Q3 2024

WILSON SONSINI

Focus on Fintech

Welcome to Wilson Sonsini's *Focus on Fintech* newsletter. This quarterly newsletter provides ongoing analysis and commentary on regulatory developments impacting the fintech industry.

In this issue, our attorneys discuss updates and developments from federal regulators, including those related to bank-fintech partnerships, cryptocurrency and virtual currency updates, and consumer protection. We also discuss rule updates from the SEC, FinCEN, and CFTC.

In This Issue

Bank-Fintech Partnerships

Agencies Remind Banks of Potential Risks Associated with Third-Party Deposit Arrangements and Request Additional Information on Bank-Fintech Arrangements

The Federal Reserve, FDIC, and OCC (the Agencies) recently released a joint statement regarding bank-fintech arrangements under which third parties, such as fintech companies, deliver bank deposit products and services. Although the statement expresses the Agencies' support for continued innovation and collaboration in the financial industry, it also emphasizes that banks relying on third parties to provide certain services nevertheless continue to bear responsibility for compliance with all applicable laws, including consumer protection and anti-money laundering requirements. The statement provides supervisory observations on potential risks, examples of effective practices for managing such risks, and a list of various compliance resources (including existing guidance) that may assist banks in managing such arrangements. Fintech companies that partner or wish to partner with banks in connection with deposit products and services may also find the statement helpful.

FDIC Issues Proposed Rule to Revise Brokered Deposit Regulations

The FDIC issued a notice of proposed rulemaking on July 30, 2024, proposing revisions to its regulations relating to the brokered deposits restrictions that apply to less than well-capitalized insured depository institutions. Adequately capitalized banks may not accept brokered deposits without an approved waiver from the FDIC, and banks that are less than adequately capitalized may not accept them at all. The proposed rule would revise the "deposit broker" definition, amend the analysis of the "primary purpose" exception to the "deposit broker" definition, and eliminate the "exclusive deposit placement arrangement" exception, among other changes. The proposed rule, if finalized, would result in fewer entities being exempt from the definition of "deposit broker" than is the case currently and, therefore, a significant amount of deposits could be reclassified as brokered.

Continued on page 2...

Bank-Fintech *(Continued from page 1)*

FDIC Proposes Deposit Insurance Recordkeeping Rule for Banks' Third-Party Accounts

The FDIC issued a notice of proposed rulemaking on September 17, 2024, inviting public comments on a proposed regulation that would enhance the recordkeeping obligations of insured depository institutions (IDIs) for deposit accounts with transactional features. In the proposal, the FDIC noted the recent events surrounding the bankruptcy of Synapse raised questions about the completeness, accuracy, and integrity of custodial deposit account records underlying arrangements with third parties at certain IDIs. Under the proposed rule, IDIs with custodial deposit accounts that are not exempt would be required, themselves or through a third party, to maintain records of beneficial ownership in in a specific data format and layout prescribed by the proposed rule for each custodial deposit account. In addition, these IDIs would be required to reconcile records for their custodial deposit accounts as of the end of each business day in order to determine the respective individual beneficial ownership interests associated with the custodial deposit account and the reconciliation of such interests to the funds on deposit in the custodial deposit account. IDIs likely do not currently have these records. Therefore, the rule, if finalized, would require IDIs to revise their existing platforms or core processing systems, as well as to develop data interface systems with any third parties they rely on for recordkeeping.

Consumer Protection Updates

CFPB Report Finds Large Retail Chains Charging Cash-back Fees to Customers Using Debit and Prepaid Cards

The Consumer Financial Protection Bureau (CFPB) has released a report on consumers' use of "cash back" services, an option consumers use to get cash at a store when making a purchase with a debit or prepaid card, and the fees some retailers charge for these transactions. Among other findings, the report noted that cash-back fees cost consumers millions of dollars each year and are levied on even low withdrawal amounts, where they can represent a disproportionately high percentage of the transaction, which could induce repeat withdrawals, with consumers incurring a new fee each time.

CFPB Issues Circular Regarding Improper Overdraft Opt-in Practices

The CFPB issued a circular clarifying its position on the question of whether a financial institution violates the law if there is no proof that it has obtained consumers' affirmative consent before levying overdraft fees for ATM and one-time debit card transactions. The CFPB's answer is yes, a bank or credit union can be in violation of the Electronic Fund Transfer Act and Regulation E if there is no proof that it obtained affirmative consent to enrollment in covered overdraft services. The circular further notes that Regulation E's overdraft provisions establish an opt-in regime, not an opt-out regime, where the default condition is that consumers are not enrolled in covered overdraft services. Financial institutions are prohibited from charging fees for such services until consumers affirmatively consent to enrollment.

The guidance cautions that, in the course of the CFPB's supervisory work, examinations have found that some institutions have been unable to provide evidence that consumers had opted into overdraft coverage before they were charged fees for ATM and one-time debit transactions. The guidance further warns of additional lapses in compliance observed by the CFPB, such as financial institutions' failure to obtain consumers' affirmative consent to enrollment in covered overdraft services and their obtaining consumer consent through deceptive and abusive acts or practices.

Continued on page 3...

Regulation and Enforcement Involving Regulated Securities Intermediaries

FinCEN Finalizes Rule Requiring AML/CFT Programs for Registered Investment Advisers and Exempt Reporting Advisers

The Financial Crimes Enforcement Network (FinCEN) has finalized a rule requiring Registered Investment Advisers (RIAs) and Exempt Reporting Advisers (ERAs) to establish and maintain anti-money laundering (AML) and countering the financing of terrorism (CFT) programs. This expansion redefines RIAs and ERAs as "financial institutions" under the Bank Secrecy Act (BSA), subjecting them to the same AML/CFT requirements that have historically applied to banks, broker-dealers, and other financial entities.

The rule aims to mitigate risks associated with illicit financial activity and strengthen national security protections, addressing concerns that advisers' lack of regulatory oversight created vulnerabilities in the U.S. financial system. Under the new framework, RIAs and ERAs must implement written AML programs tailored to their size, structure, and risk profile. These programs must include policies and procedures for detecting and reporting suspicious activities, appointing AML compliance officers, and conducting independent audits.

FinCEN has set January 1, 2026, as the compliance deadline, providing firms time to adapt their operations and establish the necessary systems. This regulatory shift marks the first time these advisers are formally integrated into the BSA's AML/CFT regime, highlighting the federal government's commitment to closing gaps in financial crime prevention and aligning with global standards.

The rule also mandates advisers to file suspicious activity reports (SARs) for transactions that meet specific thresholds or raise red flags of potential money laundering or terrorist financing. It extends to ERAs, which include certain private fund advisers exempt from full SEC registration, underscoring the broad scope of these measures.

For further details, see our alert here.

SEC Charges Crypto-Focused Advisory Firm Galois Capital Management for Custody Failures

The U.S. Securities and Exchange Commission (SEC) has reached a settlement with Galois Capital Management LLC (Galois) based on alleged violations of the Investment Advisers Act of 1940 (Advisers Act) related to, among other things, improper custody of crypto asset securities, false and misleading statements regarding redemption practices, and inadequate compliance policies.

According to the SEC order, Galois failed to maintain client crypto asset securities with qualified custodians (e.g., a bank or broker-dealer), as required under Rule 206(4)-2 under the Advisers Act (the Custody Rule), and instead kept assets on trading platforms that were not registered banks, brokers, or other intermediaries—including FTX. Importantly, it is unclear that compliance with the Custody Rule is possible with respect to crypto asset securities. Galois also misled investors in a fund it managed by allegedly allowing certain investors, including affiliates, to redeem their investments with less notice than disclosed to others. Additionally, Galois also allegedly neglected to implement necessary written compliance policies during its registration period with the SEC.

The SEC charged that Galois was in willful violation of the antifraud provisions of the Advisers Act as well as, among other rules, the Custody Rule. As part of the settlement, Galois agreed to a cease-and-desist order, censure, and a $225,000 civil penalty, but did not admit or deny the SEC's findings in the order.

SEC Charges OTC Link LLC with Failing to File Suspicious Activity Reports

The SEC has issued an order settling charges against OTC Link LLC (OTC Link) for alleged violations of the Securities Exchange Act of 1934 (Exchange Act). OTC Link, a broker-dealer operating multiple alternative trading systems, facilitates tens of thousands of daily transactions involving over-the-counter (OTC) securities, including many classified as microcap or penny stocks. OTC Link allegedly failed to file Suspicious Activity Reports (SARs) for numerous suspicious financial transactions between March 2020 and May 2023. The SEC stated that these failures arose from inadequate anti-money laundering (AML) policies, insufficient surveillance of trading activity, and understaffed compliance efforts.

The SEC found that OTC Link did not properly investigate or report suspicious activities, such as large-volume trades in thinly traded securities, pre-arranged trades including wash or cross trades in thinly-traded securities, and transactions involving parties with known regulatory or criminal histories. The deficiencies allegedly allowed potentially fraudulent activities to go unreported.

In response, OTC Link agreed to remedial measures, including hiring additional compliance staff and retaining a third-party consultant to review and

Continued on page 4...

Regulation and Enforcement *(Continued from page 3)*

enhance its AML policies. As part of the settlement, OTC Link, without admitting or denying the findings in the order, consented to a cease-and-desist order, censure, and a $1.19 million civil penalty. It also committed to ongoing compliance enhancements and periodic reviews by the SEC.

SEC Charges Transfer Agent Equiniti Trust Co. with Failing to Protect Client Funds Against Cyber Intrusions

The SEC has announced a settlement with Equiniti Trust Company, LLC (Equiniti), formerly known as American Stock Transfer & Trust Company, LLC, addressing alleged violations of Section 17A(d) and Rule 17Ad-12 under the Exchange Act. The alleged violations stemmed from cybersecurity failures that the SEC charged left client funds and securities vulnerable to theft, resulting in two significant cyber incidents in 2022 and 2023, with total losses amounting to approximately $4.08 million.

According to the order, in September 2022 a threat actor impersonated a legitimate client and infiltrated an ongoing email chain to direct Equiniti to issue millions of new shares of a client's stock, liquidate them, and transfer the proceeds—approximately $4.78 million—to bank accounts in Hong Kong. Equiniti's employee allegedly failed to detect the fraudulent email address and did not verify the instructions through required call-back procedures. The fraud was discovered two months later, and Equiniti managed to recover $1 million. It fully reimbursed the affected client for the remaining losses.

In April 2023, a separate threat actor exploited vulnerabilities in Equiniti's online platform, which automatically linked accounts based on matching Social Security numbers. Using stolen Social Security numbers, the attacker gained access to legitimate accounts, liquidated securities, and transferred approximately $1.9 million in proceeds to external accounts. This breach was detected only after a bank flagged the transactions. Approximately $1.6 million was recovered and Equiniti reimbursed the remaining $300,000 in losses. Following the incident, Equiniti shut down its online portal, launched an investigation, and implemented system enhancements to prevent similar attacks, including removing the default linking feature.

The SEC found that Equiniti failed to ensure adequate safekeeping of securities and protection of funds, as required under Rule 17Ad-12, and willfully violated the Exchange Act by neglecting to address evident risks of theft and misuse. As part of the settlement, Equiniti agreed, without admitting or denying the findings, to a cease-and-desist order, censure, and an $850,000 civil penalty. In determining penalties, the SEC recognized the company's remedial actions, including hiring a Chief Control Officer, engaging a third-party cybersecurity firm, and fully compensating affected clients for their losses.

SEC Enforcement Involving Cryptocurrency and Digital Assets

eToro Reaches Settlement with SEC and Ceases Trading Activity in Nearly All Crypto Assets

eToro USA LLC (eToro) has agreed to pay $1.5 million to settle SEC charges that it has been operating as an unregistered broker and clearing agency, in violation of Sections 15(a) and 17A of the Securities Exchange Act of 1934 (Exchange Act). eToro provided U.S. customers with a trading platform for crypto assets, including crypto asset securities.

According to the settlement order, from 2020 onwards, eToro facilitated transactions in crypto assets for approximately 240,000 U.S. customers, acting as an intermediary by holding customer funds, maintaining omnibus wallets for crypto assets, and processing trades. The SEC found that eToro's actions met the definitions of a broker and clearing agency under the Exchange Act, but eToro failed to register in either capacity.

In response, without admitting or denying the findings in the order, eToro has ceased offering most crypto assets to U.S. customers, limiting its services to Bitcoin, Bitcoin Cash, and Ether transactions. The company also agreed to liquidate any remaining unsupported crypto assets held in customer accounts within 180 days of the order and return proceeds to affected customers.

As part of the settlement, eToro agreed to a cease-and-desist order and make changes to its operations, along with paying the monetary penalty.

Continued on page 5...

SEC Enforcement *(Continued from page 4)*

SEC Charges Nader Al-Naji with Fraud and Unregistered Offering of Crypto Asset Securities

The SEC has filed charges against Nader Al-Naji, founder of blockchain-based platform BitClout (now rebranded as Decentralized Social (DeSo)), in the United States District Court for the Southern District of New York alleging fraudulent activities and violations of securities laws. According to the SEC, Al-Naji raised over $257 million through the unregistered sale of BitClout's native token, BTCLT, and falsely claimed the project was decentralized. He allegedly diverted more than $7 million of investor funds for personal expenses, including luxury purchases for himself and gifts to family members.

The SEC's complaint states Al-Naji misled investors by portraying BTCLT as an investment tied to the platform's success, with promises of eventual trading on external platforms. Using the pseudonym "Diamondhands," Al-Naji allegedly sought to obscure his control over the project while privately admitting to attempts to evade regulatory scrutiny. Al-Naji allegedly used investor proceeds to finance his lifestyle and compensate project developers despite making claims that funds would not be used for personal gain. The SEC seeks financial penalties, disgorgement of gains, and injunctions to prevent future violations.

SEC Charges DeFi Platform Rari Capital and Its Founders with Misleading Investors and Acting as Unregistered Brokers

The SEC entered into a settlement with Rari Capital Infrastructure LLC (Rari Capital) based on alleged violations of Sections 5(a) and 5(c) of the Securities Act of 1933 (Securities Act) and Section 15(a) of the Exchange Act for operating as an unregistered broker and offering unregistered securities. Among other things, Rari Capital operated a crypto asset trading platform called Fuse, which allowed users to create and participate in pools for depositing and borrowing crypto assets.

Users depositing crypto assets received tokens, known as "fTokens," representing their share of interest earned from borrowing activity within each pool. The complaint alleges that these tokens were investment contracts and thus securities, which required registration of the distribution under the Securities Act. Rari Capital also collected performance-based fees of approximately 10 percent on the interest earned in these pools, tying its fortunes to those of the investors.

The platform code was hacked in May 2022, resulting in theft of $80 million in crypto assets. Following this, Rari Capital ceased operations, began winding down the platform, and used the $2.32 million in collected fees to compensate affected users. At its peak, Fuse handled crypto assets with a market value of approximately $1 billion and facilitated transactions for over 10,000 users.

As part of the settlement, Rari Capital agreed to cease and desist from future violations but was not assessed a monetary penalty due to its cooperation and remedial actions, including halting the platform and returning collected fees to harmed users.

SEC Charges Crypto Companies TrustToken and TrueCoin with Defrauding Investors Regarding Stablecoin Investment Program

The SEC settled charges against TrueCoin LLC and TrustToken, Inc. that were filed in the United States District Court for the Northern District of California and alleged violations of federal securities laws related to 1) the unregistered offer and sale of securities and 2) fraudulent misstatements about the backing of the purported stablecoin, TrueUSD (TUSD). TrueCoin was the issuer of TUSD, and TrustToken was the developer and operator of TrueFi, a purported lending protocol.

According to the complaint, TUSD was falsely marketed as being safe, fully collateralized, and "1:1" backed by the U.S. dollar. In reality, a significant portion of its reserves was invested in a high-risk offshore commodity fund (Fund) beginning in 2020. By Fall 2022, TrueCoin and TrustToken became aware that the Fund was facing redemption delays and liquidity issues, but continued to market claims that TUSD reserves were liquid, secure, and backed one-for-one by US dollars. According to the SEC, by September 2024, 99 percent of the reserves were invested in the Fund.

SEC Enforcement *(Continued from page 5)*

Between November 2020 and April 2023, the companies offered TUSD and associated lending opportunities on TrueFi, allowing investors to earn interest by lending TUSD to uncollateralized borrowers. The SEC alleges that these offerings constituted unregistered offerings of securities and that the companies failed to disclose material risks associated with the reserves backing TUSD.

Without admitting or denying the allegations, TrueCoin and TrustToken agreed to settle the charges by consenting to final judgments enjoining them from violating applicable provisions of the federal securities laws and to pay civil penalties of $163,766 each. TrueCoin agreed to pay disgorgement of $340,930 with prejudgment interest of $31,538. The settlements are subject to court approval.

SEC Charges Entities Operating Crypto Asset Trading Platform Mango Markets for Unregistered Offers and Sales of the Platform's "MNGO" Governance Tokens

The SEC settled charges with Mango Labs LLC (Mango Labs), Mango DAO, and Blockworks Foundation, alleging violations of federal securities laws for engaging in the unregistered offering and sale of MNGO tokens and failing to register as a broker-dealer. These charges relate to the operation of the crypto asset trading platform Mango Markets. Mango Markets, built on the Solana blockchain, facilitated trading in crypto assets the SEC charges were offered and sold as securities.

According to the complaint, Mango DAO and Blockworks Foundation raised over $70 million in August 2021 through the unregistered sale of 500 million MNGO tokens. The SEC argues that as the "governance token" of Mango Markets, MNGO tokens were sold as investment contracts and therefore, securities. They further allege that the companies' failure to register denied investors essential protections under the federal securities laws.

The SEC also alleges that Blockworks Foundation and Mango Labs performed brokerage functions by soliciting users, providing investment advice, and handling user funds and crypto asset securities on the Mango Markets platform. Neither entity took steps toward broker-dealer registration.

The SEC seeks to permanently enjoin the defendants, who did not admit or deny the findings, from further violations of the federal securities laws and to impose monetary penalties.

CFTC Enforcement Regarding Cryptocurrency and Digital Assets

CFTC Issues Order Against Uniswap Labs for Offering Illegal Digital Asset Derivatives Trading

The Commodity Futures Trading Commission (CFTC) has settled with Universal Navigation Inc., operating as Uniswap Labs, for allegedly violating Section 2(c)(2)(D) of the Commodity Exchange Act (CEA), which generally prohibits engaging in transactions in commodities with retail investors on a leveraged or margined basis if the transaction does not result in delivery within 28 days; without that delivery, the agreement is subject to Section 4(a) of the CEA, which generally requires that all commodities futures contracts are traded on exchange. Uniswap Labs facilitated off-exchange leveraged commodity transactions via its decentralized digital asset trading protocol and web interface, which allowed users to trade digital assets, including leveraged tokens, without proper registration. The transactions involved commodities such as Bitcoin and Ethereum and were available to retail users who were not, as typically required, "eligible contract participants" as defined in the CEA.

The CFTC found that the leveraged tokens offered through Uniswap's interface did not result in actual delivery of underlying assets within 28 days, violating rules for retail commodity transactions. During the relevant period, over $21.5 million in such trades occurred, representing less than 0.25 percent of total platform activity. The order acknowledges Uniswap Labs'cooperation and remediation efforts, reflected in a reduced civil monetary penalty of $175,000. Uniswap Labs consented to the order without admitting or denying the findings, agreeing to cease further violations and enhance compliance measures.

CFTC Obtains $12.7 Billion Judgment Against FTX and Alameda

The CFTC has settled with FTX Trading Ltd. (FTX) and Alameda Research LLC (Alameda) based on alleged violations of the CEA through fraud, misappropriation, and improper use of customer funds. The entities, controlled by founder Samuel Bankman-Fried, were found to have (among other things) commingled billions of dollars in customer assets, using them for speculative trading, loan repayments, and business expenses, despite public assurances that funds were secure. Alameda had undisclosed privileges, including unlimited withdrawals and immunity from liquidation, which enabled its misuse of funds deposited on the FTX platform.

The consent order imposes a permanent trading ban on FTX and Alameda and mandates the repayment of $8.7 billion in customer restitution and $4 billion in disgorgement through bankruptcy proceedings.

Federal Reserve Enforcement Regarding Cryptocurrency and Digital Assets

Federal Reserve Board Fines Silvergate Capital Corporation and Silvergate Bank $43 Million for Deficiencies in Compliance with Anti-Money Laundering Law

The Federal Reserve Board imposed on Silvergate Capital Corporation, a bank holding company, and Silvergate Bank (together, Silvergate), a $43 million civil penalty for alleged deficiencies in their monitoring of transactions in compliance with anti-money laundering laws. The penalty stems from a Federal Reserve Board investigation into the operations of Silvergate Bank that identified deficiencies in Silvergate's monitoring of on-us book transfers through the Silvergate Exchange Network (SEN). The order describes SEN as an internal platform launched by Silvergate to facilitate near real time, on-us transfers of U.S. dollars between Silvergate customers engaged in buying and selling crypto-assets.

The Federal Reserve's action was taken in coordination with an action by the Department of Financial Protection and Innovation of the State of California, the state supervisor of Silvergate Bank. The penalties announced by the Board and state total $63 million. The SEC separately announced a penalty against Silvergate Capital Corporation. Silvergate Bank began voluntarily winding down operations in March 2023; in July 2023, Silvergate agreed to a cease-and-desist order with the Federal Reserve intended to facilitate the voluntary self-liquidation.

Select Publications

Wilson Sonsini Alert
Five Issues for Wealthtech Companies to Consider Under the U.S. Securities Laws
July 24, 2024

Wilson Sonsini Alert
The Critical Reporting Requirement U.S. Companies Can't Afford to Ignore: Upcoming Deadlines for Beneficial Ownership Information Compliance
August 14, 2024

Fintech in Brief
Fintech in Brief: Recent SEC Enforcement Activity on the Custody Rule: Clues for the Focus of Anticipated Rules on Safekeeping Client Assets?
September 11, 2024

Wilson Sonsini Alert
FinCEN Finalizes Rule Requiring AML/CFT Programs for Registered Investment Advisers and Exempt Reporting Advisers
October 3, 2024

Speaking Engagements

Wilson Sonsini Partner Jess Cheng Speaks at APABA-DC's Women's Forum and Government Attorneys Forum

Fintech and financial services partner Jess Cheng recently spoke on a fintech panel titled, "Legal, Regulatory, and Policy Leaders," at the APABA-DC's Women's Forum and Government Attorneys Forum. Also joining the panel were Linda Jeng (Digital Self Labs, Georgetown, Duke), Suyash Paliwal (CFTC), and Sanjeev Bhasker (White House).

Wilson Sonsini Partner Jess Cheng Speaks at ETA Transact Tech NYC Conference

Fintech and financial services partner Jess Cheng spoke on the "Artificial Intelligence and Fintechs" panel at the ETA Transact Tech NYC Conference on October 16, joining Donald Riddick (Featurespace) and Kevin Shamoun (Fortis Pay). The panel focused on the benefits and challenges that AI technologies pose for payments and fintechs.

Amy Caiazza
(202) 973-8887
acaiazza@wsgr.com

Jess Cheng
(212) 453-2853
jcheng@wsgr.com

Josh Kaplan
44-20-39634069
jkaplan@wsgr.com

Stephen Heifetz
(202) 973-8802
sheifetz@wsgr.com

Maneesha Mithal
(202) 973-8834
mmithal@wsgr.com

Drew Minick
(415) 947-2075
dminick@wsgr.com

Troy Jenkins
(202) 920-8732
tjenkins@wsgr.com

Clinton Oxford
(202) 920-8750
coxford@wsgr.com

Alice Cao
(202) 973-8967
alice.cao@wsgr.com

WILSON SONSINI

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Wilson Sonsini has 18 offices in technology and business hubs worldwide. For more information, visit wsgr.com/offices.