UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

DAN CARMAN, COIN CENTER, RAYMOND WALSH, QUIET INDUSTRIES CORP.,

Plaintiffs,

v.

JANET YELLEN, in her official capacity as Secretary of the Treasury; UNITED STATES DEPARTMENT OF TREASURY; CHARLES RETTIG, in his official capacity as Commissioner of the Internal Revenue Service; INTERNAL REVENUE SERVICE; MERRICK GARLAND, Attorney General, in his official capacity; UNITED STATES OF AMERICA,

Defendants.

Case No. _____

COMPLAINT

Plaintiffs file this complaint against Defendants for declaratory and injunctive relief against the enforcement of 26 U.S.C. §6050I's reporting mandate, as expanded by the 2021 Infrastructure Investment and Jobs Act.

NATURE OF THE ACTION

1. In 2021, President Biden and Congress amended a little-known tax reporting mandate. If the amendment is allowed to go into effect, it will impose a mass surveillance regime on ordinary Americans.

2. The amendment makes an ill-fitting reporting requirement apply to millions of citizens who participate in a wide range of transactions using "digital assets," a category defined to include any digital representation of value recorded on a cryptographically secured distributed ledger.

3. Digital assets include Bitcoin and similar technologies, commonly referred to as cryptocurrencies.

4. A cryptocurrency is a medium for payments, savings, and other economic activity. Thanks to digital software with fixed rules of operation, it facilitates the transfer of value without reliance on a "middleman" such as a bank or other financial institution. It allows people to transact with each other directly, securely, and privately.

5. Cryptocurrency plays a major role in the American economy. Some 59 million Americans already use cryptocurrency. The use of cryptocurrency creates jobs, drives economic growth, and spurs innovation. Cryptocurrency supports civil liberties and facilitates economic inclusion by making secure digital payments available to everyone.

6. No country has embraced cryptocurrency more than America and no State has embraced cryptocurrency more than Kentucky, which has become a world leader in cryptocurrency mining and innovation. The fate of many Kentuckians is wrapped up with and dependent on the future of cryptocurrency.

7. The 2021 amendment's reporting mandate threatens to hamstring cryptocurrency innovation and curtail the privacy rights of cryptocurrency users with overbearing surveillance.

8. The reporting mandate would force Americans using cryptocurrency to share intrusive details about themselves, both with each other and with the federal government. Under the terms of the mandate, everyday senders and receivers of cryptocurrency would be forced to reveal their names, Social Security numbers, home addresses, and other sensitive personal identifying information.

9. Receivers would then have fifteen days to report all of that information about both parties, along with the details of their transactions, to the federal government.

10. The 2021 amendment's reporting mandate would also require the receivers to maintain records of their transactions and the personal identifying information of senders for five years.

11. Cryptocurrency transactions are recorded on public ledgers. These public ledgers, available for viewing online, list alphanumerical "addresses" associated with

the participants in cryptocurrency transactions. But they do not reveal otherwise private information about senders and recipients. In this respect cryptocurrency transactions are uniquely private. If, however, a third party learns the real name of a person using a cryptocurrency address, then she can use the public ledger as a comprehensive database of all transactions sent to or received by that person.

12. Therefore, reports to the government about identifiable cryptocurrency transactions would provide a window into not only the transactions being reported, but also the participants' full unrelated transaction histories.

13. The reports required by the reporting mandate would therefore uncover a detailed picture of a person's personal activities, including intimate and expressive activities far beyond the immediate scope of the mandate. The reports would give the government an unprecedented level of detail about transactions within a realm where users have taken a series of steps to protect their transactional privacy.

14. The amendment's reporting mandate applies against all persons without the need for a warrant or probable cause. It is not narrowly tailored to any legitimate government interest because it reaches more conduct than necessary to achieve any income-tax or related objectives.

15. In practice, the amendment's reporting mandate would often be impossible to comply with because its terms do not coherently map onto the nature of the technology that it regulates.

16. And the reporting mandate does not include a jurisdictional or other hook connecting it to any constitutionally enumerated power.

17. The American Constitution forbids this. The amendment's surveillance regime is antithetical to the Bill of Rights. *See* U.S. Const., amends. I, IV, V. It is incompatible with a government of "few and defined" powers. *See* The Federalist No. 45 (Madison) at 292-293 (C. Rossiter ed. 1961). And it flouts recent Supreme Court jurisprudence meant to curtail exactly this sort of surveillance regime. *See Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Americans for Prosperity Found. v. Bonta*, 141 S. Ct. 2373 (2021); *United States v. Davis*, 139 S. Ct. 2319 (2019).

18. The amendment is scheduled to take effect for reports due on January 1, 2024, which could directly implicate digital asset receipts that occurred up to a year earlier and indirectly implicate transactions that are occurring now.

19. Plaintiffs Dan Carman, Coin Center, Raymond Walsh, and Quiet Industries use and intend to continue to use digital assets in transactions covered and affected by the reporting mandate. The mandate would force the disclosure of sensitive information in violation of their reasonable expectations of privacy and their property rights. It also would threaten to expose their protected associations and thereby chill their expressive activities.

20. Plaintiffs are entitled to a declaration that the amended §6050I's reporting mandate is facially unconstitutional and an injunction against its enforcement.

THE PARTIES

21. Plaintiff Dan Carman is an individual who regularly uses cryptocurrency. Mr. Carman resides in Fayette County, Kentucky.

22. Plaintiff Coin Center is an independent, non-profit research center focused on the public policy issues facing digital asset technologies. Coin Center's mission is to defend the rights of individuals to build and use free and open cryptocurrency networks: the right to write and publish code, to assemble into peer-to-peer networks, and to do all this privately. Coin Center's primary place of business is Washington, D.C.

23. Plaintiff Raymond Walsh is an individual who regularly uses cryptocurrency. Mr. Walsh resides in California.

24. Plaintiff Quiet Industries Corp. is a corporation with its principal place of business in Jessamine County, Kentucky.

25. Defendants Janet Yellen, United States Department of Treasury, Charles Rettig, Internal Revenue Service, Merrick Garland, and the United States of America and their agents are responsible for enforcement and administration of the amended 26 U.S.C. §6050I.

JURISDICTION AND VENUE

26. This Court has jurisdiction under 28 U.S.C. §§1331 and 1346(a)(2).

27. Plaintiffs' claims for declaratory and injunctive relief are authorized by 28 U.S.C. §§2201 and 2202 and by the general legal and equitable powers of this court.

28. Venue is proper in this judicial district under 28 U.S.C. §1402(a) and §1391(e) because Mr. Carman resides in Fayette County, Kentucky and Quiet Industries Corp. has its principal place of business in Jessamine County, Kentucky. Intradistrict venue is proper in the Lexington Division pursuant to Local Rule 3.2(a)(3).

BACKGROUND

Section 6050I

29. 26 U.S.C. §6050I, enacted in 1984, requires participants in certain transactions to report information about themselves and their transactions to the federal government. In the main, it requires persons engaged in a trade or business to file a report when they receive over $10,000 in cash:

> Any person … who is engaged in a trade or business, and … who, in the course of such trade or business, receives more than $10,000 in cash in 1 transaction (or 2 or more related transactions), shall make [a §6050I report].

26 U.S.C. §6050I(a).

30. Until now, the "cash" that was subject to §6050I meant physical "coin" or "currency." 26 C.F.R. §1.6050I-1(c)(1)(ii)(A). It also meant, in certain limited circumstances, cashier's checks. *Id.*

31. In other words, on those rare occasions when someone received over $10,000 worth of physical coins or dollar bills in the course of his trade or business—as opposed to ordinary checks, credit card payments, or other bank transfers—that

receiver would be required to submit a §6050I report to the government providing detailed information about the parties to the transaction and about the transaction itself.

32. The term "trade or business" means those transactions in which the receiver is engaged in a regular gain-seeking activity, which is defined in contradistinction to an "amusement diversion," a "hobby," or a "sporadic activity." *Comm'r v. Groetzinger*, 480 U.S. 23, 35 (1987); 26 C.F.R. §1.6050I-1(c)(6) (incorporating 26 U.S.C. §162's meaning of "trade or business"). The analysis of whether an activity constitutes a diversion, hobby, or sporadic activity as opposed to a trade or business depends on a nine-factor test with categories such as "[e]lements of personal pleasure or recreation," "[t]he expertise of the taxpayer or his advisors," and "[e]xpectation that assets used in activity may appreciate in value." 26 C.F.R. §1.183-2.

33. Non-profits and individuals can receive cash in the course of a "trade or business." *IRS Publication 557: Tax-Exempt Status for Your Organization*, 18 (2022), bit.ly/39yzo6I; *see, e.g.*, Yale University, *Memo of Cash Payer to Yale* (2022), bit.ly/3zgyTsT ("When the University receives in excess of $10,000 in cash in a single transaction (or in two or more related transactions), it is required to obtain the following information from the payor and provide it, along with payment information, to the IRS: Payer's name … address … date of birth … Social Security Number … occupation … passport or driver's license.").

34. The only "trades or businesses" that are exempt from the reporting mandate are banks and other financial institutions. 26 U.S.C. §6050I(c)(1)(B). The statute authorizes the Treasury Department to further exempt certain transactions from §6050I reporting if a bank or financial institution is involved in those transactions. 26 U.S.C. §6050I(c)(1)(A).

35. The exemptions for banks and financial institutions exist because those institutions are more highly regulated and subject to other reporting requirements. Among those reporting requirements is the Bank Secrecy Act's requirement that banks and similar financial institutions report the details of large cash transactions to the federal government. 31 U.S.C. §5313. These requirements are conventionally justified by the special nature of banks and financial institutions, which act as intermediaries and must collect personal identifying information in the ordinary course of business in order to reliably serve their customers' interests.

36. Section 6050I does not authorize the Treasury Department to exempt any additional transactions from mandatory reporting.

37. The statute also does not cover those transactions for which the "entire transaction occurs outside the United States," although it authorizes the Secretary to extend the statute to cover those transactions. 26 U.S.C. §6050I(c)(2).

38. Although a report need only be filed once the "$10,000" threshold is met, §6050I can affect a wide range of payments at much smaller dollar values. By its terms,

§6050I forces a receiver to keep track of whether any given transaction is "related" to any number of other transactions—including up to a full year earlier or later—that, when all are combined, amount to over $10,000.

39. As a result, even a small payment, such as for a concert ticket or lunch at a country club, could be related to other payments over the course of a year that, when combined, constitute a transaction or related transactions in excess of $10,000. And one person's very small payment could be a part of a larger transaction involving multiple people and therefore subject to §6050I.

40. But because §6050I was long limited to transactions in physical cash, payments were simple and receivers would meet senders in person. They therefore would know whether they had engaged in a large number of related cash transactions with them. This practical check has, until now, limited the impact of §6050I on smaller payments.

An Introduction to Digital Assets

41. The 2021 Infrastructure Investment and Jobs Act amended the definition of "cash" in §6050I to include, counterintuitively, "digital assets."

42. According to the Act, a "digital asset" is "any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology as specified by the Secretary." Pub. Law No. 117-58, §80603(b)(1)(D) (2021), *to be codified at* 26 U.S.C. §6045(g)(3)(D).

43. This definition targets Bitcoin and similar technologies that use cryptographically secured distributed ledgers, widely known as cryptocurrencies.

44. A cryptocurrency operates using open-source code, which is a computer program that anyone can view, copy, and use without the need to purchase it or seek a license. A person who wants to use cryptocurrency may do so simply by downloading and operating the program on his computer.

45. A cryptocurrency program consists of a system of fixed rules of operation designed to facilitate secure and reliable transactions. Any given cryptocurrency's rules may vary, but they tend to share the same common features.

46. To use a typical cryptocurrency, a person generates a "private key" which is a random but unique string of several letters and numbers. This key is unique to him. Unless he shares it or unless his computer is stolen or hacked, nobody else knows it.

47. A person's "private key" is mathematically linked to an "address," which is another string of letters and numbers. The address is also unique to the person. In some ways, an "address" is like a username and a "private key" is like a password.

48. To make a transaction, a receiver provides a sender with his address. The sender writes a transaction message to that address specifying the quantity of cryptocurrency that he is sending, such as 1 bitcoin.

49. The sender then digitally signs that message with his private key to prove that he is authorizing the transfer.

50. Other users of the cryptocurrency then review and validate the transaction message through a process called "mining." These miners check that the message is correctly signed and that the sending address controls sufficient cryptocurrency to fund the transaction.

51. Miners do not have any personal or business relationship with other users. They receive cryptocurrency automatically for any mathematically correct work they perform reviewing and validating transactions.

52. The mining process results in a public listing of the transaction on a public ledger. The listing includes the addresses of the sender and receiver, the quantity transferred, and the time of the transaction.

53. Anybody can view any transaction on the public ledger.

54. But the transactions listed on the public ledger are not linked to individuals' identities. The public ledger shows a series of transactions, but those transactions list only addresses that could belong to anybody and the amounts sent and received.

55. A cryptocurrency user does not need to share his personal identifying information, such as his name, address, and Social Security number, with anyone in order to use the technology. He does not need to provide it to a bank or similar middleman because the technology eliminates the need for such middlemen. He does not need to share his identifying information even with the parties with whom he

transacts. So when his transactions are posted to the public ledger, he may be the only one who knows that those transactions are his.

56. The Bitcoin "white paper," a computer science article written by Bitcoin's creator to introduce the technology to the world, described this as cryptocurrency's "new privacy model." Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 6 (2009), bit.ly/3uwVr5J.

57. As the white paper explained, when two users complete a transaction using Bitcoin, the public would be able to see "that someone is sending an amount to someone else." But, without more information, the public would not be able to "link[] the transaction to anyone." Nakamoto, *supra*, at 5.

58. But if a user's personal identifying information *is* linked to an address, then a person may access the public ledger and recognize that user's transactions. Such a person could search for the user's address and establish that user's personal transaction history, determine what causes he has supported, and uncover intimate details about his private affairs.

59. The Bitcoin white paper warned of this vulnerability: "[I]f the owner of a key is revealed, linking [on the public ledger] could reveal other transactions that belonged to the same owner." Nakamoto, *supra*, at 6.

60. There are two ways for an outsider to link someone's personal identifying information to his address. First, the user might simply share his address publicly.

Sharing his address would make it easy to identify all of his transactions, but it would also make it easier to transact with him, and some users are willing to do this. Second, the user could share the details of one of his transactions, which would allow someone to locate that transaction on the public ledger and deduce that the address involved was his. They could then search for other, unrelated transactions connected to the same address.

61. Although steps can be taken to increase the difficulty of linking multiple transactions, those steps are not ordinarily taken and are often insufficient. For example, although a user can create multiple private keys and multiple addresses to use in different transactions, public ledger analysts are often able to identify connected addresses. Complaint at ¶¶14-19, *United States v. 155 Virtual Currency Assets*, 2021 WL 1340971 (D.D.C. Apr. 9) (explaining law enforcement's use of "sophisticated, commercial services" to identify a user's multiple addresses).

62. To illustrate the cryptocurrency transactional process, imagine a cryptocurrency user named Bob. Bob's private key is "BBB" and his address is "XYZ123."

63. As long as Bob does not tell anybody that he controls that cryptocurrency address, then nobody will know.

64. Bob uses his cryptocurrency address to engage in a transaction with another user, Alice. Alice's cryptocurrency address is "ABC555." Bob signs a message with his corresponding private key, "BBB," to authorize the transaction.

65. Miners will then validate Bob's signature to complete the transaction. They will make sure that Bob used the correct private key and that Bob's key controlled the amount that he intended to send.

66. If the signature is valid then the public ledger will list Bob and Alice's transaction. The format of the listing may vary, but it will look something like this:

[Date and time] [Amount] XYZ123 → ABC555.

Anybody could see that listing on the public ledger.

67. Bob and Alice could both confirm their transaction on the public ledger because they know that those two addresses belong to them. But to anyone who does not know whom those addresses belong to, the transaction would simply involve two random addresses.

68. Bob and Alice may choose to keep their addresses to themselves and thereby keep their transactions private.

69. If their addresses become known to others, though, then those others would be able to find all of the transactions using those addresses. Public ledger analysts may also find all of Bob and Alice's transactions using *other* addresses by analyzing the activity of their known addresses. In other words, if Bob and Alice were

forced to reveal that they were the participants in the above transaction, then they would each also effectively reveal their participation in a wide range of other, unrelated transactions.

70. Cryptocurrency technology has many additional features and advantages. It allows people to transfer value across long distances without meeting in person and without middlemen. It secures transactions with mathematically robust systems that guarantee the validity and irreversibility of every transaction. It allows people to protect against inflation by using a store of value whose supply cannot be increased except according to predetermined formulas.

71. Cryptocurrency is far from perfect. Similar to the early days of the Internet, there are growing pains as cryptocurrency users learn, adjust, and explore the possibilities of their new technology.

72. But at the end of the day, cryptocurrency more than anything before it allows people to transact without leaving their privacy in the hands of others. Users can rest assured that, so long as they do not share their personal identifying information in combination with their public addresses, nobody in the world will be able to see and publicize what they choose to do with their own assets. They do not have to share their credit card numbers with every stranger with whom they transact. They do not have to share their personal identifying information with financial institutions. And they do not need to subject their every transaction to the supervision and approval of a bank that

may not share their interests or their values. Cryptocurrency users have finally developed and adopted a technology that allows them to conduct their affairs with genuine personal agency and privacy.

Digital Assets in America and Kentucky

73. For these reasons and many more, digital assets have become popular in America generally, and Kentucky particularly.

74. The archetypal digital asset, Bitcoin, was created in 2009. By 2018, about 25 million Americans owned Bitcoin or other cryptocurrencies. Nova, *Just 8 Percent of Americans Are Invested in Cryptocurrencies, Survey Says*, CNBC (Mar. 16, 2018), cnb.cx/3O2GQqk. The events of 2020 generated a wave of new users of cryptocurrency, and by early 2021, an estimated 46 million Americans owned Bitcoin. Reeves, *46 Million Americans Now Own Bitcoin, as Crypto Goes Mainstream*, Newsweek (May 11, 2021), bit.ly/3rdE1ZQ. About 59 million Americans were using some form of cryptocurrency by mid-2021. Laycock & Choi, *A Rising Number of Americans Own Crypto*, Finder (Jun. 14, 2021), bit.ly/3KrOXKV.

75. A wide range of businesses, from large corporations to corner stores and artisans, now accept cryptocurrency payments for everyday transactions. Contractors and employees accept wages in cryptocurrency and many people make a living mining cryptocurrency.

76. Many people use cryptocurrency to engage in expressive activities. And many charitable and advocacy organizations rely on cryptocurrency donations.

77. No State has embraced cryptocurrency more than Kentucky. Despite being less than 2% of the population, Kentuckians are responsible for approximately 19% of all Bitcoin mining in America. Sigalos, *New York and Texas Are Winning the War to Attract Bitcoin Miners*, CNBC (Oct. 9, 2021), cnb.cx/3rcSLbC (providing statistical breakdown by state). "Companies have set up racks of mining rigs … at sites left empty when coal mines shut down in Eastern Kentucky." Estep, *Kentucky's Digital Gold Rush. What's Behind the Crypto Mining Boom in Coal Country?*, Lexington Herald-Ledger (Mar. 29, 2022), bit.ly/3NRVCPN.

78. Cryptocurrency mining and use creates jobs for technicians, miners, and energy suppliers throughout Kentucky. Hawke, *Service Center Opening in Eastern Kentucky to Aid Bitcoin Mining Operations*, WYMT (Nov. 16, 2021), bit.ly/3vc4Z5v; Ashraf, *Blockware Solutions Builds 20MW Bitcoin Mining Data Center in Kentucky*, CoinDesk (Mar. 29, 2022), bit.ly/3vaDdpM. "Kentuckians are getting paid millions of dollars to serve as trusted validators of financial transactions happening around the world." Hadden, *Bitcoin Has the Potential to Be a Force for Good in Kentucky*, Lexington Herald-Ledger (Apr. 21, 2022), bit.ly/3NMalvM.

79. The Kentucky Legislature recently enacted legislation to attract even more cryptocurrency mining to the State. Chawla, *State of Kentucky Will Give Tax Exemptions*

for Bitcoin Mining, Crypto Briefing (Mar. 4, 2021), bit.ly/3urkgQu. Kentucky "can be not only a national, but global leader in this emerging market through these legislative efforts." Mudd, *Kentucky Poised to Be National Cryptomining Leader with New Tax Legislation*, Frost Brown Todd (Mar. 29, 2021), bit.ly/3NL1UAU.

The State and Cryptocurrency

80. As cryptocurrency grew in popularity, totalitarian governments around the world initiated a series of attacks on it.

81. The Chinese government banned banks from participating in transactions relating to cryptocurrency in 2013. It then threatened to label Bitcoin mining an "undesirable" industry and phase it out of existence. It began blocking websites that offered cryptocurrency trading services. And finally, in 2021, it outright banned all cryptocurrency trading and mining. *See* Sergeenkov, *China Crypto Bans: A Complete History*, CoinDesk (Sep. 29, 2021), bit.ly/38HVEuz.

82. When Canadian Prime Minister Justin Trudeau punished truckers for demonstrating against his vaccine mandates, he singled out cryptocurrency and sought to freeze the cryptocurrency activities of his opponents. Ashraf & Nelson, *Canada Sanctions 34 Crypto Wallets Tied to Trucker 'Freedom Convoy'*, Yahoo! News (Feb. 16, 2022), yhoo.it/39eDIrT. (Because cryptocurrency is not controlled by any central government or bank, Prime Minister Trudeau's efforts were only partly effective.) The Iranian government has banned cryptocurrency mining multiple times, purportedly to save

electricity. Haghdoost & Shahla, *Iran Orders Crypto-Mining Ban to Save Power During Winter Crunch*, Bloomberg (Dec. 28, 2021), bloom.bg/3v4QKR5. A handful of other governments have followed suit and banned it entirely. Quiroz-Gutierrez, *Crypto Is Fully Banned in China and 8 Other Countries*, Fortune (Jan. 4, 2022), bit.ly/3LmhFh3.

83. Meanwhile, cryptocurrency has played a role in supporting pro-freedom and pro-democracy protesters and communities around the world. Hamacher, *Hong Kong Protests Are Accelerating Bitcoin Adoption*, Yahoo! (Sep. 2, 2019), yhoo.it/3wIowuN; Gladstein, *In the Fight Against Extremism, Don't Demonize Surveillance-Busting Tools like Signal and Bitcoin*, Time (Jan. 26, 2021), bit.ly/3Gbpc07; Harper, *Nigerian Banks Shut Them Out, so These Activists Are Using Bitcoin to Battle Police Brutality*, CoinDesk (Oct. 16, 2020), bit.ly/38BhEaR; Barrett, *Ukraine Tweeted It Was 'Now Accepting Cryptocurrency Donations.' In two days, $12 Million Worth of Bitcoin, Ethereum, and USDT Poured in*, MSN (Feb. 28, 2022), bit.ly/3MAXlcn; Huang, *Dissidents Are Turning to Cryptocurrency as Protests Mount Around the World*, Forbes (Oct. 19, 2020), bit.ly/3KzA4q6.

84. Human rights activists from around the world have attested that "[w]hen crackdowns on civil liberties befell Nigeria, Belarus, and Hong Kong, Bitcoin helped keep the fight against authoritarianism afloat." Letter from Aderinokun et al. to Congress in Support of Responsible Crypto Policy (June 7, 2022), bit.ly/3ziQQad. As one freedom-fighting Ukrainian explained, cryptocurrency "literally saved the lives of my friends and many Ukrainians. Without it, we would not have been able to raise

money so quickly to pay for protective equipment for soldiers in the early days of the Russian invasion." *Id.*; *see also* Deutsch & Eglitis, *Putin's Crackdown Pushes Independent Russian Media Into Crypto*, Bloomberg (May 10, 2022), bloom.bg/3zsX6fL.

85. Cryptocurrency has also played an important role in empowering poor people in developing countries who lack access to credit cards and bank accounts. White & White, *Figure of the Week: The Rapidly Increasing Role of Cryptocurrencies in Africa*, Brookings (Jan. 27, 2022), brook.gs/3rXkT2v; *Bitcoin Adoption and Its Impacts on the Developing World*, The Guardian (Nigeria) (Oct. 28, 2021), bit.ly/38vSSIF; Ostroff & Malsin, *Turks Pile Into Bitcoin and Tether to Escape Plunging Lira*, Wall St. J. (Jan. 12, 2022), on.wsj.com/3auskZj. Venezuelans have written that cryptocurrency sustained them amidst economic turmoil. Hernandez, *Bitcoin Has Saved My Family*, N.Y. Times (Feb. 23, 2019), nyti.ms/3mlajiV. And human rights advocates say that "when currency catastrophes struck Cuba, Afghanistan, and Venezuela, Bitcoin gave our compatriots refuge." Letter from Aderinokun et al., *supra*.

86. For some time, it was widely believed that the United States would lead the way in embracing cryptocurrency. The United States mines more Bitcoin than any other nation in the world. *Bitcoin Mining Hashrate—the USA Dominates Global Mining Space, Commanding 35.4% of Global Hash Power*, Crypto Signals (Jan. 25, 2022), bit.ly/3JuFTnt; Sigalos, *How the U.S. Became the World's New Bitcoin Mining Hub*, CNBC (Jul. 17, 2021), cnb.cx/3JyQz4v.

87. Many American governors, legislators, mayors, and public figures across the political spectrum have celebrated America's pioneering role in the use of cryptocurrency. *See, e.g.*, Stewart, *Cryptocurrency Gets Warm Texas Welcome from Gov. Abbott*, Houston Chronicle (Jun. 22, 2021), bit.ly/3O0vtzk; *Gov. DeSantis Seeks 'Crypto Friendly' Florida*, CBS Miami (Dec. 10, 2021), cbsloc.al/3riBn52; Sigalos, *New York's Incoming Mayor Says Crypto Should Be Taught in Schools*, CNBC (Nov. 8, 2021), cnb.cx/3vdGu7F; Yaffe-Bellany, *The Rise of the Crypto Mayors*, N.Y. Times (Jan. 25, 2022), nyti.ms/3O4MUyB.

88. But America's role in this development has been cast into doubt by recent efforts to stifle cryptocurrency innovation. Special interests have won victories under the Biden Administration, including a broad new regulatory agenda targeted specifically at cryptocurrency. Klein, *How Biden's Executive Order on Cryptocurrency May Impact the Fate of Digital Currency and Assets*, Brookings (Mar. 17, 2022), brook.gs/3vaMxKl; Warmbrodt, *Elizabeth Warren's Anti-crypto Crusade Splits the Left*, Politico (Mar. 15, 2022), politi.co/3xlCPaF. They also have won legislative victories, none more damaging than the amendment to 26 U.S.C. §6050I at issue in this lawsuit.

The Amendment to §6050I

89. The amendment to 26 U.S.C. §6050I was inserted in the late stages of the legislative process surrounding the $1.2 trillion Infrastructure Investment and Jobs Act

of 2021. It was added as a "tax revenue" provision with no explanation or justification. 167 Cong. Rec. S5240-47 (daily ed. Aug. 1, 2021).

90. The amendment provides, in full, as follows:

> TREATMENT AS CASH FOR PURPOSES OF SECTION 6050I.— Section 6050I(d) of [the Tax] Code is amended by [adding to the definition of "cash" the following]: "(3) any digital asset (as defined in section 6045(g)(3)(D))."

Pub. Law No. 117-58, §80603(b)(3) (2021).

91. Section 6045(g)(3)(D), in turn, defines a "digital asset" as "any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology as specified by the Secretary."

92. In other words, the amendment takes the §6050I statutory and regulatory regime that has long applied to actual, physical cash and imposes those same rules on transactions involving digital assets. If the amendment is allowed to go into effect, transactions involving digital assets would be subject to §6050I's requirements that participants report detailed and sensitive information to the federal government.

93. Those requirements are as follows.

94. First, the sender would have to reveal to the receiver his Social Security number, name, and address. 26 U.S.C. §6050I(b). The receiver would then have to enter the sender's personal identifying information on a report transmitted to the government.

95. Second, the receiver would have to reveal to the government his own Social Security number, his name, and his address.

96. Third, the receiver would have to reveal the amount of digital assets that he received, the date of the transaction, and the "nature" of the transaction. 26 U.S.C. §6050I(b); 26 C.F.R. §1.6050I-1(e)(2).

97. Fourth, the receiver would have to reveal "any other information required by Form 8300," which is the IRS's mandatory template for all reports. 26 C.F.R. §1.6050I-1(e)(2). Additional information required by Form 8300 includes the Social Security number and identifying information of any person on whose behalf the sender acted. *Id.*

98. The receiver would also have to take steps to "verify the identity" of the sender. 26 C.F.R. 1.6050I-1(e)(3)(ii). He would have to do so by examining the sender's passport, driver's license, or similar documentation. *Id.*

99. The IRS Form 8300, on which all reports would have to be filed, is displayed here.

IRS Form **8300** (Rev. August 2014)
Department of the Treasury
Internal Revenue Service

Report of Cash Payments Over $10,000 Received in a Trade or Business

▶ See instructions for definition of cash.
▶ Use this form for transactions occurring after August 29, 2014. Do not use prior versions after this date.
For Privacy Act and Paperwork Reduction Act Notice, see the last page.

FinCEN Form **8300** (Rev. August 2014)
OMB No. 1506-0018
Department of the Treasury
Financial Crimes Enforcement Network

1 Check appropriate box(es) if: a ☐ Amends prior report; b ☐ Suspicious transaction.

Part I Identity of Individual From Whom the Cash Was Received

2 If more than one individual is involved, check here and see instructions ▶ ☐

3 Last name	4 First name	5 M.I.	6 Taxpayer identification number

7 Address (number, street, and apt. or suite no.)	8 Date of birth (see instructions) ▶ M M D D Y Y Y Y

9 City	10 State	11 ZIP code	12 Country (if not U.S.)	13 Occupation, profession, or business

14 Identifying document (ID)	a Describe ID ▶ c Number ▶	b Issued by ▶

Part II Person on Whose Behalf This Transaction Was Conducted

15 If this transaction was conducted on behalf of more than one person, check here and see instructions ▶ ☐

16 Individual's last name or organization's name	17 First name	18 M.I.	19 Taxpayer identification number

20 Doing business as (DBA) name (see instructions)	Employer identification number

21 Address (number, street, and apt. or suite no.)	22 Occupation, profession, or business

23 City	24 State	25 ZIP code	26 Country (if not U.S.)

27 Alien identification (ID)	a Describe ID ▶ c Number ▶	b Issued by ▶

Part III Description of Transaction and Method of Payment

28 Date cash received M M D D Y Y Y Y	29 Total cash received $ .00	30 If cash was received in more than one payment, check here ▶ ☐	31 Total price if different from item 29 $ .00

32 Amount of cash received (in U.S. dollar equivalent) (must equal item 29) (see instructions):

a	U.S. currency	$ .00	(Amount in $100 bills or higher $ .00)
b	Foreign currency	$ .00	(Country ▶)
c	Cashier's check(s)	$ .00	Issuer's name(s) and serial number(s) of the monetary instrument(s) ▶
d	Money order(s)	$ .00	
e	Bank draft(s)	$ .00	
f	Traveler's check(s)	$ .00	

33 Type of transaction

a	☐ Personal property purchased	f	☐ Debt obligations paid
b	☐ Real property purchased	g	☐ Exchange of cash
c	☐ Personal services provided	h	☐ Escrow or trust funds
d	☐ Business services provided	i	☐ Bail received by court clerks
e	☐ Intangible property purchased	j	☐ Other (specify in item 34) ▶

34 Specific description of property or service shown in 33. Give serial or registration number, address, docket number, etc. ▶

Part IV Business That Received Cash

35 Name of business that received cash	36 Employer identification number

37 Address (number, street, and apt. or suite no.)	Social security number

38 City	39 State	40 ZIP code	41 Nature of your business

42 Under penalties of perjury, I declare that to the best of my knowledge the information I have furnished above is true, correct, and complete.

Signature ▶ _____ Authorized official **Title** ▶ _____

43 Date of signature M M D D Y Y Y Y	44 Type or print name of contact person	45 Contact telephone number

Multiple Parties

(Complete applicable parts below if box 2 or 15 on page 1 is checked.)

Part I **Continued—Complete if box 2 on page 1 is checked**

3	Last name		4 First name		5 M.I.	6 Taxpayer identification number
7	Address (number, street, and apt. or suite no.)			8 Date of birth . . . ▶ (see instructions)		M M D D Y Y Y Y
9	City	10 State	11 ZIP code	12 Country (if not U.S.)	13 Occupation, profession, or business	
14	Identifying document (ID)	a Describe ID ▶ c Number ▶			b Issued by ▶	

3	Last name		4 First name		5 M.I.	6 Taxpayer identification number
7	Address (number, street, and apt. or suite no.)			8 Date of birth . . . ▶ (see instructions)		M M D D Y Y Y Y
9	City	10 State	11 ZIP code	12 Country (if not U.S.)	13 Occupation, profession, or business	
14	Identifying document (ID)	a Describe ID ▶ c Number ▶			b Issued by ▶	

Part II **Continued—Complete if box 15 on page 1 is checked**

16	Individual's last name or organization's name		17 First name		18 M.I.	19 Taxpayer identification number
20	Doing business as (DBA) name (see instructions)					Employer identification number
21	Address (number, street, and apt. or suite no.)				22 Occupation, profession, or business	
23	City	24 State	25 ZIP code	26 Country (if not U.S.)		
27	Alien identification (ID)	a Describe ID ▶ c Number ▶			b Issued by ▶	

16	Individual's last name or organization's name		17 First name		18 M.I.	19 Taxpayer identification number
20	Doing business as (DBA) name (see instructions)					Employer identification number
21	Address (number, street, and apt. or suite no.)				22 Occupation, profession, or business	
23	City	24 State	25 ZIP code	26 Country (if not U.S.)		
27	Alien identification (ID)	a Describe ID ▶ c Number ▶			b Issued by ▶	

Comments – Please use the lines provided below to comment on or clarify any information you entered on any line in Parts I, II, III, and IV

100. The receiver would have to sign the report under penalty of perjury and file it within 15 days of the transaction. 26 C.F.R. §1.6050I-1(e)(1).

101. The receiver would file the report by mailing it to the IRS's processing center in Detroit, Michigan, or by establishing an account with the government's E-Filing system and filing it online.

102. The receiver would also have to send a yearly written statement to each sender he reported to the IRS with the receiver's name and address along with the details of all of their covered transactions. 26 U.S.C. §6050I(e); 26 C.F.R. §1.6050I-1(f)(1).

103. The receiver would have to maintain in his possession a copy of every report made under §6050I for five years. 26 C.F.R. §1.6050I-1(e)(3)(iii).

104. The Government estimates that a §6050I report takes about 21 minutes to complete, assuming that the sender is fully compliant, easy to communicate with, and produces verifiable copies of all identification documents.

The Effects of the Amendment to §6050I

105. As a result of the amendment, every sender and receiver in a covered transaction would be forced to comply with this entire, intrusive process. Every receiver would be required to provide reports to the federal government within 15 days of the transaction, to maintain them in his own files, and to send yearly reports to all involved parties.

106. The reports would provide enough information about the transactions to allow the government to identify them in the public ledger.

107. The government could then ascertain the addresses of the individuals involved in the transaction. Using those addresses, it could ascertain the other, unrelated activities of those individuals, regardless of the amount involved in such other transactions and no matter when they occurred.

108. From one §6050I report in 2024, the government could discover that a person donated to a local mosque in 2016, paid for a son's sobriety treatment in 2018, contributed to an unpopular political cause in 2020, and hired a marriage counselor in 2022.

109. The government knows that the amended §6050I would enable such widespread surveillance. Already today, when it ascertains the identities of participants in cryptocurrency transactions—using other means, such as warrants—the government pays public-ledger analysts to determine what other transactions the participants have engaged in and what other addresses might belong to the participants. The government has enlisted agents and contractors to "analyz[e] blockchain and de-anonymiz[e] [crypto] transactions" to be "able to track, find, and work to seize crypto." *See* Moore, *Operation Hidden Treasure Is Here*, Forbes (Mar. 6, 2021), bit.ly/3Cnjh6k.

110. As anticipated, when the government ascertains the identity of a person using a cryptocurrency address, it "link[s]" him to other, "decentralized" addresses by

deciphering the addresses that he "transfer[s] to from [his] centralized exchanges." *How Does the IRS Track Your Cryptocurrency Transactions*, Daily Meta (Feb. 1, 2022), bit.ly/361Ci2d. One transaction can allow the government to access a person's entire transaction history. *See id.*

111. The government brags about how effective this method of surveillance can be at unearthing a cryptocurrency user's personal affairs. *See* Brief for United States, *United States v. Gratkowski*, 964 F.3d 307 at 7-8 (5th Cir. 2020) ("law enforcement has used these services in numerous past investigations and found it [sic] to produce reliable results"); Complaint at ¶¶14-19, *155 Virtual Currency Assets*, 2021 WL 1340971 ("generally, the owners of BTC addresses are not known unless the information is made public by the owner (for example, by posting the BTC address in an online forum or providing the BTC address to another user for a transaction)," but "analyzing the public transactions can sometimes lead to identifying both the owner of a BTC address and any other accounts [*i.e.*, addresses] that the person or entity owns and controls").

112. The amended §6050I would allow the government to use this method of surveillance against every user of cryptocurrency who engages in a single covered transaction.

113. It would thereby cause the disclosure of a detailed and intimate transaction history that would paint a mosaic of a person's life.

114. It would do so without a warrant, without a subpoena, without probable cause, and even without statutorily defined limiting factors or an opportunity for precompliance review.

115. Section 6050I's "related" transactions rule would cause the statute to affect even cryptocurrency users who never once made a covered transaction. Unlike transactions involving physical cash, there is no natural, common-sense way for a receiver to ensure that any cryptocurrency transaction is not "related" to other transactions up to a year earlier or later because cryptocurrency transactions are made digitally and without interfacing with the sender.

116. Therefore, to ensure compliance with §6050I, every receiver would have to demand every sender's personal identifying information and then maintain a database of all senders to ensure that he would know if and when the threshold was met. In other words, even the buyer of a $200 artwork or a $500 online course would be subject to the intrusive and burdensome demands of §6050I because the receiver would be obligated to ascertain whether those single purchases were related to past or future transactions.

117. It would also affect cryptocurrency users who paid small sums in transactions with many people that, in total, were worth more than $10,000. 26 CFR §1.6050I-1(e)(2); Form 8300, Part I. And it would affect these users even if they were merely the persons "on whose behalf the transaction was conducted" with no direct participation in the transaction. 26 CFR §1.6050I-1(e)(2); Form 8300, Part II. These rules

mean that even small upstream payments would require the collection and reporting of each sender's personal information.

118. The requirement that a sender provide a driver's license, passport, or similar form of identification would be nearly impossible to comply with in cryptocurrency transactions because they occur across vast distances and can involve an indeterminate number of persons.

119. The §6050I reports that go to the government may be shared with local, state, federal, and foreign law enforcement agencies, including for purposes unrelated to tax enforcement. *See* 26 U.S.C. §6103(l)(15). The prospect of these reports being shared would further invade the participants' privacy and chill their expressive activities.

120. The §6050I reports would also be kept by the receivers, who would include ordinary traders, merchants, laborers, and others engaging in "gain-seeking" activity. These people and entities have varying degrees of data security sophistication and not all could protect the reports from hackers, meddlesome employees, and identity thieves. Such intruders could use public ledger analysis to ascertain the unrelated private or expressive activities of the persons governed by §6050I and publicize those activities.

121. As a result of the amendment, users of cryptocurrency would be required to reveal information that belongs to them. And they would present to the government a mosaic of their lives incomparable to that generated by traditional financial reporting

requirements. They would do so in a sphere of activity in which they took careful and affirmative steps to preserve their privacy.

122. The reporting mandate effectively transforms a public activity that would reveal minimal private information about participants into an activity that reveals significant private information. In that sense, if a transaction on a public ledger is somewhat like driving a car on a public road, reporting the participants to that transaction is like putting a GPS tracker on that car.

123. Users of cryptocurrency would also be required to report expressive associations that fall within §6050I's coverage and they would be required to report commercial activities that, as a result of the nature of public ledgers, allow the government to ascertain their unrelated expressive activities.

124. As a result, users would naturally and foreseeably refrain from engaging in such expressive activities. They already are doing so in anticipation that present-day transactions may eventually be revealed.

125. Users would also be unable to determine how to comply with §6050I's terms that do not map coherently onto digital asset technology. In a wide range of cryptocurrency transactions, they would be unable to identify the statutory "person" that they must identify and report. 26 U.S.C. §6050I(a). For example, a miner receives cryptocurrency from cryptocurrency software itself, not any person at all, because a miner is automatically rewarded with new cryptocurrency when she performs

mathematically verifiable work to secure the public ledger. Similarly, a decentralized-exchange trader receives cryptocurrency through a decentralized exchange protocol that has no centralized entity or operator to identify the persons whose assets are combined in any given trade. And a user of certain kinds of advanced cryptocurrency protocols receives cryptocurrency upon the triggering actions of dozens or hundreds of people.

126. Users would also be unable to determine whether the "entire transaction occurr[ed] outside the United States," 26 U.S.C. §6050I(c)(2), when all cryptocurrency transactions are validated and stored on computers all around the world, including the United States, but otherwise exist purely in digital form.

127. Congress's terminological and conceptual confusion would prevent many people from engaging in cryptocurrency transactions altogether, even though these underlying transactions would, of course, remain entirely legal.

Punishment

128. Section 6050I is enforced through a number of severe criminal and civil sanctions. These sanctions apply to *senders* of digital assets, who must provide accurate and complete personal information to the receivers for the purposes of their reports. And they apply to *receivers* of digital assets, who must submit timely, complete, and accurate reports to the government and annual statements to each sender.

129. First, under 26 U.S.C. §7203, although willful violations of other tax-code reporting requirements are misdemeanors, "a willful violation of any provision of section 6050I" is a felony. Accordingly, the following willful conduct is a felony subject to a five-year prison term:

a. A receiver of digital assets fails to file a required §6050I report or files a report containing *any* "material omission or misstatement of fact." 26 U.S.C. §§7203, 6050I(f)(1)(B).

b. A sender of digital assets attempts to cause, or does cause, the receiver of those assets to fail to file a §6050I report, or to file an incorrect report. *Id.* §§6050I(f)(1)(A), (B).

c. A sender or receiver of digital assets—or any other person—assists or attempts to assist in "structuring" a transaction to evade the 6050I reporting requirement. *Id.* §6050I(f)(1)(C). "Structuring means breaking up a large cash transaction into small cash transactions." *IRS Publication 1544: Reporting Cash Payments of Over $10,000*, 4 (2014), bit.ly/3EB8EOm.

In other words, if either party does not wish to divulge his personal identifying information and every detail of his personal transactions to the other party and the government, then he commits a felony.

130. A number of additional provisions create additional penalties for those subject to §6050I.

a. A receiver of digital assets who intentionally disregards the requirement to file a timely and correct report is subject to a *minimum* fine of $25,000 per report. 26 U.S.C. §6721(e)(2)(C).

b. Regardless of intention, a receiver who files an incomplete or incorrect report or fails to file a report on time is subject to a fine of $250 per report. 26 U.S.C. §6721(a).

c. A receiver who intentionally disregards the duty to timely furnish an annual statement to the sender or to include all of the information required is subject to a minimum fine of $500 per statement. 26 U.S.C. §6722(e).

131. Civil penalties for violations of §6050I must first be paid in part before they can be challenged.

The Plaintiffs

132. Dan Carman was born and raised in Kentucky and today lives with his family in Fayette County, Kentucky. Mr. Carman attended school in Kentucky and served in the Marines in Iraq. He now works as a businessman and lawyer in Lexington. He regularly uses Bitcoin and engages in a wide range of transactions using Bitcoin. He intends to use it more going forward. He anticipates that some of his transactions would be directly subject to the amended 6050I and that others would be indirectly exposed as a result of the amended 6050I.

133. Mr. Carman intends to engage in several categories of conduct arguably covered by the amended §6050I.

134. First, he intends to receive cryptocurrency as payment for services in his business as a Bitcoin consultant. As a Bitcoin consultant, Mr. Carman helps provide small businesses with the wherewithal and technology to accept Bitcoin payments. Mr. Carman intends to receive payments for these services over $10,000 in both single transactions and multiple related transactions. He already today receives cryptocurrency as payment for his services as a Bitcoin consultant.

135. Second, he intends to mine cryptocurrency. He intends to mine Bitcoin personally and to have partial ownership in a Bitcoin mining company. He intends to receive over $10,000 in single and related transactions as a miner. He currently mines Bitcoin personally and has already identified associates, prepared a business plan, and identified mining sites for the Bitcoin mining company in which he will have partial ownership. He would personally be filing §6050I reports on behalf of this company.

136. Third, he intends to send cryptocurrency in a wide range of transactions. He intends to purchase Bitcoin mining machines for his mining operations. A typical Bitcoin mining machine can cost over $10,000. He intends to send and receive cryptocurrency through his participation in networks that facilitate high-speed transactions by passing cryptocurrency users' addresses at high volume according to predetermined agreements. He also intends to use Bitcoin for personal transactions,

from his transactions with general stores to pharmacies to hospitals. He knows firsthand from his consulting business that cryptocurrency use in businesses like these is already common and is likely to become prevalent. He already sends cryptocurrency in his business, through his participation in high-speed transaction networks, and in his personal affairs.

137. Mr. Carman also intends to use cryptocurrency to advance his expressive associations. He intends to use cryptocurrency to donate to advocacy and religious organizations. He donates to organizations that speak for the cryptocurrency community and intends to continue to donate to those organizations. He also regularly contributes to religious organizations, tithes to his community church, and intends to do so in the future using cryptocurrency.

138. Mr. Carman anticipates that he would have to reveal his receipt and sending of cryptocurrency and his personal identifying information against his will as a result of §6050I. He also anticipates that §6050I would make businesses more reluctant to use Bitcoin, which would hurt his business financially. He anticipates that as a result of §6050I, the government would use public ledger technology to uncover his unreported, unrelated transactions, which would include private and personal affairs that he does not wish to reveal to the government.

139. He also anticipates that as a result of §6050I, the government and other parties would use public ledger technology to uncover his expressive associations. Mr.

Carman believes that the private parties and governmental agencies who would store and collect these reports lack the cybersecurity capabilities to protect his personal information. As a result of these pressures caused by the anticipated enforcement of §6050I, he is already and would continue to be less likely to make contributions to advocacy and religious organizations and engage in other expressive activities.

140. Coin Center advances the civil liberty interests of cryptocurrency users. Coin Center educates policy makers about cryptocurrency and defends the rights of individuals to build and use free and open cryptocurrency networks—to write and publish code, to assemble into peer-to-peer networks, and to do all of this privately.

141. In the course of that activity, Coin Center receives contributions and sells sponsorships for fundraising events. Senders pay Coin Center in cryptocurrency worth over $10,000, including in single transactions. Coin Center would arguably be required to report its donors' personal identifying information as a result of §6050I. Coin Center does not wish to compile lists of its donors and share those lists with the government.

142. Coin Center engages in a wide range of activities using cryptocurrency. It receives payments of over $10,000 in cryptocurrency in exchange for tables, sponsorships, and promotions at its annual dinner. It receives payments of over $10,000 in cryptocurrency as contributions to its public advocacy activities. It intends to engage in these and similar transactions in the future.

143. Coin Center's advocacy activities depend on the contributions of many individuals. Many of these individuals would be subject to §6050I for their unrelated, commercial transactions. Many contribute to Coin Center anonymously. Many wish to keep their contributions private. As a result of §6050I, Coin Center anticipates that some of its donors would be less likely to donate out of fear that their unrelated donor activity would be revealed to the government and to other parties.

144. Raymond Walsh is a software engineer, small businessman, and self-taught Bitcoin miner. He lives with his family in California and they have a home in Jessamine County, Kentucky. He has built software for a range of successful American technology companies.

145. Mr. Walsh taught himself how to purchase and transact with cryptocurrency and eventually how to mine it. He prefers cryptocurrency to other assets for many reasons, including that it is more private and promotes personal autonomy.

146. Mr. Walsh now owns and operates Quiet Industries, a Bitcoin mining company with its principal place of business in Jessamine County, Kentucky. He travels to Kentucky regularly to install and maintain machines and improve his mining facility.

147. As the owner and operator of Quiet Industries, Mr. Walsh regularly receives Bitcoin payments over $10,000 in single transactions or related transactions. For the work that he does validating transactions, he is rewarded out of a common pool of

assets. Some of those assets come from cryptocurrency users whose transactions he is validating. Given the information available to him, it is likely impossible to trace them and secure the personal identifying information of every person from whom they were received. Other assets come from the Bitcoin software itself, which produces new bitcoins based on predetermined rules and delivers them to miners. The software that facilitates this system is owned by nobody, and directed by nobody.

148. Mr. Walsh also regularly spends over $10,000 in cryptocurrency in single transactions or related transactions. For his mining business, he buys mining machines for over $10,000 in Bitcoin.

149. Mr. Walsh expects to continue to send and receive those payments on a regular basis in the future. Mr. Walsh expects these payments to be his only source of income, and his family's livelihood will depend on them.

150. Mr. Walsh believes that his transactions would arguably be subject to §6050I. He believes that it would be exceedingly difficult and confusing to attempt to comply with §6050I as a miner.

151. Mr. Walsh also intends to use cryptocurrency to engage in other, unrelated activity. He believes that because of §6050I, the government would be able to use public ledger technology to connect him to those transactions.

152. Mr. Walsh does not wish to share the details of any of his transactions with the government.

153. Quiet Industries is a Bitcoin mining corporation with its principal place of business in Jessamine County, Kentucky. Quiet Industries regularly receives Bitcoin payments over $10,000 in single transactions and related transactions. It receives those payments from cryptocurrency users and the Bitcoin software itself. It also sends Bitcoin in exchange for mining machines. Quiet Industries will continue to engage in these transactions in the future.

154. Quiet Industries' activities would likely be subject to §6050I. It would be difficult or impossible to comply with §6050I's terms, many of which do not coherently map onto Quiet Industries' activities. As a result, Quiet Industries would face an uncertain and compromised business environment and would likely lose business.

CLAIMS FOR RELIEF

Count One
Fourth Amendment Unreasonable Search

155. Plaintiffs hereby incorporate by reference the allegations contained in all of the previous paragraphs as if fully set forth herein.

156. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The founding generation crafted the Fourth Amendment as a "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 134 S.Ct. 2473, 2494 (2014).

157. The antithesis of the Fourth Amendment is a regime by which the government can ascertain the private details of citizens' lives effortlessly and without suspicion of illegality. The Fourth Amendment is designed to "place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948). Its "basic purpose" is "to safeguard the privacy and security of individuals" against the government. *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528 (1967).

158. When the government violates a person's "reasonable expectation of privacy," then it has conducted a search. *United States v. Jones*, 565 U.S. 400, 407 (2012); *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

159. An individual has a reasonable expectation of privacy in "his or her personal affairs." *United States v. Haddix*, 239 F.3d 766, 767 (6th Cir. 2001).

160. When people take steps to keep matters private, then they are entitled to an enhanced expectation of privacy in those matters. A person loses a reasonable expectation in matters that he "knowingly exposes to the public." *Katz*, 389 U.S. at 351. But a person enjoys an enhanced expectation in matters that he takes affirmative steps to keep private. *Id.* at 352. When he "shuts the door" to a phone booth or "plac[es] his personal effects inside a double-locked footlocker," for instance, he manifests an expectation of privacy that is reasonable. *Id.* at 352; *United States v. Chadwick*, 433 U.S. 1, 11 (1977).

161. The amended §6050I would violate the reasonable expectations of privacy of both senders and receivers in covered transactions. It would force both parties to share their personal identifying information in conjunction with the details of their covered transactions, and thereby reveal sensitive details about their personal affairs.

162. This invasion of privacy would not be limited to cases in which the parties already shared their identifying information with the public, with an intermediary, or even with each other, but instead would apply to every covered transaction by every person, no matter how personal or confidential, and even though the transactions themselves would be perfectly legal.

163. The amended §6050I's surveillance would be more ubiquitous and unavoidable than even the reviled general warrants and writs of assistance of the colonial era. It would set the government up to passively collect the transactional histories of millions of Americans, imposing a universal and onerous requirement and turning citizens into involuntary reporters.

164. Digital asset users have developed and adopted a technology designed to preserve personal agency and protect enhanced privacy in transactions, which entitles them to an enhanced expectation of privacy. *See Katz*, 389 U.S. at 352.

165. Courts may not "uncritically extend existing precedents" under the Fourth Amendment without adjusting for "new concerns wrought by digital technology." *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018). Instead, "the Fourth

Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010). At bottom, courts must "assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Accordingly, the nature of cryptocurrency technology and the detailed picture of a person's affairs that it can generate deserve Fourth Amendment protection.

166. It does not help the government that this privacy infringement is achieved by legislative mandate rather than physical invasion by an executive officer. The Fourth Amendment protects people against "orderly taking under compulsion of process," *United States v. Morton Salt Co.*, 338 U.S. 632, 651-52 (1950), "administrative agency subpoenas [seeking] corporate books or records," *See v. City of Seattle*, 387 U.S. 541, 544 (1967), laws requiring people to unilaterally furnish evidence to the government, *Chandler v. Miller*, 520 U.S. 305, 313 (1997), and laws requiring businesses to report details of their transactions to the government, *Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467, 472 (S.D.N.Y. 2019). The "substance of the offense" under the Fourth Amendment "is the compulsory production of private papers," whatever the means. *Hale v. Henkel*, 201 U.S. 43, 76 (1906).

167. Even when the government does not invade a reasonable expectation of privacy, it conducts a search when it violates a person's property rights. *See Florida v.*

Jardines, 569 U.S. 1, 11 (2013); *United States v. Jones*, 565 U.S. 400, 405 (2012). The property-rights based approach "ask[s] if a house, paper or effect was *yours* under law." *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting) (emphasis added). To determine whether something was yours, courts look to preexisting property law and other sources of positive law. *Id*. (Gorsuch, J., dissenting); *see also United States v. Miller*, 982 F.3d 412, 432-33 (6th Cir. 2020).

168. Traditionally, "[t]he protection of private property extended to letters, papers, and documents." *Miller*, 982 F.3d at 432. If someone accessed such documents without consent, they would commit "trespass to chattels." *Id.* at 433.

169. Accordingly, if the government inspected someone's mail, that would violate the Fourth Amendment. *Ex Parte Jackson*, 96 U.S. 727 (1877).

170. In modern terms, it follows that even the opening of digital "files" without consent could therefore "be characterized as a 'trespass to chattels' and an illegal 'search.'" *Miller*, 982 F.3d at 433.

171. Personal information and data about one's activities are the "modern-day" versions of the "papers" and "effects" that the Fourth Amendment protects. *See Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

172. Here, the personal information subject to §6050I's reporting mandate is the modern-day equivalent of the "papers" and "effects" of the parties to the transaction. The government's collection of personal identifying information and

transactional information would be analogous to the collection of a vast number of paper receipts detailing otherwise private cash transactions.

173. Section 6050I's reporting mandate is in fact a worse rights violation than a standard compulsory disclosure of private papers and effects because it would force subjects to first create the papers and effects before delivering them to the government. It is analogous to coercion by threat followed by trespass to chattels.

174. Nor can the amended §6050I be saved by the so-called "third party doctrine."

175. First, the parties to §6050I transactions are not conventional third parties because they do not serve in an intermediary role. One of the central stated goals of cryptocurrency is to allow transactions *without* the intermediary institutions that implicate the third-party doctrine, such as banks and telephone companies. *See Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976).

176. Second, the parties to covered transactions do not even share the personal information in question with each other, so the simplest premise of the third-party doctrine is missing. *See Miller*, 425 U.S. at 443 ("[A defendant] takes the risk, *in revealing his affairs to another*, that the information will be conveyed by that person to the Government.") (emphasis added). Parties to cryptocurrency transactions may have no reason to share even their names with each other in the course of a transaction, let alone their Social Security numbers.

177. Third, if the parties did share that information, they would do so because §6050I coerces them to, rather than "voluntarily." *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 744.

178. Fourth, the parties to covered transactions do not have reason to share the information at issue "in the ordinary course of business" or "for a variety of legitimate business purposes." *Miller*, 425 U.S. at 443; *Smith*, 442 U.S. at 744. While a bank needs to know its customers' personal information to protect against fraud and identity theft, digital asset technology exists precisely to overcome those risks and to ensure security through verifiable mathematical techniques, such as digital signatures.

179. Fifth, the third-party doctrine is restricted to the sharing of information that provides a "limited" view of a person's affairs, not a detailed mosaic. *Smith*, 442 U.S. at 742; *Carpenter*, 138 S. Ct. at 2217. Heightened protection applies to information that would reveal a person's "familial, political, professional, religious, and sexual associations," which is exactly what revealing the names associated with public cryptocurrency transactions would do. *Carpenter*, 138 S. Ct. at 2217; *see also United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) ("*Miller* involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue here"). That heightened protection especially applies when the intimate information is collected effortlessly. *Carpenter*, 138 S. Ct. at 2217-19.

180. Sixth and finally, the third-party doctrine, even where it would otherwise apply, is limited to transactions at a sufficiently high value, which, due to inflation, §6050I's "$10,000" threshold no longer satisfies. *See California Bankers Ass'n v. Shultz*, 416 U.S. 21, 78-79 (1974) (Powell, J., concurring, joined by Blackmun, J.) ("In their full reach [to transactions under $10,000], the reports apparently authorized by the open-ended language of the [Bank Secrecy] Act touch upon intimate areas of an individual's personal affairs. 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."); *id.* at 79 (Douglas, J., dissenting); *id.* at 91 (Brennan, J., dissenting); *id.* at 93 (Marshall, J., dissenting); *CPI Inflation Calculator*, Bureau of Labor Statistics (accessed June 5, 2022), bit.ly/3KUnZvb (showing that $10,000 in 1974 would be the equivalent of $60,000 in 2022).

181. The search regime that the amended §6050I would impose is "unreasonable," U.S. Const, amend. IV, because it would not satisfy the warrant requirement or any exception to the warrant requirement. "[W]arrantless searches are per se unreasonable under the Fourth Amendment" unless a "specifically established and well-delineated exception[]" applies, such as for exigent circumstances. *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) (cleaned up); *see also Katz*, 389 U.S. at 357; *Arizona v. Gant*, 556 U.S. 332, 338 (2009).

182. Here, the government would not comply with the warrant requirement in effecting searches under the amended §6050I. It would effect a Fourth Amendment search on every person who engaged in a covered transaction without any attempt at judicial authorization. Its search regime would not fall within an exception for administrative searches because there is no "special need" here that makes warrant requirements impracticable. In any event, amended-§6050I searches would be effected with no opportunity for "precompliance review." *See City of Los Angeles v. Patel*, 576 U.S. 409, 420 (2015); *see also Airbnb*, 373 F. Supp. 3d at 491. And the amended §6050I search regime would not fall within an exception for a "closely regulated industry" because it would cover the entire economy.

183. Accordingly, the amended §6050I would effect an unreasonable search in violation of the Fourth Amendment.

Count Two
First Amendment Association

184. Plaintiffs hereby incorporate by reference the allegations contained in all of the previous paragraphs as if fully set forth herein.

185. The First Amendment protects "the freedom of speech," and "of the press," and "the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. Const., amend. I. These "First Amendment freedoms" have "always occupied a preferred status in constitutional

jurisprudence," "for it is these freedoms which ensure a free and democratic society." *Martin v. Kelley*, 803 F.2d 236, 240 (6th Cir. 1986).

186. "[I]mplicit in the right to engage in activities protected by the First Amendment" is "a corresponding right to associate with others." *Roberts v. United States Jaycees*, 468 U.S. 609, 622 (1984). That is because the "freedom to speak, to worship, and to petition the government for the redress of grievances could not be vigorously protected from interference by the State unless a correlative freedom to engage in group effort toward those ends were not also guaranteed." *Id*.

187. The First Amendment protects Americans' freedom to associate for "a wide variety of political, social, economic, educational, religious, and cultural ends." *Shelton v. Tucker*, 364 U.S. 479, 486 (1960).

188. Freedom of association includes a right to associational privacy. There is a "vital relationship between freedom to associate and privacy in one's associations." *Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960). Without associational privacy, many unpopular viewpoints would not be voiced at all. *Talley v. California,* 362 U.S. 60, 64 (1960).

189. Infringements on associational privacy "chill[] speech by exposing anonymous donors to harassment and threats of reprisal." *Del. Strong Fams. v. Denn*, 136 S. Ct. 2376 (2016) (Thomas, J., dissental). Individuals have a "strong associational interest in maintaining the privacy of" their associational activities. *Gibson v. Fla. Legis.*

Investigation Comm., 372 U.S. 539, 555-56 (1963). Therefore, the Supreme Court has concluded that "[i]nviolability of privacy in group association" is "indispensable to preservation of freedom of association" and is protected by the First Amendment. *Bates*, 361 U.S. at 523.

190. The inviolability of privacy in associations means that Americans presumptively enjoy a right against reporting mandates.

191. "[C]ompelled disclosure of affiliation with groups engaged in advocacy" constitutes an "effective restraint on freedom of association." *NAACP v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 462 (1958); *see also Buckley v. Valeo*, 424 U.S. 1, 64 (1976).

192. Reporting mandates chill protected associational activities in at least two ways. First, mandatory reporting laws deter the associational activities of those who would prefer to remain anonymous. *See Buckley v. Valeo*, 424 U.S. at 68. The "decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible." *Watchtower Bible Tract Society v. Village of Stratton*, 536 U.S. 150, 166 (2002). If someone is forced to reveal his identity "as a precondition to expression," he is less likely to engage in that expressive activity. *Peterson v. National Telecommunications*, 478 F.3d 626, 632 (4th Cir. 2007).

193. Second, reporting mandates deter associational activities of everyone "by exposing donors to retaliation." *Citizens United v. FEC*, 130 S. Ct. 876, 916 (2010); *see also*,

e.g., Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 100 (1982). While it is one thing to share your personal information with a friendly association, it may be quite another to share it with the government. Reporting of expressive activities to the government discourages proponents of controversial viewpoints from taking action because it exposes them to harassment or retaliation. *See Peterson*, 478 F.3d at 632.

194. Reporting mandates need not *target* advocacy associations to violate the First Amendment. To the contrary, in a successful associational challenge, "[t]he governmental action challenged may appear to be totally unrelated to protected liberties." *Patterson*, 357 U.S. at 461. "Revealing the names of persons who participated in [an entity's] commercial activities, for example, could also reveal the names of adherents to [that entity's] ideology." *In re Grand Jury Proceeding*, 842 F.2d 1229, 1235 (11th Cir. 1988).

195. What matters to the First Amendment inquiry is whether the reporting mandate, whatever its target, "ha[s] the consequence of unduly curtailing the liberty" of those subject to it. *Patterson*, 357 U.S. at 461-62. This unconstitutional consequence is sometimes achieved through forced disclosure of membership and contributor lists, *Patterson*, 357 U.S. at 453; *Baldwin v. Commissioner*, 648 F.2d 483, 485-87 (8th Cir. 1981); *Familias Unidas v. Briscoe*, 619 F.2d 391, 402 (5th Cir. 1980), forced disclosure of the personal information of those who hold interests or accounts in a business, *East Brooks Books, Inc. v. City of Memphis*, 48 F.3d 220, 226 (6th Cir. 1995); *In re First National Bank*,

701 F.2d 115, 116 (10th Cir. 1983), or forced disclosure of financial records that would "identify the members of and contributors to [an organization]," *United States v. Citizens State Bank*, 612 F.2d 1091, 1093 (8th Cir. 1980).

196. The presumption against reporting mandates was prescient. Today, journalists, hackers, and political operatives work together to reveal and publicize the personal information of people who privately associate with or donate as little as $10 to unpopular causes. *See, e.g.*, Lambrecht, *CNN Analyst Doxxes Recent Hillsdale Grad*, Hillsdale Collegian (Sep. 3, 2020), bit.ly/3zftlP9. Kaminsky, *ABC Utah Reporter Stalks, Doxes Private Citizen Who Donated $10 To Kyle Rittenhouse Defense Fund*, The Federalist (Apr. 19, 2021), bit.ly/3vXWsVR. Private donors' addresses and other identifying information are spread without their permission. Annable, *Hacked Convoy Donation Data Shows Concentration of Donors from Southern Manitoba*, CBC (Feb. 17, 2022), bit.ly/3ECN9N8. Government agencies and politicians use information that they receive about protected activities to retaliate against those involved in them. *See, e.g.*, Gregory, *The Timeline of IRS Targeting of Conservative Groups*, Forbes (Jun. 25, 2013), bit.ly/36VnOkG; *Editorial: Durbin's Enemies List*, Chicago Tribune (Aug. 8, 2013), bit.ly/3KkYLpH. Victims of these tactics span the political spectrum. *See, e.g.*, Lee, *How Right Wing Extremists Stalk, Dox, and Harass Their Enemies*, The Intercept (Sep. 6, 2017), bit.ly/3tQSDyO.

197. A recent survey revealed that 62% of Americans now feel that "the political climate these days prevents me from saying things I believe." *Summer 2020 National Survey*, Cato Institute (Jul. 22, 2020), bit.ly/35ra7Kd. Within every political group except "strong liberals," a majority of people feel that they can no longer say things that they believe. *Id.* And 32% of all Americans believe that their personal views, if revealed, could affect their jobs and livelihoods. *Id.*

198. As a result, truly private associations have become the last refuge of Americans fearful of the consequences of engaging in public life. Any form of "disclosure of donor information, whether it be compelled by the government or hacked and leaked, causes people to think twice before exercising their rights to speak or support organizations with which they agree." Hauenschild & Marchese, *Chilling Effect: Donor Disclosure, Hackers, and the Freedom Convoy*, ALEC (Feb. 25, 2022), bit.ly/35O235U. Would-be donors regularly tell groups and politicians that they cannot donate for fear of public revelation. Strassel, *Challenging Spitzerism at the Polls*, Wall St. J. (Aug. 1, 2008), on.wsj.com/3Kiw6Bv.

199. The Supreme Court recently expanded the First Amendment's protection against reporting mandates. In *Americans for Prosperity Foundation v. Bonta*, it held that the First Amendment forbade a state government from mandating that charitable organizations report the personal identifying information of their donors who sent them over $5,000. 141 S. Ct. 2373, 2389 (2021). It reasoned that a reporting requirement

was unconstitutional because it "cast[] a dragnet" for sensitive information about people and organizations engaged in advocacy activities. *Id.* at 2387. And it held the reporting mandate unconstitutional on its face because "a substantial number of its applications [were] unconstitutional" as compared to "the statute's plainly legitimate sweep." *Id.*

200. The amended §6050I would infringe on expressive activity and therefore triggers First Amendment scrutiny. It is a quintessential reporting mandate in that it would require parties to reveal expressive associations to the government. The reporting mandate would chill and is already chilling protected associational activities in at least three ways.

201. First, §6050I's reporting mandate would chill expressive activity because it would allow the government to ascertain the unrelated expressive associations of parties to all covered transactions. If a person disclosed to the government that he gave $10,000 worth of bitcoin to a known recipient on a certain date in a commercial transaction, for example, then the government would be able to use public-ledger analysis to determine that five years earlier he gave $5 worth of Bitcoin to a dissident journalist or a minority religious sect.

202. Second, the design of §6050I would all but guarantee that hackers would be able to access and publicize the information contained in §6050I reports. A §6050I report can be completed only if the receiver collects the sender's personal information

and completes the detailed report himself. Under §6050I(e), receivers would be required to keep copies of all forms submitted to the government in their files. *See* 31 C.F.R. §1.6050I-1(e)(3)(iii). Such receivers would include traders, merchants, and laborers who would not be accustomed to safeguarding the highly sensitive information of others. Hackers, and possibly employees of these receivers, would likely target these reports, knowing that they would be able to use them to link an identity to a public address and reveal previously unknown expressive activity.

203. Third, §6050I's reporting mandate would directly mandate the reporting of expressive associations. Although §6050I would apply only to receipts in the course of a "trade or business," that criterion does not exclude protected activities. "The First Amendment's protection of expressive association is not reserved for advocacy groups." *Boy Scouts of America v. Dale*, 530 U.S. 640, 648 (2000). Rather, "to come within its ambit, a group must engage in some form of expression, whether it be public or private." *Id.* And in any event, many contributions to advocacy groups would fall within the course of a trade or business. A wide range of expressive associations—from funders of independent media to non-profits that sell sponsorships to friendly supporters—would be protected but nonetheless subject to §6050I.

204. Furthermore, the §6050I reports that would go to the government could be shared with local, state, federal, and foreign law enforcement agencies, each of which could have its own security vulnerabilities. Because "each governmental demand for

disclosure brings with it an additional risk of chill," *Bonta*, 141 S. Ct. at 2389, and because these entities may not be well equipped to secure their files, this sharing arrangement would exacerbate the chilling effects generated by §6050I.

205. Reporting mandates must be "narrowly tailored to the government's asserted interest." *Id.* at 2383. That means that "a substantial relation to an important interest," which may suffice in other First Amendment contexts, "is not enough to save a disclosure regime[.]" *Id.* at 2384.

206. In other words, "[r]egardless of whether there is any risk of public disclosure, and no matter if the burdens on associational rights are slight, heavy, or nonexistent, disclosure regimes must *always* be narrowly tailored." *Id.* at 2398 (Sotomayor, J., dissenting) (emphasis added).

207. The amended §6050I is not narrowly tailored. Because §6050I imposes its mandatory reporting regime universally, it can hardly be said to reflect the sort of careful proportionality that First Amendment scrutiny demands. It does not even tailor its scope to reportable income or to activities with some heightened likelihood of criminality. It instead "casts a dragnet" for sensitive information from everyone who participates in high-value cryptocurrency transactions, "even though that information will become relevant in only a small number of cases." *See id.* at 2387 (majority).

208. "Mere administrative convenience does not remotely 'reflect the seriousness of the actual burden' that the demand for [§6050I reports] imposes on

[participants'] association rights." *See id.* The Government must instead pursue its interests by less invasive and universal means.

209. The amended §6050I's reporting mandate therefore violates the First Amendment right to associational privacy.

Count Three
Fifth Amendment Vagueness

210. Plaintiffs hereby incorporate by reference the allegations contained in all of the previous paragraphs as if fully set forth herein.

211. The Fifth Amendment protects against government "depriv[ations] of life, liberty, or property, without due process of law." U.S. Const., amend. V. The Constitution's separation of powers ensures that all federal "legislative powers" are vested exclusively in Congress. U.S. Const., Art. I. The government violates the Fifth Amendment's Due Process Clause and the separation of powers when it seeks to punish citizens based on vague laws. *See United States v. Davis*, 139 S. Ct. 2319, 2323 (2019).

212. A statute is void for vagueness when it does not provide fair notice of what the law demands. *Id.*

213. When Congress attempts to impose a reporting mandate for technology that it does not understand by extending rules from a different context, it creates intractable vagueness problems. Although §6050I's statutory elements of senders, receivers, and receipt have clear meanings when applied to face-to-face transfers of

physical cash, they do not translate to transactions using digital asset technology. The translation problems render the statute incoherent—and impossible to understand how to comply with—in many ways.

214. First, the amended §6050I assumes that the notion of a "person from whom the [digital assets were] received," *see* 26 U.S.C. §6050I(b)(2)(A), remains coherent and that such a person remains identifiable in the context of digital assets. But that is not the case. While it is hard to imagine obtaining $10,000 in physical cash in the course of a trade or business from nobody at all or from people who cannot possibly be identified, the technology underlying digital assets changes that.

215. Cryptocurrency miners, for example, "receive" digital assets for mining. They receive these assets from the global users of the platform, but also in the form of newly-minted assets that do not come from any person at all. The software that facilitates the miner-reward system is owned by nobody, and directed by nobody. Yet a miner, upon his lawful receipt of such assets, would be fined or subject to prison time unless he could determine the name, Social Security number, and other identifying information of the "person from whom" that value was received. The law therefore demands the impossible of him and cannot be understood by anyone, let alone someone of common intelligence.

216. A similar problem occurs in attempting to map the notion of a "person from whom the [digital assets were] received," onto another cryptocurrency activity,

"decentralized exchange." Decentralized exchange describes a common cryptocurrency method for exchanging one digital asset for another. The exchange is not facilitated by a person, but rather by a computer program that is, again, beyond the control of any person. The digital assets that a receiver acquires through decentralized exchange may have once belonged to one person or may have been supplied by a combination of thousands of people, but the software itself provides them. A receiver in this situation would have no way to identify any "person from whom the [digital assets were] received" and the proposition that such a person exists is metaphysically dubious.

217. Second, the amended §6050I assumes that a transfer of digital assets, when attributable to human beings at all, can be attributable to an identifiable "person." 26 U.S.C. §6050I(b)(2)(A). But many cryptocurrency transactions depend on the coordinated actions of many persons, no single one of whom can be said to be the "person from whom" such assets "are received." For example, cryptocurrency technology allows for transfers of value when a certain number of users out of a larger set sign off on a transaction. Funds may be transferable upon the approval of 20 out of 30 potential signers. When such transfers occur, receivers have no way to identify the "person" who sent them the asset.

218. A similar problem occurs in online cryptocurrency sales. Cryptocurrency enables the sale of digital items in a manner that makes it difficult or impossible for a seller to ascertain a buyer's personal identifying information. A merchant who would

like to sell a digital item, such as digital artwork, often puts that item for sale such that the sale is completed automatically and securely once any buyer meets the asking price. Once someone provides a cryptocurrency payment, a seller would automatically receive that cryptocurrency in a qualifying transaction for the purposes of §6050I. But that seller may not even know that he has received the payment and would often have no way to determine anything about the sender.

219. Third, the statutory requirement of a "receipt" is vague in the context of digital assets. A sender may relinquish control of digital assets in various ways without any new person securing control of them. For instance, a sender may assign assets to a "multi-signature" address or to an address where multiple people possess the private key. In those instances, no person will immediately or exclusively "receive" the assets. But felony prison time will depend on ascertaining the proper time and person to fill out and submit a report.

220. This problem is made worse by the fact that there is no way to tell that an address has received digital assets besides checking regularly. Unlike an exchange of physical cash, a cryptocurrency transaction requires no affirmative activity or awareness on the part of the receiver. Anyone may provide cryptocurrency to an address at any time. A receiver who doesn't monitor transactions involving his address regularly may revisit it one day to discover that a valuable asset was sent to him two months earlier.

Under the terms of the amended §6050I, such a person may have committed a crime when he did not report it.

221. Fourth, §6050I applies only to transactions for which it cannot be said that "the entire transaction occurs outside the United States." 26 U.S.C. §6050I(c)(2). But this element of geographical location does not work with digital asset technology because digital assets never exist in one place at any given time. Instead, they exist on a public ledger that is validated and maintained by computers all over the world. A person with digital assets does not physically possess anything like cash, but instead simply knows the private key that will enable him to use those assets, stored on servers around the world, when he would like to do so from anywhere in the world. It could be plausibly argued that every transaction occurs within the United States because digital asset transactions by their nature implicate computers in the United States, but the same transactions also lack any specific geographic, physical location. Users would have no way to know whether they satisfied this element of §6050I.

222. These difficulties are exacerbated by underlying vulnerabilities of the §6050I framework itself, difficulties which had long been minimized due to the rarity of high-value transactions in cash. The statute's restriction to receipts in the course of a "trade or business" implicates a notoriously vexing definitional problem. The term "trade or business" is defined to cover a range of gain-seeking activity, the scope of which may depend on an amorphous nine-factor test. 26 C.F.R. §1.183-2. The nine-factor

test comes from another section of the tax law that governs whether a taxpayer is eligible for certain deductions. The vagueness of the test was offset, to some degree, by the fact that in that context it could only affect the allocation of benefits. But now Americans engaged in ordinary transactions would face a felony prison term if they could not decipher it.

223. And the test is particularly ill-suited for the cryptocurrency economy. To take one example, many people engage in cryptocurrency trading. Under current law, sporadic trading activity is *not* engaged in in the course of a "trade or business"—even though it is engaged in for profit—but rather is treated as an "[e]xpense[] for the production of income" under 28 U.S.C. §212. But at some point, investment activity becomes sufficiently common that it qualifies as a "trade or business." Nobody knows where that line is drawn—courts have held that it's somewhere between 303 and 1,543 trades per year. *Endicott v. Comm'r*, 106 T.C.M. 184 (T.C. 2013). And nobody has explained how this legal doctrine, which imposes a trade-or-business line on trades *per year*, can be applied to a reporting mandate that imposes a trade-or-business line on individual transactions.

224. The prohibition on "structuring" transactions to avoid regulation under §6050I is similarly problematic. The IRS has said that this term encompasses "[s]etting up, helping to set up, or trying to set up a transaction in a way that would make it seem unnecessary to file Form 8300." *IRS Publication 1544: Reporting Cash Payments of Over*

$10,000, 4 (2014), bit.ly/3EB8EOm. But because nobody wants to file a highly intrusive and time-consuming report, many would take steps to avoid implicating §6050I, such as pricing goods and services below the threshold if the difference in value is not worth their time or using alternative methods of payment. It is difficult to tell which of these steps, which would become far more common upon §6050I's expansion, would constitute felonies.

225. Finally, it is difficult to imagine how digital asset users are to understand the requirement that they take steps to "verify the identity" of the sender by examining his passport, driver's license, or similar documentation. 26 C.F.R. 1.6050I-1(e)(3)(ii). Digital asset users interact across the world and cannot compare driver's licenses to faces in person or verify identification documents in any surefire way. They would therefore be forced to guess as to whether their new verification methods sufficed or give up on making a wide range of transactions altogether.

226. Congress may regulate new technologies, but it must do so using categories and terms that reflect the nature of those technologies. If it would like to regulate cell phones like it regulated landlines, then it must not legislate in terms of wires and fibers and jacks. And if it would like to regulate cryptocurrency like it regulated cash, then it must not legislate on the assumption that all transactions are conventional, in-person, and bilateral. The categories and terms of §6050I cannot be

reconciled with the nature of cryptocurrency technology, so the law is unconstitutionally vague.

Count Four
Congress's Enumerated Powers

227. Plaintiffs hereby incorporate by reference the allegations contained in all of the previous paragraphs as if fully set forth herein.

228. "The powers delegated by the [ ] Constitution to the federal government are few and defined." *United States v. Lopez*, 514 U.S. 549, 552 (1995) (quoting The Federalist No. 45 (Madison) at 292-293 (C. Rossiter ed. 1961)). The design of a federal government with few and defined powers "was adopted by the Framers to ensure protection of our fundamental liberties." *Gregory v. Ashcroft*, 501 U.S. 452, 458 (1991).

229. The Sixteenth Amendment grants to Congress the power to "lay and collect taxes on incomes." U.S. Const., amend. XVI. It "authorizes the imposition of an income tax without apportionment among the states." *Broughton v. United States*, 632 F.2d 706, 707 (8th Cir. 1980). It thereby expands on the original Article I power to lay and collect taxes but only in limited circumstances. *See* U.S. Const, Art. I, §8.

230. The amended §6050I is not an exercise of the power to "lay and collect taxes on incomes." It neither lays nor collects any taxes. Its terms are not even limited to transactions involving income that is reportable for tax purposes. Rather, it forces receivers in certain transactions to report to the government detailed information about themselves, the senders, and their transactions simply by virtue of participating in those transactions.

231. Congress also has the power to "make all Laws which shall be necessary and proper for carrying into Execution" its enumerated powers. U.S. Const., art. I, §8, cl. 18. The Necessary and Process Clause "vests Congress with authority to enact provisions incidental to the enumerated power, and conducive to its beneficial exercise." *Nat'l Fed'n of Indep. Bus. v. Sebelius*, 567 U.S. 519, 559 (2012) (cleaned up).

232. Although the Clause gives Congress authority to "legislate on that vast mass of incidental powers which must be involved in the constitution," it does not license the exercise of any "great substantive and independent power[s]" beyond those specifically enumerated. *Id.*; *see also Bond v. United States*, 572 U.S. 844 (2014). The Clause is "merely a declaration, for the removal of all uncertainty, that the means of carrying into execution those [powers] otherwise granted are included in the grant." *NFIB*, 567 U.S. at 559.

233. Any laws not "consistent with the letter and spirit of the Constitution" are "not proper means for carrying into execution Congress's enumerated powers." *Id*. at 559-60 (cleaned up).

234. The amended §6050I is not "necessary and proper" for executing the power to "lay and collect taxes on incomes." It is rather an exercise of a great substantive and independent power to implement broad surveillance on the daily transactions of people who use a technology that the government disfavors. The income tax can be executed competently without indiscriminate surveillance of every high-value transaction using digital assets. Extending §6050I to digital assets would not meaningfully assist the IRS's administration of the income tax. It is not "incidental" to the exercise of the taxing power, but rather a disproportionate and draconian surveillance regime derived from a constitutional provision to which it bears little relation. And in any event, Congress included no jurisdictional hook or legislative findings tethering §6050I to the taxing power (or any other power). Deficit Reduction Act of 1984, Pub. L. 98–369, 98 Stat 494; amended Pub. L. 100–690, 102 Stat 4181 (1988); Pub. L. 104–168, 110 Stat 1452 (1996). *See also United States v. Morrison*, 529 U.S. 598, 613 (2000) (a statute that "contains no jurisdictional element establishing that the federal cause of action is in pursuance of Congress' power to regulate" is likely untethered from that power).

235. Nor could the amended §6050I be justified as "necessary and proper" for executing the power to "regulate commerce … among the several states." The amended §6050I is not a regulation of primary activity at all; it is a reporting requirement. And nothing in the amended §6050I requires a nexus to interstate commerce. The terms of the requirement apply to receipts of digital assets regardless of whether they involve interstate commerce at all. Further, Congress made no findings that the §6050I reports had any connection to interstate commerce. Deficit Reduction Act of 1984, Pub. L. 98–369, 98 Stat 494; *Morrison*, 529 U.S. at 611-12; *Lopez*, 514 U.S. at 562, 612.

236. Therefore, no enumerated power authorizes the amended §6050I.

Count Five
Fifth Amendment Compelled Self-Incrimination

237. Plaintiffs hereby incorporate by reference the allegations contained in all of the previous paragraphs as if fully set forth herein.

238. The Fifth Amendment provides that "[n]o person ... shall be compelled in any criminal case to be a witness against himself." U.S. Const., amend. V. The "Fifth Amendment protects against the compelled production not just of incriminating testimony, but of any incriminating evidence." *United States v. Hubbell*, 530 U.S. 27, 49 (2000) (Thomas, J., dissenting). The 18th-century common-law privilege against self-incrimination protected against the compelled production of incriminating physical evidence such as papers and documents. *See* Morgan, *The Privilege against Self-Incrimination*, 34 Minn. L. Rev. 1, 34 (1949). Dictionaries published around the time

of the Founding included definitions of the term "witness" as a person who gives or furnishes evidence. *Hubbell*, 530 U.S. at 50 (Thomas, J., dissenting).

239. The Supreme Court used to abide by the doctrine that "compulsory production of [] private books and papers" for eventual use against the provider, even in a nominally civil proceeding, violates the Fifth Amendment. *Boyd v. United States*, 116 U.S. 616, 634-35 (1886). The Supreme Court has since rejected that position and that rejection remains binding on district and circuit courts. *Hubbell*, 530 U.S. at 34. Plaintiffs present this claim to preserve it for further review.

240. Under the original understanding of the Fifth Amendment, the amended §6050I would unconstitutionally compel the production of evidence without exception for evidence that could be self-incriminating. It would force receivers and senders to furnish documents that could be used against them, including for non-tax criminal investigations. Because the government's purported justification of the amendment concerns income-tax crimes by the participants in §6050I transactions, the reports would be used by the government in those cases in which the evidence that it compelled production of was self-incriminating.

241. The amended §6050I therefore violates the Fifth Amendment.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiffs respectfully request that the Court grant the following relief:

A. A declaration that the amended §6050I is facially unconstitutional;

B. An injunction preventing the Defendants from enforcing the amended §6050I;

C. An order awarding Plaintiffs their costs in this action, including attorneys' fees;

D. Any other relief that the Court deems just and proper.

Respectfully submitted,

s/ Jason L. Hargadon

Jason L. Hargadon
Hargadon Law Group LLC
111 Church Street, Suite 100
Lexington, Kentucky 40507
(Tele) (859) 971-0060
jhargadon@hargadonlawgroup.com

DATED: June 10, 2022

CONSOVOY MCCARTHY PLLC
Cameron T. Norris*
Jeffrey M. Harris*
Jeffrey S. Hetzel*
1600 Wilson Boulevard, Suite 700
Arlington, VA 22209
Telephone: 703.243.9423

J. Abraham Sutherland*
106 Connally Street
Black Mountain, NC 28711
Telephone: 805.689.4577

Attorneys for Plaintiffs

* *Pro hac vice* applications forthcoming.