. 138 (LGS) (S.D.N.Y.).

A corporation may be held criminally liable for illegal acts of its employees that were within the scope of their employment duties and intended, at least in part, to benefit the corporation. See *N.Y. Central & Hudson River R. Co. v. United States*, 212 U.S. 481, 493-97 (1909). Based on this principle, the DOJ has secured criminal sanctions against corporations for insider trading by their employees. See, e.g., *United States v. SAC Capital Advisors L.P.*, 13 Cr. 541 (LTS) (S.D.N.Y.).

Measures That Exchanges Can Adopt To Limit Their Exposure

There are a variety of preventive measures that digital asset exchanges can adopt to reduce their exposure to penalties for insider trading in digital assets by their employees. Cf. SEC OCIE Staff Summary Report on Examinations of Information Barriers (Sept. 27, 2012) (discussing broker-dealers' programs to prevent misuse of material, nonpublic information). For example, exchanges can:

(1) adopt policies requiring employees to maintain confidentiality over material, nonpublic information relating to digital assets, refrain from trading any digital assets for which they or the firm possess such inside information (absent preclearance from the firm's chief legal or compliance officer), and periodically certify their compliance with such policies;

(2) periodically train employees on such policies, the potential civil and criminal penalties for insider trading in digital assets, and maintaining secrecy over market-sensitive information to reduce the likelihood of information leaks;

(3) provide employees with restricted trading lists of digital assets that they are barred from trading (temporarily or permanently, depending on the circumstances) absent an exemption from the firm's chief legal or compliance officer, because the firm has access to material, nonpublic information or a conflict of interest relating to such assets;

(4) limit the group of employees with access to sensitive information about digital assets to only those with a need to know the information; and

(5) keep access logs tracking the names of employees with access to such sensitive information, require employees to communicate about work matters exclusively via firm-approved modes of communication that are subject to monitoring by the firm, and preserve such communications.

The DOJ, SEC, and CFTC have long maintained policies promoting leniency for corporations that **cooperate in investigations of misconduct** and measure such cooperation, in part, by the sufficiency of any **compliance programs** implemented to prevent misconduct.

Implementing measures like these can have a variety of potential benefits for a digital asset exchange, including: (a) building the trust of customers and business partners that their secrets will not be exploited for insider trading gains; (b) reducing the risk of employee insider trading and the potential penalties that can follow; and (c) improving the likelihood of securing cooperation credit from the DOJ, SEC, or CFTC that may avoid or limit penalties imposed in the event of employee insider trading despite such measures. The DOJ, SEC, and CFTC have long maintained policies promoting leniency for corporations that cooperate in investigations of misconduct and measure such cooperation, in part, by the sufficiency of any compliance programs implemented to prevent misconduct.