Wenchi Hu PLLC
Regulatory Recap
May 31, 2024

Notable Developments:

- **SEC Adopts Amendments to Regulation S-P to Require Notification of Data Breaches.**
- **SEC Approves Listing of Spot Ethereum ETPs.**
- **Senate Follows House and Votes Disapproval of SEC Staff Accounting Bulletin No. 121**
- **House Passes Major Crypto Legislative Bill---Financial Innovation and Technology for the 21st Century Act.**

SEC Enforcement:

- **Intercontinental Exchange and Nine Affiliates Settles SEC Charges regarding Failing to Report a Cyber Intrusion to the SEC.**
- **Broker-Dealer Receives Remedial Sanctions Concerning Reg BI Disclosure Failure.**
- **Federal Court Rules That Crypto Influencer Conducted Unregistered Offering of Crypto Asset Securities**

In Case You Missed It:

- **SEC Director of Corporation Finance Issues Statement Concerning Materiality and Reporting of Cybersecurity Incidents.**
- **FINRA Initiates Remote Inspections Program.**
- **FINRA Publishes AI Communication Guidance.**
- **Crypto Firm Settles CFTC Charges for Failing to Register as an FCM.**
- **Congressional Research Service Issues Considerations for Central Bank Digital Currencies**
- **House Passes CBDC Anti-Surveillance State Act.**
- **Congressional Members Deliver Letter Urging Implementation of the Financial Data Transparency Act.**

[Insert Image here]

Notable Developments:

SEC Adopts Amendments to Regulation S-P to Require Notification of Data Breaches

On May 16, 2024, the SEC adopted a final rule mandating that broker-dealers (including funding portals), investment companies, investment advisers and transfer agents that are registered with the SEC or another appropriate regulatory agency ("covered institutions") develop, implement and maintain written policies and procedures for an incident response program reasonably designed to detect, respond to and recover from unauthorized access to or use of customer information.

Under the final rule, a response program must include procedures for, with certain limited exceptions, covered institutions to provide notice to individuals whose sensitive customer information was, or is reasonably likely to have been, subject to unauthorized access or use. Such a notice must be provided to affected individuals as soon as practicable, but not later than 30 days, after covered institutions becoming aware that an incident involving such unauthorized access where use of customer information has reasonably likely to have occurred. Such a notice must include details about the incident, the nature of the data accessed and how affected individuals can respond to the incident to protect themselves.

The final rule will become effective 60 days after publication in the Federal Register. Larger entities will have 18 months after the date of publication in the Federal Register to comply and smaller entities will have 24 months after the date of publication to comply.

SEC Approves Listing of Spot Ethereum ETPs

On May 23, 2024, the SEC issued an order granting approval of proposed rule changes filed by CBOE, Nasdaq and NYSE to list exchange-traded products ("ETPs") tied to the spot price of ether.

In their proposed rule changes, the exchanges made clear that they would subject the ETP to their rules governing "Commodity-Based Trust Shares." In the order, the SEC described ether as "a digital asset that is native to, and minted and transferred via, a distributed, open-source protocol used by a peer-to-peer computer network through which transactions are recorded on a public transaction ledger known as 'Ethereum,'" and that "the Ethereum protocol governs the creation of new ether and the cryptographic system that secures and verifies transactions on Ethereum."

In approving the ether trust shares to be listed on the exchanges, the SEC found the exchanges' proposed rule changes were consistent the Exchange Act and the SEC was approving all of the spot ether ETP proposals at the same time in order to foster competition by potentially providing investors with several spot ether-based ETPs from which to choose. The ETP shares, however, may not begin trading on its applicable exchange unless and until its corresponding registration statement becomes effective." As of today, the SEC has not

declared any of the registration statements of the spot ETP trust shares effective and therefore, trading of ether ETP has not commenced.

Senate Follows House and Votes Disapproval of SEC Staff Accounting Bulletin No. 121

On May 16, 2024, the U.S. Senate, following similar House action, voted 60 to 38 to overturn the SEC Staff Accounting Bulletin No. 121 that requires entities with obligations to safeguard crypto-assets, including maintaining the cryptographic key information necessary to access the crypto-assets, to present a liability on their balance sheets to reflect their obligation to safeguard the crypto-assets, backed by corresponding capital. Crypto industry groups had criticized this staff interpretation, claiming it stifled innovation.

The resolution received bipartisan support in the Senate, but President Biden has expressed his intention to veto the bill. See our prior coverage here.

House Passes Major Crypto Legislation --- Financial Innovation and Technology for the 21st Century Act

On May 22, 2024, the House voted approval of the passage of the Financial Innovation and Technology for the 21st Century Act (FIT 21), further shaping crypto regulation.

As passed in the House, the FIT 21, among other things, gives the CFTC jurisdiction over digital commodities and clarifies the SEC's jurisdiction over digital assets offered as part of an investment contract. The bill also establishes a process to permit the secondary market trading of digital commodities if they were initially offered as part of an investment contract. The bill also imposes customer disclosure, asset safeguarding, and operational requirements on all entities required to be registered with the CFTC and/or the SEC.

SEC Chair Gensler issued a statement concerning the proposed legislation (prior to its passage in the House), opposing its passage, stating, among other reasons, that it would "create new regulatory gaps and undermine decades of precedent regarding the oversight of investment contracts, putting investors and capital markets at immeasurable risk." CFTC Enforcement Director Ian McGinley, in a recent statement, also stressed the importance of digital asset regulation in the market.

SEC Enforcement:

Intercontinental Exchange and Nine Affiliates Settles SEC Charges regarding Failing to Report a Cyber Intrusion to the SEC.

On May 22, 2024, the SEC settled charges against Intercontinental Exchange, Inc. (ICE) and nine wholly-owned subsidiaries, including the New York Stock Exchange, for failures to timely inform the SEC of a cyber intrusion as required by Regulation SCI. According to the

SEC's order, ICE learned about a potential system intrusion involving a previously unknown vulnerability in ICE's virtual private network (VPN). ICE investigated and was immediately able to determine and confirm the occurrence of a system intrusion but ICE personnel did not notify the legal and compliance officials at ICE's subsidiaries of the intrusion until four days later. And at that point, ICE also determined that the system intrusion was a de minimis event. SEC alleged that ICE violated its own internal cyber incident reporting procedures. As a result, the subsidiaries allegedly did not fulfill their regulatory disclosure obligations under Regulation SCI, which requires them to immediately contact SEC staff about the intrusion and provide an update within 24 hours unless they immediately concluded or reasonably estimated that the intrusion had or would have no or a de minimis impact on their operations or on market participants.

ICE and its subsidiaries consented to the entry of the SEC's order and agreed to pay a $10 million fine without admitting or denying the SEC's findings.

SEC Commissioners Peirce and Uyeda issued a statement of dissent over the SEC's penalty, stating that a "$10 million civil penalty on ICE for its subsidiaries' failure to notify the Commission of a single, *de minimis* incident is an overreaction."

Broker-Dealer Receives Remedial Sanctions Concerning Reg BI Disclosure Failure

On May 21, 2024, the SEC settled charges with dually registered broker-dealer and investment adviser Key Investment Services for failure to comply with Regulation BI's Disclosure Obligation, Conflict of Interest Obligation, and Compliance Obligation, which require broker-dealers to, among other things, provide certain prescribed written disclosures to their customers; have policies and procedures reasonably designed to identify and address conflicts of interest; and establish, maintain and enforce written policies and procedures reasonably designed to achieve compliance with Regulation BI.

According to the SEC's order, Key Investment Services, through its registered representatives and investment adviser representatives, recommended that certain of its brokerage customers and advisory clients transfer securities from Key Investment Services accounts to new investment accounts with Key Investment Services' affiliate Key Private Bank, a wealth management firm that is part of the same parent organization, without disclosing that the representatives would receive compensation for making the recommendations and for any securities transfers. The SEC also alleged that Key Investment Services' written policies and procedures were not reasonably designed to achieve compliance with Key Investment Services' disclosure obligations under Regulation BI and the Advisers Act.

Federal Court Rules That Crypto Influencer Conducted Unregistered Offering of Crypto Asset Securities

On May 22, 2024, the U.S. District Court for the Western District of Texas granted partial summary judgment to the SEC against crypto influencer Ian Balina. The Court held that the SEC prevailed as a matter of law as to its unregistered offering claim and that Balina offered and sold crypto assets called SPRK Tokens as securities in unregistered transactions and U.S. securities laws apply to Balina's conduct.

In Case You Missed It:

SEC Director of Corporation Finance Issues Statement Concerning Materiality and Reporting of Cybersecurity Incidents

On May 21, 2024, SEC Director of the Division of Corporation Finance Erik Gerding issued a statement concerning the disclosure of cybersecurity incidents. While material cybersecurity incidents are required to be reported on a firm's 8-K, Director Gerding wanted to clarify the efficacy and method of reporting incidents for which the materiality thereof had not yet been determined, or which was determined to be immaterial.

The statement also reiterated the factors in determining an incident's materiality, namely by assessing the incident's impact (or reasonably likely impact), not limited to the impact on the firm's "financial condition and results of operation." Further, "companies should consider qualitative factors alongside quantitative factors."

FINRA Initiates Remote Inspections Program

FINRA's voluntary, three-year Remote Inspections Pilot Program starts on July 1, 2024 and ends on June 30, 2027. Under the Pilot Program, eligible member firms will have the flexibility to satisfy their inspection obligation under FINRA Rule 3110(c)(1)(A), (B) and (C) without an on-site visit to the office or location, subject to specified terms that include conducting and documenting a risk assessment and producing written supervisory procedures for conducting remote inspections and inspection data to FINRA.

A firm that participates in the Pilot Program must conduct and document a risk assessment for that office or location. The assessment must document the factors considered, including, but not limited to, the firm's size, number and location of offices, the nature and complexity of the products and services the firm offers and the volume of business, and must take into account any higher risk activities that take place at, or higher risk associated persons that are assigned to, that office or location.

Factors a Pilot Program participant must consider as part of the risk assessment include, but are not limited to:

- The volume and nature of customer complaints;

- The volume and nature of outside business activities, particularly investment-related;
- The volume and complexity of products offered;
- The nature of the customer base, including vulnerable adult investors;
- Whether associated persons are subject to heightened supervision;
- Failures by associated persons to comply with the member's written supervisory procedures; and
- Any recordkeeping violations.

In addition, consistent with Rule 3110.12, a Pilot Program participant should conduct on-site inspections or make more frequent use of unannounced, on-site inspections for high-risk offices or locations or where there are indicators of irregularities or misconduct (*i.e.*, "red flags"). Moreover, a Pilot Program participant must develop a reasonable risk-based approach to using remote inspections, and consistent with Rule 3110(a), the supervisory system must take into consideration any red flags when determining whether to conduct a remote inspection of an office or location.

Furthermore, a Pilot Program participant must have written supervisory procedures that must cover:

- the methodology, including technology, that may be used to conduct remote inspections;
- the factors considered in the risk assessment;
- the use of other risk-based systems employed generally by the member to identify and prioritize for review those areas that pose the greatest risk of potential violations of applicable securities laws and regulations and of applicable FINRA rules;
- procedures for escalating significant findings;
- procedures for new hires;
- procedures for supervising brokers with a significant history of misconduct;
- procedures related to outside business activities (OBAs) and doing business as (DBA) designations; and
- compliance with data and information collection, and transmission under Rule 3110.18(h).

FINRA has published a FAQ for the program on their website.

FINRA Publishes AI Communication Guidance

FINRA added to their advertising regulation guidance new FAQ concerning the use of AI communication. FINRA's FAQ states that, depending on the nature and number of persons receiving chatbot communications, the communications may be subject to FINRA communications rules as correspondence, retail communications, or institutional communications. Therefore, chatbot communications must be supervised by the distributing firm in accordance with applicable FINRA rules. See FINRA Rules 2210(a), 2210(b), and h3110(b)(4) and 3110.06 through .09. Among other things, Rule 3110(b)(4) requires firms to establish, maintain, and enforce written procedures for the review of incoming and outgoing written (including electronic) correspondence relating to the firm's investment banking or securities business that must be appropriate for the member's business, size, structure, and customers. In addition, the content must be consistent with applicable standards, such as those in FINRA Rule 2210(d).

Crypto Firm Settles CFTC Charges for Failing to Register as an FCM

On May 13, 2024, a crypto prime brokerage firm settled CFTC charges for failing to register as a futures commission merchant ("FCM"). In a press release accompanying the enforcement order, the CFTC said the case marks its first action against an unregistered FCM that inappropriately facilitated access to digital asset exchanges.

According to the Order, the firm solicited orders from U.S. customers for digital asset derivatives, including futures and swaps, and accepted money and property in connection with those orders. The CFTC found that the firm provided its customers with direct access to exchanges by first creating a main account in its own name and then creating associated sub-accounts. The CFTC stated that the exchanges generally did not require, and the firm generally did not provide, customer-identifying information for the sub-account holders. The CFTC found that the firm violated Commodity Exchange Act Section 4d(a)(1) (7 U.S.C. § 6d(a)(1)).

In a concurring statement, CFTC Commissioner Caroline D. Pham agreed with the CFTC's finding that the firm had violated the law but criticized, among other aspects of the order, the CFTC's approach to establishing jurisdiction.

Congressional Research Service Issues Considerations for Central Bank Digital Currencies

On May 12, 2024, Congressional Research Service published a report that identified policy issues in the current debate on whether the Federal Reserve should create a central bank digital currency ("CBDC").

The report reviewed the 2022 Fed report on a potential CBDC, which it defined as "a digital liability of a central bank that is widely available to the general public." The Fed report identified four characteristics necessary "to best serve the needs of the United States." Namely, that a CBDC should be (i) privacy-protected to the extent compatible with deterring criminal use, (ii) intermediated (sold or distributed through financial institutions), (iii) widely transferable among holders and (iv) identity-verified (not anonymous).

The report highlighted the following key policy considerations for Congress, including that CBDCs could:

- raise more legal and practical challenges in cross-border payments than domestic use;
- displace private activity by partially displacing crypto and maintaining the government's role in issuing money;
- promote financial inclusion which would "depend largely" on whether CBDCs were less expensive and easier to access than traditional banking services;
- prevent bank runs through a "partial shift" from private bank accounts, or because of a consumer's option to switch to an alternative to CBDC accounts during periods of bank distress;
- prevent illicit activity, such as tracking and storing information regarding users and transactions;
- reduce user privacy, but ultimately curb criminal activity, including money laundering; and
- potentially cause the U.S. dollar to decline if central banks in other countries offer cross-border payment options via CBDC initiatives.

House Passes CBDC Anti-Surveillance State Act

On May 23, 2024, the U.S. House of Representatives passed H.R. 5403, the CBDC Anti-Surveillance State Act, which prevents "unelected bureaucrats" from issuing a central bank digital currency (CBDC) without explicit authorization from Congress. According to Chairman of the House Financial Services Committee Patrick McHenry, the bill would "[halt] unelected bureaucrats from issuing a central bank digital currency, or CBDC, that would be detrimental to Americans' right to financial privacy." As an example of such a detriment to

privacy, the representative cited “the Chinese Communist Party [use of] a CBDC to track spending habits of its citizens.”

Congressional Members Deliver Letter Urging Implementation of the Financial Data Transparency Act

On May 14, 2024, the Chair of the House Financial Services Committee, Patrick McHenry, Ranking Member Maxine Waters, U.S. Senator Mike Crapo and U.S. Senator Mark Warner urged federal financial regulators to finalize rulemakings implementing the Financial Data Transparency Act. In the letter, the legislators argued that "Publishing machine-readable data in a consistent format will facilitate the use of these technologies [e.g., data sifting algorithms and AI], leading to increased transparency and greater market efficiencies."