Wenchi Hu PLLC
Regulatory Recap
June 28, 2024

Notable Developments:

- **U.S. Supreme Court Strikes Down SEC's Ability to Use Administrative Judges in Securities Fraud Enforcement Cases**
- **FICC Proposes Rules to Implement Mandatory Clearing of US Government Securities**

SEC Enforcement:

- **SEC Sues Consensys Software over MetaMask Staking Services and MetaMask Swaps**
- **SEC Charges R.R. Donnelley & Sons Co. for Accounting Control Failures Related to Cybersecurity Practices.**

In Case You Missed It:

- **Coinbase Sues SEC and FDIC for Failure to Comply with FOIA Requests**
- **FINRA Settles Charges with a Broker Dealer for Impermissible Language in Confidentiality Agreements**
- **SEC Publishes Taxonomy to be Used by Security-Based Swap Execution Facilities**

Notable Developments:

U.S. Supreme Court Strikes Down SEC's Ability to Use Administrative Judges in Securities Fraud Enforcement Cases

On June 27, 2024, the U.S. Supreme Court, 6-3, ruled that when the SEC seeks civil penalties against a defendant for securities fraud, the Seventh Amendment entitles the defendant to a jury trial. As a result, the SEC cannot use administrative law judges to decide civil charges against persons who allegedly committed violations of the Federal securities law. In an enforcement action, the SEC may file a complaint in federal court or can adjudicate the matter in-house by instituting an administrative proceeding in front of an administrative law judge. The Supreme Court's decision upends the SEC's ability to impose civil penalties on a defendant for securities fraud, even in a case where the defendant agrees to a civil penalty and settles with the SEC. Justice Sotomayor issued the dissent, arguing that the court's decision is a "power grab" that "arrogates Congress's policymaking role to itself" and violates well established precedent that Congress had long given federal agencies the right to adjudicate certain cases.

FICC Proposes Rules to Implement Mandatory Clearing of US Government Securities

FICC proposed new rules in response to the SEC mandate that a registered clearing agency for US Government securities require its members to clear certain of their Treasury cash market and repurchase transactions.

The FICC proposes to require that each Netting Member "submit all eligible secondary market transactions, both for repurchase agreements and certain categories of cash transactions, to which it is a counterparty to FICC for clearance and settlement;" and to "define the scope of such trade submission requirement;" and seek to "facilitate FICC's ability to identify and monitor Netting Members compliance," and enhance rules qualifications, standards and disclosures.

Certain aspects of the FICC rule proposals go beyond implementing the requirements of the SEC's Rule. These include:

- Additional requirements that will be imposed on firms that seek to become clearing members, including additional requirements to confirm the availability of sufficient financial resources;
- Periodic reporting requirements that a clearing member will be required to make to FICC to certify that it is in compliance with the clearing mandate;
- Express requirements to adopt procedures to maintain connectivity and to adopt cybersecurity measures; and
- Expanded authority of FICC to impose fines for noncompliance by clearing members and an increase in the amount of fines that FICC may impose.

SEC Enforcement:

SEC Sues Consensys Software over MetaMask Staking Services and MetaMask Swaps

On June 28, 2024, the SEC announced charges against Consensys Software Inc. ("Consensys") with engaging in unregistered offer and sale of securities through its MetaMask Staking services and with operating as an unregistered broker through MetaMask Staking and MetaMask Swaps. According to the SEC's complaint filed in the U.S. District Court for the Eastern District of New York, Consensys operated a crypto staking program, through which Consensys offered and sold crypto tokens for two issuers – Lido and Rocket Pool. Lido and Rocket Pool each offer liquid staking programs. Staking refers to the commitment of native crypto asset of a blockchain by investors in order to act as a "validator" of transactions recorded on that blockchain network. Lido and Rocket pool Ether contributed by investors and stake the Ether tokens on the blockchain, using their technological expertise to earn returns that the typical investors would not be able to earn on their own. Each investor participating in the staking program receives a new crypto asset

in return, representing the investor's pro-rata interest in the staking pool and its rewards. The investor's interests represented by the new crypto assets are tradable on the secondary market, thereby providing investors a mechanism to exit their investment position, whereas tokens staked directly on the blockchain cannot be easily accessed while they are staked. SEC argues that the Lido and Rocket Pool staking programs are investment contracts and therefore, Consensys was engaging in illegal offers and sales of securities through the Lido and Rocket Pool staking programs.

In addition, SEC alleged that Consensys had acted as an unregister broker of crypto asset securities through its MetaMask Swaps service and has collected over $250 million in fees. MetaMask Swaps is a digital platform that effects the exchange of one crypto asset for another on behalf of the investors. "Consensys solicits potential investors to transact on MetaMask Swaps, holds itself out as a place to buy and sell crypto assets (which include crypto asset securities), recommends trades with—as Consensys itself puts it—the "best" value, accepts investor orders, routes investor orders, handles customer assets, carries out trading parameters and instructions on the customer's behalf, and receives transaction-based compensation."

SEC's complaint asked the court to permanently enjoin Consensys from continuing the staking and swaps services and order Consensys to pay civil monetary penalties and grant other relief as deemed appropriate or necessary by the court.

SEC Charges R.R. Donnelley & Sons Co. for Accounting Control Failures Related to Cybersecurity Practices

On June 18, 2024, the SEC announced its charges against, and acceptance of the settlement offer from, R.R. Donnelley & Sons Co. ("RRD") relating to RRD's cybersecurity controls practices.

According to the SEC's order, RRD violated the Exchange Act's disclosure controls and procedures and internal accounting control provisions relating to its cybersecurity practices. As a global provider of business communications services and marketing solutions, RRD's IT network regularly stored and transmitted confidential data and information of its clients, which included SEC-registered firms, healthcare organizations, publicly-traded companies and financial institutions. Between November 2021 and January 2022, RRD's internal intrusion detection systems issued a significant number of cyber alerts each month, which were first reviewed and analyzed by RRD's third-party managed security services provider to determine whether to escalate to RRD's internal cybersecurity personnel. According to the SEC's order, RRD did not reasonably manage the third-party security services provider's allocation of resources to the task. In its contract and

communications with the third-party security services provider, RRD failed to reasonably set out a sufficient prioritization scheme and workflow for review and escalation of the alerts. In addition, RRD did not have sufficient procedures to audit or otherwise oversee the third-party security services provider in order to confirm that their review and escalation of the alerts was consistent with RRD's expectations and instructions. RRD's internal staff allocated to the task of reviewing and responding to the escalated alerts also did not have sufficient time to dedicate to the escalated alerts. RRD's internal policies governing its personnel's review of cybersecurity alerts and incident response also failed to sufficiently identify lines of responsibility and authority, lacking clear criteria for alert and incident prioritization and clear workflows for alert review and incident response and reporting. Between November 29 and December 23, 2021, RRD experienced a ransomware network intrusion. After the third-party security services provider received and escalated three alerts to RRD's internal security personnel, RRD did not take the infected instances off the network and failed to conduct its own investigation of the activity, or otherwise take steps to prevent further compromise. During the same period, the third-party security services provider also reviewed, but did not escalate to RRD, at least 20 other security alerts related to the same ransomware malware being installed or executed on multiple other computers across the network and compromise of a domain controller server, which provided the threat actor with access to and control over a broader sweep of network resources and credentials. The threat actor was able to use hacking techniques to install encryption software on certain RRD computers and exfiltrated 70 gigabytes of data, including data belonging to 29 clients, some of which contained personal identification and financial information.

As a result, the SEC charged RRD with violation of Exchange Act Section 13(b)(2)(B) relating to the obligations of issuers with a class of registered securities to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that access to company assets is permitted only in accordance with management's general or specific authorization. In addition, SEC also charged RRD with violation of Exchange Act Rule 13a-15(a), which requires issuers of registered securities to maintain disclosure controls and procedures designed to ensure that information required to be disclosed in reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the SEC rules and forms.

In a statement in dissent, SEC Commissioners Peirce and Uyeda stated that the SEC's interpretation of accounting controls to include cybersecurity relies on "a broad interpretation of Section 13(b)(2)(B)" that "gives the Commission a hook to regulate public companies' cybersecurity practices." "While an enforcement action may be warranted in some circumstances," they argued, "distorting a statutory provision to form the basis for such an action inappropriately amplifies a company's harm from a cyberattack."

In a related story, the SEC's Division of Corporation Finance issued a new FAQ on June 24, 2024, relating to material cybersecurity incident disclosure requirements for Form 8-K filings.

In Case You Missed It:

Coinbase Sues SEC and FDIC for Failure to Comply with FOIA Requests

On June 27, 2024, Coinbase filed a lawsuit against FDIC to compel FDIC to provide copies of the letters it had sent to supervised financial institutions asking them to pause crypto-related activities and a lawsuit against the SEC to compel the agencies to provide access to government records regarding "Ethereum's shift to a proof-of-stake consensus mechanism that have been created since January 1, 2018, including.... factual or investigatory documents".

FINRA Settles Charges with a Broker Dealer for Impermissible Language in Confidentiality Agreements

An introducing broker-dealer settled FINRA charges for including confidentiality provisions in settlement agreements that could impede investigations by regulatory agencies.

According to the letter of acceptance, waiver and consent ("AWC"), Mutual Securities, Inc. entered into several settlement agreements restricting a customer's ability to communicate with regulators, violating FINRA Rule 2010. According to the AWC, (i) one provision prohibited a customer from disclosing settlement terms to regulatory bodies without a court order or order from a regulatory body; (ii) one broad confidentiality provision did not provide express permission to the customer to engage with securities regulators, should the regulators inquire about the settlement agreement; and (iii) one provision, while generally allowing disclosure to FINRA, "[prohibited] disclosure to one specified department within FINRA."

SEC Publishes Taxonomy to be Used by Security-Based Swap Execution Facilities

The SEC published the final Security-Based Swap (SBS) taxonomy along with illustrative sample documents in advance of the EDGAR 24.2 release, which will incorporate the final SBS taxonomy into EDGAR. The SEC's draft version of this taxonomy was published on March 27, 2024. The taxonomy will be used by security-based swap execution facilities to file specified information electronically with the SEC using EDGAR in Inline eXtensible Business Reporting Language for public comments.