

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION**

ERIK DAVIDSON, JOHN RESTIVO, and NATIONAL
CENTER FOR PUBLIC POLICY RESEARCH,

Plaintiffs,

-against-

GARY GENSLER, U.S. SECURITIES AND
EXCHANGE COMMISSION, and CONSOLIDATED
AUDIT TRAIL, LLC,

Defendants.

Case No. 6:24-cv-00197-ADA

**BRIEF OF *AMICI CURIAE*
BLOCKCHAIN ASSOCIATION AND DEFI EDUCATION FUND**

TABLE OF CONTENTS

INTERESTS OF *AMICI CURIAE* 1

INTRODUCTION AND SUMMARY OF ARGUMENT 2

STATEMENT OF FACTS 5

 A. Blockchains, Cryptocurrency, and Wallets..... 5

 B. Traditional Finance Firms Are Offering Services Related to Digital Assets..... 6

 C. The CAT and the NMS Plan..... 8

 D. The SEC Believes that Many Digital Asset Market Participants Are “Exchanges,”
 “Brokers,” and/or “Dealers,” Meaning That Those Entities Will Have to Report
 Blockchain Information to the CAT 9

ARGUMENT 13

 I. THE CAT WOULD SWEEP IN BLOCKCHAIN-BASED INFORMATION,
 RISKING A MASSIVE INVASION OF PERSONAL PRIVACY FOR MILLIONS
 13

 II. THE CAT DATABASE IS VULNERABLE TO DATA LOSS OR HACKING 16

CONCLUSION..... 19

TABLE OF AUTHORITIES

Cases

Cal. Bankers Ass’n v. Schultz,
416 U.S. 21 (1974)..... 15

Carpenter v. U.S.,
585 U.S. 296 (2018)..... 15

Kyllo v. U.S.,
533 U.S. 27 (2001)..... 15

Matter of Search of Multiple Email Accts.,
585 F. Supp. 3d 1 (D.D.C. 2022)..... 6

Olmstead v. U.S.,
277 U.S. 438 (1928)..... 20

Risley v. Universal Navigation Inc.,
690 F. Supp. 3d 195 (S.D.N.Y. 2023) 5

SEC v. Coinbase, Inc.,
2024 U.S. Dist. LEXIS 56994 (S.D.N.Y. Mar. 27, 2024) 5

Statutes and Regulations

17 C.F.R. § 242.613(a)(1)..... 8

17 C.F.R. § 242.613(j)(7)..... 14

81 Fed. Reg. 84696..... 9

87 Fed. Reg. 15646..... 10

88 Fed. Reg. 29448..... 11

89 Fed. Reg. 14938..... 12

Pleadings

Crypto Freedom All. of Tex, et al. v. SEC, et al., Case No. 4:24-cv-00361-O, ECF No. 1 (N.D. Tex. Apr. 23, 2023)..... 13

S.E.C. v. Beaxy Digital, Ltd., et al., No. 23-cv-1962, ECF No. 1 (N.D. Ill. Mar. 29, 2023)..... 12

S.E.C. v. Binance Holdings Limited, et al., No. 1:23-cv-01599, ECF No. 1 (D.D.C. June 5, 2023)
..... 10, 11, 12

S.E.C. v. Coinbase, Inc. et al., No. 23 Civ. 4738, ECF No. 1 (S.D.N.Y. June 6, 2023)..... 10, 11

S.E.C. v. Consensus Software Inc., No. 24 Civ. 4578, ECF No. 1 (E.D.N.Y. June 28, 2024) 11

S.E.C. v. Payward, Inc., et al., No. 3:23-cv-06003, ECF No. 1 (N.D. Cal. Nov. 20, 2023).. 10, 11, 12

Comment Letters

Jake Chervinsky & Marisa T. Coppel, Blockchain Association, Comment Letter on Reopening of the Comment Period: Proposed Amendments to Exchange Act Rule 3b-16 (June 13, 2023), <https://www.sec.gov/comments/s7-02-22/s70222-204059-410802.pdf>..... 10

Jake Chervinsky, Blockchain Association & Miller Whitehouse-Levine, DeFi Education Fund, Comment Letter on Amendments to Exchange Act Rule 3b-16 (June 13, 2022), <https://www.sec.gov/comments/s7-02-22/s70222-20131087-301122.pdf>..... 10

Kristin Smith & Jake Chervinsky, Blockchain Association, Comment Letter on Amendments to Exchange Act Rule 3b-16 (Apr. 18, 2022), <https://www.sec.gov/comments/s7-02-22/s70222-20124039-280165.pdf>..... 10

Kristin Smith & Jake Chervinsky, Blockchain Association, Comment Letter on Proposed Further Definition of the Dealer Rule (May 27, 2022), <https://www.sec.gov/comments/s7-12-22/s71222-20129925-296179.pdf>..... 12

Miller Whitehouse-Levine & Amanda Tuminelli, Comment Letter on Reopening of the Comment Period; Proposed Amendments to Exchange Act Rule 3b-16 (June 12, 2023), <https://www.sec.gov/comments/s7-02-22/s70222-202979-407862.pdf>..... 10

Miller Whitehouse-Levine, DeFi Education Fund, Comment Letter on Amendments to Exchange Act Rule 3b-16 (Apr. 18, 2022), <https://www.sec.gov/comments/s7-02-22/s70222-20123960-280119.pdf>..... 10

Miller Whitehouse-Levine, DeFi Education Fund, Comment Letter on Proposed Further Definition of the Dealer Rule (May 27, 2022), <https://www.sec.gov/comments/s7-12-22/s71222-20131214-296907.pdf>..... 13

Other Authorities

Amanda Tuminelli & Marisa T. Coppel, *Crypto’s Latest Privacy Battle*, CoinDesk (June 5, 2024, 3:39 PM), <https://www.coindesk.com/opinion/2024/06/05/cryptos-latest-privacy-battle/> 2

Andrew Ackerman, *CFPB Says Staffer Sent 250,000 Consumers’ Data to Personal Account*, The Wall Street Journal (Apr. 19, 2023, 4:35 PM), <https://www.wsj.com/articles/in-major-incident-cfpb-says-staffer-sent-250-000-consumers-data-to-personal-account-fdc0a540> 17

Bitcoin ETFs List, VettaFi (Aug. 19, 2024), <https://etfdb.com/themes/bitcoin-etfs/>; *Ethereum ETFs List*, <https://etfdb.com/themes/ethereum-etfs/>..... 8

| | |
|--|--------|
| <i>BTC Explorer by Redot</i> , Btcsan, https://btcsan.org/ | 6 |
| <i>Citi Develops New Digital Asset Capabilities for Institutional Clients</i> , businesswire (Sept. 18, 2023, 9:00 AM), https://www.businesswire.com/news/home/20230918024720/en/Citi-Develops-New-Digital-Asset-Capabilities-for-Institutional-Clients | 7 |
| <i>Crypto Assets</i> , SEC, https://www.sec.gov/securities-topics/crypto-assets (last visited Aug. 7, 2024) | 9 |
| <i>Cybersecurity Advisory: Russian State Sponsored and Criminal Cyber Threats to Critical Infrastructure</i> , CISA (May 9, 2022), https://perma.cc/C5TN-QL62 | 19 |
| Dave Michaels, <i>Exchanges Cite Hacking Risk of SEC’s Planned Market Data Repository</i> , The Wall Street Journal (Sept. 15, 2017, 4:53 PM), https://www.wsj.com/articles/exchanges-cite-hacking-risk-of-secs-planned-market-data-repository-1505508831 | 17 |
| Dave Michaels, <i>SEC Discloses Edgar Corporate Filing System Was Hacked in 2016</i> , The Wall Street Journal (Sept. 20, 2017, 11:10 PM), https://www.wsj.com/articles/sec-discloses-edgar-corporate-filing-system-was-hacked-in-2016-1505956552 | 16, 17 |
| David W. Perkins, <i>Cryptocurrency: The Economics of Money and Selected Policy Issues</i> , Congressional Research Service, at 7 (Apr. 9, 2020), https://perma.cc/G8UA-SXD6 | 5 |
| <i>Explore Solana Blockchain</i> , SOLSCAN, https://solscan.io/ | 6 |
| Ezra Reguerra, <i>Swiss Bank UBS Launches Tokenized Money Market Fund on Ethereum</i> , Cointelegraph (Oct. 2, 2023), https://cointelegraph.com/news/ethereum-ubs-tokenize-money-market-fund-launch | 7 |
| <i>Franklin Templeton Announces Availability of Peer-to-Peer Transfers for Franklin OnChain U.S. Government Money Fund</i> , Franklin Templeton (Apr. 25, 2024), https://www.franklintempleton.com/press-releases/news-room/2024/franklin-templeton-announces-availability-of-peer-to-peer-transfers-for-franklin-onchain-u.s.-government-money-fund | 7 |
| Gary Gensler, <i>Kennedy and Crypto</i> , SEC (Sept. 8, 2022), https://www.sec.gov/newsroom/speeches-statements/gensler-sec-speaks-090822 | 9 |
| <i>Guide to Broker-Dealer Registration</i> , SEC (Apr. 2008), https://www.sec.gov/about/reports-publications/divisionsmarketregbdguidehtm | 13 |
| Hester M. Peirce, <i>Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19</i> , SEC (May 15, 2020), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-response-release-34-88890-051520 | 16 |
| <i>In the Matter of ShapeShift AG</i> , SEC Administrative Proceeding No. 3-21891, Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order (Mar. 5, 2024) https://www.sec.gov/files/litigation/admin/2024/34-99676.pdf | 12 |

James Rundle, *SEC’s \$10 Million Fine of NYSE Owner Shows Focus on Cyber Disclosures*, The Wall Street Journal (May 22, 2024, 4:39 PM), <https://www.wsj.com/articles/secs-10-million-fine-of-nyse-owner-shows-focus-on-cyber-disclosures-45f2d456> 17

Jay Clayton, *Statement on Cybersecurity*, SEC (Sept. 20, 2017), <https://www.sec.gov/newsroom/speeches-statements/statement-clayton-2017-09-20>..... 16

Jose Pagliery, *Russian Hackers Placed ‘Digital Bomb’ in Nasdaq – Report*, CNN Business (July 17, 2014. 3:49 PM), <https://money.cnn.com/2014/07/17/technology/security/nasdaq-hack/index.html>..... 17

Katherine Ross, *Gensler’s SEC Brought 46 Crypto-Related Enforcements in 2023*, Blockworks (Jan. 24, 2024, 2:13 PM), <https://blockworks.co/news/sec-2023-crypto-enforcement-actions..> 9

Kenneth E. Bentsen, Jr., *A Safer CAT for Investors*, SIFMA (Apr. 25, 2024), <https://www.sifma.org/resources/news/a-safer-cat-for-investors/> 19

Krisztian Sandor, *BlackRock’s BUIDL Becomes Largest Tokenized Treasury Fund Hitting \$375M, Toppling Franklin Templeton’s*, CoinDesk (Apr. 30, 2024, 10:45 AM), <https://www.coindesk.com/markets/2024/04/30/blackrocks-buidl-becomes-largest-tokenized-treasury-fund-hitting-375m-toppling-franklin-templetons/> 7

Krisztian Sandor, *DTCC, Chainlink Complete Pilot to Accelerate Fund Tokenization with JPMorgan, Templeton, BNY Mellon Participating; Link Gains 7%*, CoinDesk (May 16, 2024, 4:30 PM), <https://www.coindesk.com/business/2024/05/16/dtcc-chainlink-complete-pilot-to-accelerate-fund-tokenization-with-jpmorgan-templeton-bny-mellon-participating/> 7

Lucien Bruggeman, *Navy Says Personal Data of Over 134,000 Sailors Was Hacked*, ABC News (Nov. 24, 2016, 12:07 PM), <https://abcnews.go.com/US/navy-personal-data-134000-sailors-hacked/story?id=43760770> 18

Lyllah Ledesma, *A \$1.4T Financial Giant Expands Its Money Market Fund on Polygon*, CoinDesk (May 9, 2023, 12:13 AM), <https://www.coindesk.com/business/2023/04/26/a-14t-financial-giant-expands-its-money-market-fund-on-polygon/> 7

Matthew Fox, *SEC Says Twitter Account Was Compromised, It’s Not Approved a Bitcoin ETF*, Business Insider (Jan. 9, 2024, 5:03 PM), <https://markets.businessinsider.com/news/currencies/bitcoin-etfs-sec-approval-twitter-hack-gary-gensler-crypto-2024-1> 17

Nathaniel Popper, *Bitcoin Thieves Threaten Real Violence for Virtual Currencies*, New York Times (Feb. 18, 2018), <https://perma.cc/3KCU-3ELC>..... 19

Niamh Rowe, *Hamilton Lane Becomes First Asset Manager to Launch a Fund on Solana Blockchain*, yahoo!finance (July 23, 2024), <https://ca.finance.yahoo.com/news/hamilton-lane-becomes-first-asset-100000656.html>..... 8

Oliver Knight, *Wall Street Giant DTCC Launches Private Blockchain in Big Crypto-Milestone for TradFi*, CoinDesk (Aug. 22, 2022, 12:16 PM),

<https://www.coindesk.com/business/2022/08/22/wall-streets-dtcc-launches-private-blockchain-platform-to-settle-trades/>..... 7

Patricia Zengerle & Megan Cassella, *Millions More Americans Hit by Government Personnel Data Hack*, Reuters (July 9, 2015, 7:20 PM), <https://www.reuters.com/article/technology/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M4/>..... 18

Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security, SEC Release No. 34-89632, File No. S7-10-20 (Aug. 21, 2020), <https://www.sec.gov/files/rules/proposed/2020/34-89632.pdf>..... 19

Register a New Broker-Dealer Firm, FINRA, <https://www.finra.org/registration-exams-ce/broker-dealers/new-firms#:~:text=To%20conduct%20securities%20transactions%20and,FINRA%2Dregistered%20broker%2Ddealer> (last visited Aug. 7, 2024) 8

Resources, Blockchain Association, <https://theblockchainassociation.org/resources-2/>..... 5

Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 6 (2008), perma.cc/5MZP-PAEX..... 6

Sean Lyngaas, *Exclusive: US Government Agencies Hit in Global Cyberattack* (June 15, 2023, 10:03 PM), <https://www.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html>..... 18

SEC Adopts Amendments to Exemption from National Securities Association Membership, SEC (Aug. 23, 2023), <https://www.sec.gov/newsroom/press-releases/2023-154> 8

Semiannual Report to Congress April 1, 2013 to September 30, 2013, SEC Office of Inspector General, at 16-17, https://www.sec.gov/about/offices/oig/reports/reppubs/2013/oig_fall2013.pdf 17

Smart NAV Pilot Report: Bringing Trusted Data to the Blockchain Ecosystem, DTCC (May 2024), https://www.dtcc.com/-/media/Files/Downloads/DTCC-Connection/Smart_NAV-Report.pdf..... 7

Stuart Madnick, *What’s Behind the Increase in Data Breaches?*, The Wall Street Journal (Mar. 15, 2024, 9:00 AM), <https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c> 16

Supplemental Information and Reopening of Comment Period for Amendments Regarding the Definition of “Exchange,” 88 Fed. Reg. 29448 (May 5, 2023), <https://www.sec.gov/files/rules/proposed/2023/34-97309.pdf>..... 11

The Ethereum Blockchain Explorer, Etherscan, <https://etherscan.io>..... 6

What Are Block Explorers and How Do They Work?, Crypto.com (June 16, 2023), <https://crypto.com/university/what-are-block-explorers>..... 6

INTERESTS OF *AMICI CURIAE*¹

Blockchain Association (the “Association”) is the leading membership organization dedicated to promoting a pro-innovation policy environment for the digital asset economy. The Association endeavors to achieve regulatory clarity and to educate policymakers, regulators, courts, and the public about how blockchain technology can create a more secure, competitive, and consumer-friendly digital marketplace. The Association represents nearly 100 member companies reflecting the wide range of the blockchain industry, including software developers, infrastructure providers, exchanges, custodians, investors, and others supporting the public blockchain ecosystem.

DeFi Education Fund (“DEF”) is a nonpartisan nonprofit organization that advocates for and educates about sound policy for decentralized finance (“DeFi”). DEF’s mission includes advocating for the interests of DeFi users, participants, and software developers working to create new DeFi products using blockchain technology that are decentralized and open to all users. Among other things, DEF educates the public about DeFi through op-eds, podcasts, and print media, meets with members of Congress to discuss DeFi issues, and submits public comments on proposed rulemakings that impact DeFi.

The Association and DEF are keenly interested in major litigation and legal issues affecting the digital asset industry. As this *amicus* brief describes in detail, the Consolidated Audit Trail (“CAT”) collects an enormous amount of information, by design. But the CAT, first proposed before blockchain technologies were in widespread use, interacts with blockchain data in a way that exposes a vast amount of personal financial data to the federal government, far beyond the

¹ This *amicus* brief reflects the views of the Association and of DEF, but does not reflect the views of any individual member of the Association. No party other than the Association and DEF contributed to this brief.

securities transactions that the CAT was intended to capture. The Association and DEF have been vocal in this criticism of the CAT database,² and appreciate the Court’s attention to this vitally important privacy issue.

INTRODUCTION AND SUMMARY OF ARGUMENT

People engage in individual, personal financial transactions as part of daily life. They do not expect the details of those transactions, including their identifying information, to be supplied to a massive government database accessible to the Securities and Exchange Commission (the “SEC”), national securities exchanges, the Financial Industry Regulatory Authority (“FINRA”), and their thousands of members and employees. While the CAT poses significant threats to individual privacy on its face, the inclusion of blockchain-based user information such as wallet addresses to the CAT database greatly magnifies those threats.

While neither Rule 613 (first establishing the CAT) nor the national market system plan “to create, implement, and maintain the CAT” (the “NMS Plan”) explicitly mention digital assets, the SEC has already taken the position, through litigation and rulemaking, that certain digital asset market participants are “Exchanges,” “Brokers,” and/or “Dealers.” As explained in Plaintiffs’ Complaint (ECF No. 1) and Motion for a Preliminary Injunction and Stay (ECF No. 25-3, the “PI Motion”), “Exchanges,” “Brokers,” “Dealers,” and others are required to provide detailed information regarding securities transactions and personal information about counterparties to the CAT database. In addition to these digital asset market participants eventually reporting transaction information to the CAT, traditional financial firms with reporting obligations to the

² See Amanda Tuminelli & Marisa T. Coppel, *Crypto’s Latest Privacy Battle*, CoinDesk (June 5, 2024, 3:39 PM), <https://www.coindesk.com/opinion/2024/06/05/cryptos-latest-privacy-battle/>.

CAT have also begun to offer blockchain-based products (and will certainly offer more in the future), bringing more blockchain-based data to the CAT.

The nature of a public blockchain, such as the Ethereum, Bitcoin, or Solana blockchains, is that all transaction information on that chain is linked and publicly accessible. With just a few details from any one transaction, any person can see all other transactions associated with a particular wallet address, along with a wealth of other information. Unlocking one transaction unlocks them all.

However, routine blockchain transactions enjoy a degree of privacy because a person's wallet address is not normally linked to their name or other personally identifying information. A casual observer can see that a transaction occurred, and that a certain amount of cryptocurrency moved from one wallet address to another, but will not know who those wallets belong to. As a result, people transacting on a public blockchain enjoy a degree of privacy in their everyday financial transactions.

The CAT, however, connects personally identifying information with wallet addresses that reveal blockchain-based user transactions. Thus, anyone with access to the CAT would be able to see not just a person's securities transactions, which the CAT is designed to trace, but all of that person's blockchain transactions in the past, present, and future. Any blockchain-based transaction that is recorded in the CAT can be used to track any and all other transactions with that person's wallet address on the blockchain: routine purchases, payments for services, donations to religious or other charities, salary payments, virtual currency holdings, and far more. The CAT would thus provide unparalleled and unprecedented insight – to the government and to a slew of private parties – into everyday Americans' everyday blockchain transactions. All that information would be available to the federal government, allowing the government to sift through the entirety of someone's financial life without a warrant or probable cause.

Making matters worse, the CAT database would be a honeypot for hackers and other bad actors – a risk exacerbated by the linkage of wallet addresses or blockchain transaction information to individual user information in the CAT. If hackers accessed the CAT database, those bad actors would have access to individual user information that could be weaponized against Americans, such as the overall amount of a person’s digital asset holdings and their identifying information. Those bad actors could use such information to extort or retaliate against digital asset users. Although personal identifying information submitted to the CAT database is purportedly housed separately, with more limited accessibility, anyone with access to both databases will be able to match blockchain transactions to a specific person. Every single employee at the SEC, FINRA, or any other organization with access to those databases will be a target for “phishing” attacks, bribery, extortion, and other hacking attempts because of the wealth of information that would be available from linking the personal identifying information in the CAT to blockchain-based data. The risk is not hypothetical; the SEC and other government agencies and self-regulatory organizations have been hacked multiple times. In 2020, the SEC proposed a rule that would have strengthened the CAT’s security but failed to adopt it.

Every American has a right to basic privacy; to avoid their everyday financial information unconstitutionally and unlawfully being submitted to an immense government database that can be searched, mined, hacked, or misused. The increasing digitization of our economy, and the shift toward blockchain technologies to securely record digital transactions, demand that regulators take into account the risks of their actions. The SEC has not done so here. The Association and DEF support the PI Motion and support Plaintiffs’ opposition to Defendants’ motions to dismiss (ECF Nos. 38-39, the “Motions to Dismiss”), and respectfully request that the Court consider the implications of the CAT database on the digital asset industry in fashioning a ruling.

STATEMENT OF FACTS

A. Blockchains, Cryptocurrency, and Wallets³

Digital assets are a digital store of value “powered by a decentralized digital ledger called a ‘blockchain.’ Blockchains consist of ‘blocks’ of data that track the ownership and transfer of crypto assets on a given network, dating back to the first-ever transaction on that network.” *Risley v. Universal Navigation Inc.*, 690 F. Supp. 3d 195, 202 (S.D.N.Y. 2023) (internal citation omitted). Unlike traditional financial transactions, public blockchain transactions are recorded on an immutable ledger that is visible to anyone.⁴

To use digital assets, a user generates a unique “wallet address,” which is a string of letters and numbers. The user can then send or receive cryptocurrency to and from his or her “wallet.” A “wallet” uses two alphanumeric strings – a private key and a public key – to interact with a blockchain and “permit the user to effectuate transactions on the associated blockchain.” *SEC v. Coinbase, Inc.*, 2024 U.S. Dist. LEXIS 56994, at *11 (S.D.N.Y. Mar. 27, 2024). “Owners typically store these keys on a piece of hardware or software known as a ‘crypto wallet’....The public key is colloquially known as the user’s blockchain ‘address’ and can be freely shared with others. The private key is analogous to a password and confers the ability to transfer a crypto-asset.” *Id.*

Those who wish to trade digital assets may do so on a centralized exchange that “allows customers to buy, sell, and spend crypto...for consideration, including U.S. dollars, other fiat currencies, or other crypto-assets.” *Id.* at *14 (quotation omitted). Or they may do so via peer-to-peer transactions using DeFi protocols, which enable “the sending, receiving, and swapping of

³ This short summary only provides the most pertinent background information for this *amicus* brief. For more comprehensive background information regarding digital assets, see *Resources*, Blockchain Association, <https://theblockchainassociation.org/resources-2/>.

⁴ See David W. Perkins, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, Congressional Research Service, at 7 (Apr. 9, 2020), <https://perma.cc/G8UA-SXD6>.

crypto-assets, among other decentralized application functions, without using intermediaries...”
Id. at *16.

When a user sends or receives digital assets on a public blockchain, the transaction information is posted to a public ledger, visible to anyone. The public ledger displays information including the sender’s address, the recipient’s address, and the digital assets that they exchanged. Because the ledger is public, tools like “block explorers,” which contain blockchain transaction records, can be used to search by wallet address and to see every other transaction involving that wallet on that particular blockchain.⁵ But because the addresses are pseudonymous, onlookers can only identify transaction participants if they can match a public key to an identifiable person.⁶ Once that happens, the public-ledger system can be used as a tool for surveillance.⁷ Consequently, user pseudonymity is a key feature of blockchain transactions.

B. Traditional Finance Firms Are Offering Services Related to Digital Assets

Given the increasing popularity of digital assets and the technical advantages of blockchain transactions, it is no surprise that traditional finance companies are increasingly offering blockchain-based services. For example, the Depository Trust & Clearing Corporation (“DTCC”), the preeminent firm for processing U.S. stock market trades, has tested the use of a private blockchain to settle and clear certain daily stock trades,⁸ and completed a pilot project with

⁵ See *What Are Block Explorers and How Do They Work?*, Crypto.com (June 16, 2023), <https://crypto.com/university/what-are-block-explorers>. For examples of block explorers on major blockchains, see, e.g., *The Ethereum Blockchain Explorer*, Etherscan, <https://etherscan.io/>; *Explore Solana Blockchain*, SOLSCAN, <https://solscan.io/>; *BTC Explorer by Redot*, Btcscan, <https://btcscan.org/>.

⁶ See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 6 (2008), perma.cc/5MZP-PAEX.

⁷ See *id.* (“[I]f the owner of a key is revealed, linking [on the public ledger] could reveal other transactions that belonged to the same owner.”). See also *Matter of Search of Multiple Email Accts.*, 585 F. Supp. 3d 1, 8 (D.D.C. 2022) (detailing such surveillance).

⁸ See Oliver Knight, *Wall Street Giant DTCC Launches Private Blockchain in Big Crypto-Milestone for TradFi*, CoinDesk (Aug. 22, 2022, 12:16 PM),

blockchain oracle provider Chainlink to provide data “that can serve as a key enabler to the exploration of new initiatives” regarding the tokenization of funds.⁹ While these programs were conducted on a private blockchain – where transactions are not available to the public at large – they demonstrate the tectonic shift to use of blockchains for mainstream financial transactions.

As further examples, Franklin Templeton offers a tokenized money market fund that uses a public blockchain to process transactions and record share ownership,¹⁰ and recently announced that shares of the fund can be transferred on a blockchain.¹¹ BlackRock and UBS also offer tokenized money market funds.¹² Citi offers “blockchain and smart contract technologies to deliver digital asset solutions for institutional clients,” for “cash management and trade finance.”¹³

<https://www.coindesk.com/business/2022/08/22/wall-streets-dtcc-launches-private-blockchain-platform-to-settle-trades/>.

⁹ See *Smart NAV Pilot Report: Bringing Trusted Data to the Blockchain Ecosystem*, DTCC (May 2024), https://www.dtcc.com/-/media/Files/Downloads/DTCC-Connection/Smart_NAV-Report.pdf. See also Krisztian Sandor, *DTCC, Chainlink Complete Pilot to Accelerate Fund Tokenization with JPMorgan, Templeton, BNY Mellon Participating; Link Gains 7%*, CoinDesk (May 16, 2024, 4:30 PM), <https://www.coindesk.com/business/2024/05/16/dtcc-chainlink-complete-pilot-to-accelerate-fund-tokenization-with-jpmorgan-templeton-bny-mellon-participating/>.

¹⁰ See Lyllah Ledesma, *A \$1.4T Financial Giant Expands Its Money Market Fund on Polygon*, CoinDesk (May 9, 2023, 12:13 AM), <https://www.coindesk.com/business/2023/04/26/a-14t-financial-giant-expands-its-money-market-fund-on-polygon/>.

¹¹ See *Franklin Templeton Announces Availability of Peer-to-Peer Transfers for Franklin OnChain U.S. Government Money Fund*, Franklin Templeton (Apr. 25, 2024), <https://www.franklintempleton.com/press-releases/news-room/2024/franklin-templeton-announces-availability-of-peer-to-peer-transfers-for-franklin-onchain-u.s.-government-money-fund>.

¹² See Krisztian Sandor, *BlackRock’s BUIDL Becomes Largest Tokenized Treasury Fund Hitting \$375M, Toppling Franklin Templeton’s*, CoinDesk (Apr. 30, 2024, 10:45 AM), <https://www.coindesk.com/markets/2024/04/30/blackrocks-buidl-becomes-largest-tokenized-treasury-fund-hitting-375m-toppling-franklin-templetons/>; Ezra Reguerra, *Swiss Bank UBS Launches Tokenized Money Market Fund on Ethereum*, Cointelegraph (Oct. 2, 2023), <https://cointelegraph.com/news/ethereum-ubs-tokenize-money-market-fund-launch>.

¹³ *Citi Develops New Digital Asset Capabilities for Institutional Clients*, businesswire (Sept. 18, 2023, 9:00 AM), <https://www.businesswire.com/news/home/20230918024720/en/Citi-Develops-New-Digital-Asset-Capabilities-for-Institutional-Clients>.

A spate of traditional finance firms offer Bitcoin and Ethereum ETPs.¹⁴ And Hamilton Lane recently announced the launch of a private credit fund on the Solana blockchain.¹⁵

C. The CAT and the NMS Plan

Every national securities exchange and broker-dealer (among other entities) is required to provide information to the CAT database. Rule 613 provides that FINRA and other national securities exchanges shall propose a “joint National Market System Plan” for the “creation, implementation, and maintenance of a consolidated audit trail and central repository” of data. 17 C.F.R. § 242.613(a)(1). It further states that each national securities exchange, national securities association (i.e., FINRA),¹⁶ and their members¹⁷ shall provide a significant amount of data to the CAT database regarding each securities transaction, including customer identification information, the date and time of the order, and the “material terms of the order.” *Id.* § 242.613(c)(2), (c)(7). The term “material terms of the order” “shall include, but not be limited to, the NMS security symbol; security type; price (if applicable); size (displayed and non-displayed); side (buy/sell); order type, if a sell order, whether the order is long, short, short exempt, open/close indicator; time in force (if applicable); if the order is for a listed option; option type (put/call), option symbol or root symbol, underlying symbol, strike price, expiration date, and open/close; and any special

¹⁴ See *Bitcoin ETFs List*, VettaFi (Aug. 19, 2024), <https://etfdb.com/themes/bitcoin-etfs/>; *Ethereum ETFs List*, <https://etfdb.com/themes/ethereum-etfs/>.

¹⁵ See Niamh Rowe, *Hamilton Lane Becomes First Asset Manager to Launch a Fund on Solana Blockchain*, yahoo!finance (July 23, 2024), <https://ca.finance.yahoo.com/news/hamilton-lane-becomes-first-asset-100000656.html>.

¹⁶ FINRA is the only registered national securities association. See, e.g., SEC Adopts Amendments to Exemption from National Securities Association Membership, SEC (Aug. 23, 2023), <https://www.sec.gov/newsroom/press-releases/2023-154>.

¹⁷ Broker-Dealers that “conduct securities transactions and business with the investing public in the United States” must register as a member with FINRA. See Register a New Broker-Dealer Firm, FINRA, <https://www.finra.org/registration-exams-ce/broker-dealers/new-firms#:~:text=To%20conduct%20securities%20transactions%20and,FINRA%2Dregistered%20broker%2Ddealer> (last visited Aug. 7, 2024).

handling instructions.” *Id.* § 242.613(j)(7). Compliance by exchanges and broker-dealers is mandatory. *Id.* § 242.613(h)(1), (g)(2).

The SEC approved the NMS Plan incorporating Rule 613 in 2016. 81 Fed. Reg. 84696 (2016). As Plaintiffs describe, broker-dealers began reporting data to the CAT database in June 2020, but after some delays, the CAT database became “fully operational” on May 31, 2024, when FINRA began requiring compliance with all reporting procedures.¹⁸

D. The SEC Believes that Many Digital Asset Market Participants Are “Exchanges,” “Brokers,” and/or “Dealers,” Meaning That Those Entities Will Have to Report Blockchain Information to the CAT

The SEC has claimed broad regulatory authority over digital assets. SEC Chair Gary Gensler stated in 2022 that the “vast majority” of the “nearly 10,000 tokens in the crypto market” are securities and that “[o]ffers and sales of these thousands of crypto security tokens are covered under the securities laws.”¹⁹ The SEC brought forty-six digital asset related enforcement actions in 2023, an increase of 53% over 2022.²⁰ The SEC has filed actions against major digital asset businesses alleging they are securities “Exchanges”; against software companies whose software purportedly acts as securities “Brokers”; and has promulgated a new rule that may make large digital traders of blockchain-based securities “Dealers.” Under this rubric, the SEC casts most blockchain transactions as securities transactions and thus requires information on those transactions to be submitted to the CAT.

¹⁸ Compl. ¶¶ 84-87; PI Motion, at 10-11.

¹⁹ Gary Gensler, *Kennedy and Crypto*, SEC (Sept. 8, 2022), <https://www.sec.gov/newsroom/speeches-statements/gensler-sec-speaks-090822>.

²⁰ See Katherine Ross, *Gensler’s SEC Brought 46 Crypto-Related Enforcements in 2023*, Blockworks (Jan. 24, 2024, 2:13 PM), <https://blockworks.co/news/sec-2023-crypto-enforcement-actions>. See also *Crypto Assets*, SEC, <https://www.sec.gov/securities-topics/crypto-assets> (last visited Aug. 7, 2024) (listing digital asset enforcement actions brought by the SEC).

1. The SEC Has Asserted in Litigation that Digital Asset Trading Platforms Are “Exchanges,” and Is Attempting to Expand the Statutory Definition of “Exchange” Through Rulemaking

The SEC has sued Coinbase, Kraken, and Binance,²¹ among other digital asset trading platforms, alleging that those companies are operating as unregistered securities “Exchanges.” If the SEC prevails in these (ongoing) cases, these “Exchanges” would have reporting obligations under Rule 613.

Separately, the SEC proposed to amend Rule 3b-16 (under the Securities Act of 1934) to expand the statutory definition of “Exchange” in ways that could lead to even more digital asset market participants being swept into the statutory definition. *See* 87 Fed. Reg. 15646.²² Many industry participants, including the Association and DEF, submitted comment letters in response to the proposal.²³ However, as revised, the proposed rule confirmed that “activities performed today using so-called ‘DeFi’ trading systems could meet the criteria of existing Rule 3b-16 and

²¹ *See* Compl., *S.E.C. v. Coinbase, Inc. et al.*, No. 23 Civ. 4738, ECF No. 1 (S.D.N.Y. June 6, 2023); Compl., *S.E.C. v. Payward, Inc., et al.*, No. 3:23-cv-06003, ECF No. 1 (N.D. Cal. Nov. 20, 2023); Compl., *S.E.C. v. Binance Holdings Limited, et al.*, No. 1:23-cv-01599, ECF No. 1 (D.D.C. June 5, 2023).

²² Available at <https://www.govinfo.gov/content/pkg/FR-2022-03-18/pdf/2022-01975.pdf>.

²³ *See* Kristin Smith & Jake Chervinsky, Blockchain Association, Comment Letter on Amendments to Exchange Act Rule 3b-16, at 3-4 (Apr. 18, 2022), <https://www.sec.gov/comments/s7-02-22/s70222-20124039-280165.pdf>; Miller Whitehouse-Levine, DeFi Education Fund, Comment Letter on Amendments to Exchange Act Rule 3b-16, at 3 (Apr. 18, 2022), <https://www.sec.gov/comments/s7-02-22/s70222-20123960-280119.pdf>; Jake Chervinsky, Blockchain Association & Miller Whitehouse-Levine, DeFi Education Fund, Comment Letter on Amendments to Exchange Act Rule 3b-16, at 5 (June 13, 2022), <https://www.sec.gov/comments/s7-02-22/s70222-20131087-301122.pdf>; Jake Chervinsky & Marisa T. Coppel, Blockchain Association, Comment Letter on Reopening of the Comment Period: Proposed Amendments to Exchange Act Rule 3b-16 (June 13, 2023), <https://www.sec.gov/comments/s7-02-22/s70222-204059-410802.pdf>; Miller Whitehouse-Levine & Amanda Tuminelli, Comment Letter on Reopening of the Comment Period; Proposed Amendments to Exchange Act Rule 3b-16 (June 12, 2023), <https://www.sec.gov/comments/s7-02-22/s70222-202979-407862.pdf>.

thus constitute exchange activity.”²⁴ If the proposed rule were adopted, DeFi protocols and digital asset platforms could be considered “Exchanges,” required to provide information to the CAT database.

2. The SEC Considers Certain Digital Asset Industry Participants to Be “Brokers”

The SEC has asserted in litigation that certain digital asset companies are acting as unregistered “Brokers” under the Exchange Act because they deployed software that enables users to conduct their own digital asset transactions.²⁵ The SEC sued Coinbase, alleging (in relevant part) that Coinbase acted as an unregistered “Broker” through its non-custodial Wallet product.²⁶ That court, in the Southern District of New York, dismissed the non-custodial wallet allegations. *SEC v. Coinbase, Inc.*, 2024 U.S. Dist. LEXIS 56994, at *98-105 (S.D.N.Y. Mar. 27, 2024). However, apparently undaunted by that loss, the SEC crossed the East River to make substantially similar allegations in a lawsuit in the Eastern District of New York, against Consensus Software Inc. (“Consensus”), in which it claimed that Consensus acts as an unregistered “Broker” via its non-custodial “Metamask” wallet application.²⁷ Thus, the SEC continues to insist (despite a previous judicial holding to the contrary) that developers of non-custodial software applications are somehow “Brokers” under securities laws. And of course, “Brokers” are required to register

²⁴ Supplemental Information and Reopening of Comment Period for Amendments Regarding the Definition of “Exchange,” 88 Fed. Reg. 29448 (May 5, 2023), <https://www.sec.gov/files/rules/proposed/2023/34-97309.pdf> (the “Reopening”).

²⁵ See Compl., *S.E.C. v. Coinbase, Inc. et al.*, No. 23 Civ. 4738, ECF No. 1 (S.D.N.Y. June 6, 2023); Compl., *S.E.C. v. Payward, Inc., et al.*, No. 3:23-cv-06003, ECF No. 1 (N.D. Cal. Nov. 20, 2023); Compl., *S.E.C. v. Binance Holdings Ltd., et al.*, No. 1:23-cv-01599, ECF No. 1 (D.D.C. June 5, 2023).

²⁶ See Compl., *S.E.C. v. Coinbase, Inc.*, et al, No. 23 Civ. 4738, ECF No. 1, ¶ 4 (S.D.N.Y. June 6, 2023).

²⁷ See Compl., *S.E.C. v. Consensus Software Inc.*, No. 24 Civ. 4578, ECF No. 1 (E.D.N.Y. June 28, 2024).

with FINRA or another self-regulatory organization (“SRO”), and Rule 613 requires them to report securities transaction information to the CAT database.

3. The SEC Considers Certain Digital Asset Industry Participants to Be “Dealers,” and Has Expanded the Statutory Definition through Rulemaking

The SEC initiated several enforcement actions in 2023, claiming that certain digital asset market participants are acting as unregistered “Dealers,” as that term was defined at the time.²⁸ Then, on February 6, 2024, the SEC issued a final rule²⁹ that further expands the regulatory definition of “Dealer,” sweeping in even more digital asset industry participants. The so-called “Dealer Rule” provides that if a person buys and sells securities even for their own account “as part of a regular business,” and if that person’s actions had the effect of providing liquidity to the market, no matter if that party interacted with customers, that person is a “Dealer.” The Dealer Rule upended many decades of understanding of the term “Dealer,” expanding the definition well beyond its meaning in the Exchange Act. And the Dealer Rule explicitly applies to “crypto assets that are securities....”³⁰

Market participants, including the Association and DEF, raised significant concerns in comment letters about how the Dealer Rule would affect the industry.³¹ In adopting the final

²⁸ See, e.g., *In the Matter of ShapeShift AG*, SEC Administrative Proceeding No. 3-21891, Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order (Mar. 5, 2024) <https://www.sec.gov/files/litigation/admin/2024/34-99676.pdf>; Compl., *S.E.C. v. Payward, Inc., et al.*, No. 3:23-cv-06003, ECF No. 1 (N.D. Cal. Nov. 20, 2023); Compl., *S.E.C. v. Binance Holdings Ltd., et al.*, No. 1:23-cv-01599, ECF No. 1 (D.D.C. June 5, 2023); Compl., *S.E.C. v. Beaxy Digital, Ltd., et al.*, No. 23-cv-1962, ECF No. 1 (N.D. Ill. Mar. 29, 2023).

²⁹ “Further Definition of ‘As Part of a Regular Business’ in the Definition of Dealer and Government Securities Dealer in Connection with Certain Liquidity Providers,” 89 Fed. Reg. 14938 (Feb. 6, 2024) (the “Dealer Rule”).

³⁰ *Id.* at 14960.

³¹ See Kristin Smith & Jake Chervinsky, Blockchain Association, Comment Letter on Proposed Further Definition of the Dealer Rule, at 1 (May 27, 2022), <https://www.sec.gov/comments/s7-12-22/s71222-20129925-296179.pdf>; Miller Whitehouse-

Dealer Rule, the SEC failed to address these concerns. The Association and another industry group have initiated an action seeking to vacate and enjoin the Dealer Rule, and that action remains pending.³² But unless the Dealer Rule is vacated, the SEC will consider a significant number of digital asset market participants – potentially including users of DeFi protocols – to be “Dealers.” And, of course, “Dealers” must register with FINRA,³³ and must provide data to the CAT database.

ARGUMENT

I. THE CAT WOULD SWEEP IN BLOCKCHAIN-BASED INFORMATION, RISKING A MASSIVE INVASION OF PERSONAL PRIVACY FOR MILLIONS

Blockchain technology, even though still relatively new, already provides a significant step forward in the security and efficiency of transactions. It also creates a permanent, public, immutable record of those transactions. That public record would be a financial privacy nightmare – except for the fact that blockchain transactions are pseudonymous and recorded without personal identifying information, a feature that affords users a necessary degree of privacy.

The CAT removes that guardrail, turning blockchains into a massive and fully deanonymized repository for the government to search at will, without any need to show cause to obtain a warrant. Due to the nature of blockchain technology, accessing even one superficially limited identity record will unlock an unprecedented trove of unrelated financial transactions conducted by that user – past, present, and future – all open for inspection by the federal government, and a host of private parties. To say that such a database would be vulnerable to abuse is a severe understatement.

Levine, DeFi Education Fund, Comment Letter on Proposed Further Definition of the Dealer Rule, at 7 (May 27, 2022), <https://www.sec.gov/comments/s7-12-22/s71222-20131214-296907.pdf>.

³² Compl., *Crypto Freedom All. of Tex, et al. v. SEC, et al.*, Case No. 4:24-cv-00361-O, ECF No. 1 (N.D. Tex. Apr. 23, 2023).

³³ See *Guide to Broker-Dealer Registration*, SEC (Apr. 2008), <https://www.sec.gov/about/reports-publications/divisionsmarketregbdguidehtm>.

Neither Rule 613 nor the NMS Plan mentions digital assets, blockchain, cryptocurrency, or wallets – unsurprising given that Rule 613 was adopted in 2012, during the infancy of digital assets. But the result of the SEC deeming digital asset market participants to be “Exchanges,” “Brokers,” or “Dealers,” coupled with the increasing use of blockchain technologies by traditional finance firms, is that blockchain-based user information inevitably would be submitted to the CAT database. A user’s public blockchain wallet address would be swept into the CAT as a “Material Term of the Order.” 81 Fed. Reg. at 84,706-77; 17 C.F.R. § 242.613(j)(7). And even without a wallet address, the other transaction terms required to be submitted – the “security” in question, the volume and price of the order, the date and time of the transaction – will allow anyone with access to the CAT database to ascertain a user’s wallet addresses.

If information connecting a user to a particular blockchain transaction is submitted to the CAT database, anyone with access to the CAT can utilize block explorers and other public sources to obtain additional information about the owner of the wallet address beyond just securities transactions, including the user’s identity, and a vast array of blockchain transactions that person has conducted, whether they include securities or not.

The deanonymization of digital asset users, by making their identities and their other blockchain transactions available, is akin to publishing that individual’s entire credit card transaction history online, but even more invasive. A person could conduct virtually any transaction involving a blockchain through a CAT-reporting “Exchange,” “Broker,” or “Dealer,” and that person’s name would be connected to their wallet address, making their full blockchain transaction history available to the federal government. Anything that person did on that blockchain – donations to political or religious organizations, books or magazines that were purchased, salary that was received – would all be available in a government database, searchable without a warrant. Everyday purchases would be laid bare for all to see, even if the person made

that purchase years prior. The amount of a person's total digital asset holdings would be visible, making that person more vulnerable to crime. If they used digital assets to pay for medical treatment, that person's medical history would be exposed. It would be like the government and other actors being able to rummage through a person's drawers, with their entire financial life on display, without being accused of any wrongdoing. "Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy. Moreover, the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process." *Cal. Bankers Ass'n v. Schultz*, 416 U.S. 21, 78-79 (1974) (Powell, J., concurring).

Plaintiffs convincingly demonstrate that the remarkable breadth of the CAT violates the Fourth Amendment's protection against unreasonable searches and seizures.³⁴ In particular, Plaintiffs explain how the CAT unreasonably intrudes on individuals' reasonable expectation of privacy of their financial information.³⁵ Without repeating Plaintiffs' compelling Fourth Amendment argument, we emphasize that Plaintiffs' concerns are, if anything, vastly understated because of the increasing adoption of blockchain technology. When confronted with "advancing technology," courts must recalibrate Fourth Amendment protections to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. U.S.*, 533 U.S. 27, 34 (2001). And "[w]hen confronting new concerns wrought by digital technology," courts must refuse "to uncritically extend existing precedents." *Carpenter v. U.S.*, 585 U.S. 296, 318 (2018). The situation created by the CAT is that the government will be able to use records of one single blockchain transaction to search all of that wallet's past and future

³⁴ See Compl. ¶¶ 143-68; PI Motion, at 27-33.

³⁵ See PI Motion, at 28-29.

blockchain transactions, no matter the nature of those transactions, and all without a warrant, or needing “probable cause.”

II. THE CAT DATABASE IS VULNERABLE TO DATA LOSS OR HACKING

It is bad enough that those with legal access to the CAT database can use information submitted to the CAT to see all of a user’s blockchain transactions. To make things far worse, there is a significant risk that user data submitted to the CAT database will be divulged to outside parties through accidents or nefarious exploits. Data breaches are on a meteoric rise, even though organizations are spending more money than ever on cybersecurity.³⁶

Even the SEC admits that the CAT database is vulnerable. In 2017, then-SEC Chair Jay Clayton acknowledged that “we expect we will face the risk of unauthorized access to the CAT’s central repository and other efforts to obtain sensitive CAT data. Through such access, intruders could potentially obtain, expose and profit from the trading activity and personally identifiable information of investors and other market participants.”³⁷ Commissioner Hester M. Peirce agrees: “[e]ven the most vigilant employer...cannot identify every possible bad actor, and one security lapse involving only one of the CAT’s thousands of users could compromise the entire database.”³⁸

These concerns are not merely hypothetical; the SEC itself has demonstrated that it is not a secure agency. The SEC’s corporate filing system, EDGAR, was hacked in 2016.³⁹ The EDGAR

³⁶ Stuart Madnick, *What’s Behind the Increase in Data Breaches?*, The Wall Street Journal (Mar. 15, 2024, 9:00 AM), <https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c> (“The number of reported data breaches in the U.S. rose to a record 3,205 in 2023, up 78% from 2022 and 72% from the previous high-water mark in 2021.”).

³⁷ Jay Clayton, *Statement on Cybersecurity*, SEC (Sept. 20, 2017), <https://www.sec.gov/newsroom/speeches-statements/statement-clayton-2017-09-20>.

³⁸ Hester M. Peirce, *Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19*, SEC (May 15, 2020), <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-response-release-34-88890-051520>

³⁹ See Dave Michaels, *SEC Discloses Edgar Corporate Filing System Was Hacked in 2016*, The Wall Street Journal (Sept. 20, 2017, 11:10 PM), <https://www.wsj.com/articles/sec-discloses-edgar-corporate-filing-system-was-hacked-in-2016-1505956552>.

hack did not come to light until September 2017,⁴⁰ shortly after executives from the New York Stock Exchange and Bats Global Markets Inc. publicly expressed concern that the CAT database itself would be a target for hackers.⁴¹ On a smaller scale, earlier this year, the SEC’s official Twitter account was hacked, posting a false statement that the SEC had approved a spot ETF for Bitcoin.⁴² And a former SEC employee once took files containing SEC employees’ personal information and uploaded them to his new employer’s computer system.⁴³

Every government agency and self-regulatory organization is vulnerable. The New York Stock Exchange and several sister companies have been hacked.⁴⁴ NASDAQ was the victim of a “digital bomb” placed by hackers.⁴⁵ An employee of the Consumer Finance Protection Bureau forwarded confidential information about hundreds of thousands of consumers to his personal email address.⁴⁶ Russian hackers have exploited multiple government agencies, including the

⁴⁰ *Id.*

⁴¹ See Dave Michaels, *Exchanges Cite Hacking Risk of SEC’s Planned Market Data Repository*, The Wall Street Journal (Sept. 15, 2017, 4:53 PM), <https://www.wsj.com/articles/exchanges-cite-hacking-risk-of-secs-planned-market-data-repository-1505508831>.

⁴² See Matthew Fox, *SEC Says Twitter Account Was Compromised, It’s Not Approved a Bitcoin ETF*, Business Insider (Jan. 9, 2024, 5:03 PM), <https://markets.businessinsider.com/news/currencies/bitcoin-etfs-sec-approval-twitter-hack-gary-gensler-crypto-2024-1>.

⁴³ See *Semiannual Report to Congress April 1, 2013 to September 30, 2013*, SEC Office of Inspector General, at 16-17, https://www.sec.gov/about/offices/oig/reports/reppubs/2013/oig_fall2013.pdf.

⁴⁴ See James Rundle, *SEC’s \$10 Million Fine of NYSE Owner Shows Focus on Cyber Disclosures*, The Wall Street Journal (May 22, 2024, 4:39 PM), <https://www.wsj.com/articles/secs-10-million-fine-of-nyse-owner-shows-focus-on-cyber-disclosures-45f2d456>.

⁴⁵ See Jose Pagliery, *Russian Hackers Placed ‘Digital Bomb’ in Nasdaq – Report*, CNN Business (July 17, 2014, 3:49 PM), <https://money.cnn.com/2014/07/17/technology/security/nasdaq-hack/index.html>.

⁴⁶ See Andrew Ackerman, *CFPB Says Staffer Sent 250,000 Consumers’ Data to Personal Account*, The Wall Street Journal (Apr. 19, 2023, 4:35 PM), <https://www.wsj.com/articles/in-major-incident-cfpb-says-staffer-sent-250-000-consumers-data-to-personal-account-fdc0a540>.

Department of Energy.⁴⁷ The U.S. Office of Personnel Management fell victim to a hack that stole the Social Security numbers and other sensitive information of 21.5 million people.⁴⁸ In 2016, hackers stole personal data – including social security numbers and names – belonging to over 100,000 U.S. Navy sailors.⁴⁹ These examples are far from exhaustive.

It is not only the SEC that would have access to the CAT's treasure trove of personal information. FINRA and numerous self-regulatory organizations – and their thousands of employees – will also have access to the data that is being submitted to the CAT database. As a result, each and every one of the thousands of employees of the SEC, FINRA, or other SROs would be subject to simple user error, phishing attacks, extortion, bribery, or worse, any of which could expose that treasure trove of information. As Commissioner Peirce has explained:

The sheer value and size of the database will make the CAT an inviting target, and the number of users and reporting entities will make it a more vulnerable one. Each of the thousands of users and each of CAT's many contributors will afford a would-be-hacker a potential point of entry. Each of these thousands of users will be able to track investors' market moves, and with a little effort, also will be able to reconstruct and misappropriate proprietary and confidential trading strategies.⁵⁰

The dangers cited by Commissioner Peirce are heightened dramatically when bad actors obtain information linking the real names of cryptocurrency users to their wallet addresses: those

⁴⁷ See Sean Lyngaas, *Exclusive: US Government Agencies Hit in Global Cyberattack* (June 15, 2023, 10:03 PM), <https://www.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html>.

⁴⁸ See Patricia Zengerle & Megan Cassella, *Millions More Americans Hit by Government Personnel Data Hack*, Reuters (July 9, 2015, 7:20 PM), <https://www.reuters.com/article/technology/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M4/>.

⁴⁹ See Lucien Bruggeman, *Navy Says Personal Data of Over 134,000 Sailors Was Hacked*, ABC News (Nov. 24, 2016, 12:07 PM), <https://abcnews.go.com/US/navy-personal-data-134000-sailors-hacked/story?id=43760770>.

⁵⁰ See Peirce, *supra*.

users can be at serious physical risk of extortionate demands.⁵¹ Dangerous groups, like Russian nationalists who follow donations of cryptocurrency to Ukraine, can use public cryptocurrency transactions as a basis for retaliation or other unsavory action.⁵²

In 2020, the SEC, recognizing the potential for the CAT database to be compromised, proposed a rule to enhance the security of the NMS Plan.⁵³ Yet, to date, that proposed rule has not been finalized, leading to criticism from prominent organizations.⁵⁴

In this litigation, the SEC waved away Plaintiffs' security concerns by arguing that personal information (names, addresses, and birth years) "is stored separately from all other [CAT] data, and its access is restricted to a limited set of authorized individuals on a need-to-know basis." ECF No. 39, at 13. But, as the SEC concedes, even this separate database is available to certain people. Moreover, as Commissioner Peirce explained, the measures to keep personal information submitted to the CAT separate from transaction information "do not adequately anonymize the data contained within the CAT, and identification of individual investors from the remaining PII [personally identifiable information] may still be possible."⁵⁵ Given the vulnerabilities, for the SEC to have this information in a separate place is no comfort. The SEC should not have it at all.

CONCLUSION

As Justice Brandeis famously wrote, "[e]xperience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are

⁵¹ See Nathaniel Popper, *Bitcoin Thieves Threaten Real Violence for Virtual Currencies*, New York Times (Feb. 18, 2018), <https://perma.cc/3KCU-3ELC>.

⁵² *Cybersecurity Advisory: Russian State Sponsored and Criminal Cyber Threats to Critical Infrastructure*, CISA (May 9, 2022), <https://perma.cc/C5TN-QL62>.

⁵³ See *Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security*, SEC Release No. 34-89632, File No. S7-10-20 (Aug. 21, 2020), <https://www.sec.gov/files/rules/proposed/2020/34-89632.pdf>.

⁵⁴ See Kenneth E. Bentsen, Jr., *A Safer CAT for Investors*, SIFMA (Apr. 25, 2024), <https://www.sifma.org/resources/news/a-safer-cat-for-investors/>.

⁵⁵ See Peirce, *supra*.

naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.” *Olmstead v. U.S.*, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting). Even if the CAT’s creation was well-intentioned, and it is potentially useful to catch some fraudulent activities, the CAT unacceptably undermines privacy and personal freedom. It is particularly dangerous to a society that is more and more “online,” and that increasingly relies on blockchain technology in everyday activities. The threat to personal privacy posed by the CAT – far beyond the mere monitoring of securities transactions as it was intended – is extreme.

The Association and DEF respectfully request that the Court considers the issues raised in this *amicus* brief when deciding the PI Motion and the Motions to Dismiss.

Dated: Dallas, Texas
August 22, 2024

DOWD BENNETT LLP

By: /s/ Ben A. Barnes

Ben A. Barnes
State Bar No. 24092085
2100 Ross Ave.
Suite 955
Dallas, TX 75201
(214) 347-7346
bbarnes@dowdbennett.com

MORRISON COHEN LLP

Jason Gottlieb (*pro hac vice* to be filed)
Michael Mix (*pro hac vice* to be filed)
Emma McGrath (*pro hac vice* to be filed)
909 Third Avenue
New York, New York 10022
(212) 735-8600
jgottlieb@morrisoncohen.com
mmix@morrisoncohen.com
emcgrath@morrisoncohen.com

Attorneys for Amici Curiae Blockchain Association and DeFi Education Fund

CERTIFICATE OF SERVICE

I certify that on August 22, 2024, a true and correct copy of the foregoing motion was filed and served in accordance with the Federal Rules of Civil Procedure via the CM/ECF filing system on all counsel of record.

Dated: Dallas, Texas
August 22, 2024

/s/ Ben A. Barnes
Ben A. Barnes