IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

Dan Carman, et al.,

Plaintiffs,

v.

Scott Bessent, et al.,

Defendants.

Case No. 5:22-cv-149-KKC

Judge Karen K. Caldwell

Magistrate Judge Edward B. Atkins

BRIEF OF PARADIGM OPERATIONS LP AS AMICUS CURIAE IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

INTEREST OF AMICUS CURIAE

Paradigm Operations LP ("Paradigm") is a U.S.-based, frontier-technology investment firm that backs entrepreneurs building in crypto, AI, robotics, and across new frontiers from the earliest stages. Among Paradigm's investments are innovative blockchain companies and protocols offering peer-to-peer software that allows users to transact without traditional financial intermediaries.

Paradigm has a significant interest in ensuring that cryptocurrency developers, businesses, and users operate under clear rules protecting innovation, privacy, and growth in the U.S. financial system. Paradigm also has a strong interest in ensuring that constitutional protections keep pace with blockchain technology. This lawsuit implicates both interests. Section 6050I requires participants in covered cryptocurrency transactions to collect and disclose identifying information that they otherwise need not share. Once a digital, blockchain address is linked to an identified, real-world person, blockchain analysis can connect that person to other transactions and reveal sensitive financial and associational information about the person. Governments can also use (and share) the resulting § 6050I returns for criminal, regulatory, intelligence, and other investigations. Paradigm has vast practical experience with cryptocurrency technologies and the developers, businesses, and users who rely on them.

Paradigm thus offers a perspective on the privacy and constitutional consequences of § 6050I that extends beyond the parties' interests.[1]

[1] Undersigned counsel for amicus curiae certifies that: (1) no party's counsel authored this brief in whole or in part; (2) no party or party's counsel contributed money intended to fund the preparation or submission of this brief; and (3) no person other than amicus curiae, its members, or its counsel contributed money intended to fund the preparation or submission of this brief.

TABLE OF CONTENTS

Interest of Amicus Curiae ii

Introduction & Summary of Argument 1

Argument 5

I. Section 6050I ignores key differences between cash and crypto. 5

II. The government conducts a search, thus implicating the Fourth Amendment, when it "accesses" § 6050I crypto returns. 11

A. Section 6050I conscripts reporters to collect information for the government. 11

B. Payors and reporters have both a reasonable expectation of privacy and a property interest in this information. 13

C. Under *Chatrie*, a search of this protected information occurs when the government demands and gains "access" to it. 17

III. The searches that § 6050I authorizes violate the Fourth Amendment. 21

A. Because the government conducts a search when it accesses this information, it must obtain a warrant. 21

B. Because the searches implicate First Amendment activity, the Fourth Amendment applies with "scrupulous exactitude." 25

C. Section 6050I's vagueness compounds its unreasonableness. 27

Conclusion 29

INTRODUCTION & SUMMARY OF ARGUMENT

Decades ago, Congress designed a detailed reporting regime requiring "returns" for transactions exceeding $10,000 in physical cash. § 6050I.[2] Congress amended the regime in 2021 such that it now sweeps in "digital asset[s]" like cryptocurrency ("crypto"). *Id.* Those amendments have drastic consequences for crypto users—both those who wish to transmit crypto to others ("payors"), and their counterparties ("reporters"), who now must file detailed returns describing certain crypto transactions. *See id.* The amendments ignore fundamental differences between cash and crypto, and they both implicate and violate the Fourth Amendment's core protections against unreasonable searches.

By treating crypto like cash, § 6050I ignores three key differences that distinguish the two. First, unlike cash, transactions involving crypto occur on a public "blockchain" and necessarily create new information that becomes part of a payor's permanent, searchable transaction history. Thus, although a cash "return" reveals only a single exchange (or series of related exchanges) between two parties, a crypto return can allow the government to connect payors and reporters to other past *and future* transactions with anyone, dramatically increasing

[2] Unless otherwise noted, this brief's statutory citations refer to Title 26 of the U.S. Code.

the threat to personal and community privacy. Second, crypto transactions allow users to transact without revealing information linked to their real-world identities, whereas cash transactions typically reveal at least a person's face. Section 6050I overrides that privacy-enhancing feature by requiring reporters to demand payors' identities. Third, crypto transactions do not always resemble a bilateral transfer of physical cash. For example, crypto transactions can involve "smart contracts" that make payments automatically, thus complicating who received crypto from whom, when receipt occurs, and which transactions are related. These differences affect the breadth of information § 6050I forces reporters to collect and the much larger set of information that a crypto return can expose.

Section 6050I's compelled collection and disclosure of information involving crypto transactions is a search that implicates the Fourth Amendment. The statute conscripts reporters to act on the government's behalf and under threat of severe civil and criminal penalties—dictating what information payors must submit and what information reporters must collect and transmit to the government. But payors have protected privacy and property interests in the otherwise-private link between their real-world identities and their crypto transactions. A search occurs when the government "invade[s] [that protected] expectation . . . [by] acquir[ing]

that information." *Chatrie v. United States*, 146 S. Ct. 2193, 2206 (2026). The government's later ability to analyze, link, and share § 6050I returns with others magnifies the Fourth Amendment concerns, but a search occurs no matter how the government may later use the information it collects. The third-party doctrine does not undermine the existence of a search, because the link between payors and their broader transaction history is revealed only because § 6050I compels it.

These searches are unconstitutional because § 6050I now supplies none of the safeguards that the Fourth Amendment requires. The government obtains the information without a warrant, and with no probable cause, no individualized suspicion, no particularity, and no prior review by a judge. The government cannot override those constitutional safeguards by appealing to policy interests, general reasonableness, or its ability to pass legislation. Instead, the government has the burden to show that a recognized exception to the Fourth Amendment's warrant requirement justifies the searches that § 6050I authorizes. It cannot meet that burden. The constitutional analysis for traditional returns involving physical cash does not extend to crypto, because crypto returns expose a qualitatively different body of information, including information that allows the government

to link payors to past and future transactions. Nor does any categorical Fourth Amendment exception validate this warrantless regime.

Two further features of § 6050I make that Fourth Amendment violation still more apparent. First, § 6050I can expose political, religious, charitable, and other expressive associations that implicate First Amendment protections. As a result, courts must apply the Fourth Amendment's warrant requirement and other safeguards with "'scrupulous exactitude.'" *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Second, § 6050I imposes inevitably vague requirements for crypto transactions. That's because these requirements were developed for cash, which is fundamentally different from crypto. These differences, in turn, mean that § 6050I's cash-focused requirements create unavoidable uncertainty for crypto users and transactions.

Section 6050I thus creates a warrantless, suspicionless, and poorly bounded search regime for identity-linked information involving crypto transactions. And as Plaintiffs have emphasized, their facial challenge implicates only § 6050I returns for crypto—not cash. Because crypto returns expose a qualitatively different body of information, resolving this challenge need not call cash reporting into question.

The Court should grant Plaintiffs' motion for summary judgment.

ARGUMENT

I. Section 6050I ignores key differences between cash and crypto.

Section 6050I treats crypto like cash. This is a "false equivalency."[3] Cash is tangible and carries no transaction history. By contrast, crypto is digital and transferred in transactions recorded on a public blockchain.[4] Three resulting differences are especially relevant here. First, identifying one crypto transaction can expose a user's broader financial activity—both past *and* future. Cash transactions cannot. Second, a crypto transaction does not necessarily reveal a payor's real-world identity. But cash transactions ordinarily put the payor and reporter face to face. Third, crypto transactions need not take the simple, bilateral form that § 6050I assumes when it refers to one person "receiv[ing]" cash "from" another person. § 6050I(b)(2)(A). Those differences affect what § 6050I demands of crypto users—and what information a § 6050I return reveals to the government.

---

[3] *See* Dylan Yaga et al., Nat'l Inst. of Standards & Tech., NISTIR 8202, *Blockchain Technology Overview* at 1-3 (2018), https://perma.cc/ZF7Q-4EVL. Of course, § 6050I's definition of "cash" now includes any "digital asset," and therefore includes crypto. § 6050I(d)(3). This brief thus uses "cash" in the ordinary sense of that word, not in any sense that treats crypto as a subset of cash.

[4] Jillian Mascelli, *Data Privacy for Digital Asset Systems*, Fin. & Econ. Discussion Series 2023-059, at 6-10 (Bd. of Governors of the Fed. Rsrv. Sys. 2023), https://perma.cc/RKW2-DS9U.

Congress designed § 6050I around physical cash decades ago. *See* MSJ at 2-6.[5] It requires a reporter—that is, a person engaged in a trade or business who receives more than $10,000 in "cash" in one transaction, or two or more related transactions—to report those transaction(s) to the government. § 6050I(a)–(b). The reporter must obtain the payor's name, address, and taxpayer-identification number, describe the transaction, and file and retain a return describing that information. § 6050I(a)(2); *see* 26 C.F.R. § 1.6050I-1(e).[6] All these requirements reflect cash's inherent physicality. Cash changes hands through possession, often in a face-to-face transaction where the reporter can identify the payor. Once the bills are exchanged, the cash itself retains no record of who previously possessed it, what they bought, or where the currency may go next. *See* Mascelli, *Data Privacy* at 6-7. Congress nevertheless amended § 6050I in 2021 to define "cash" to include "any digital asset," while leaving this cash-based reporting framework in place. 26 U.S.C. § 6050I(d)(3); *see Carman v. Yellen*, 112 F.4th 386, 391-96 (6th Cir. 2024).

[5] Citations in this format refer to the memorandum in support of Plaintiffs' motion for summary judgment ("MSJ") (Dkt. 80-1).

[6] *See* I.R.S., Form 8300, Report of Cash Payments Over $10,000 Received in a Trade or Business (rev. Dec. 2023), https://tinyurl.com/5bwpcs96 ("Form 8300").

Crypto is fundamentally different. A blockchain is a digital ledger maintained by a disaggregated network, not a central bank or other intermediary. Users control crypto through digital keys and authorize transfers by digitally authenticating transactions. Network users then validate those transactions and record them on a shared ledger. *See* Yaga, *Blockchain Technology Overview* at 1-3; *Carman*, 112 F.4th at 392-93. Although the ledger is public, users' identities usually are not. Instead, the ledger records pseudonymous digital "addresses," together with amount and transaction information, without itself connecting those addresses to names or other identifying information. *See Carman*, 112 F.4th at 392-93.[7] The differences between cash and crypto are relevant to how the Court should analyze the Plaintiffs' facial challenge to § 6050I in at least three respects.

First, unlike cash, a crypto transaction necessarily creates new information that sits within a broader transaction history. To see the difference, consider a cash payment from Jones to Smith. Neither the transaction itself nor Smith's § 6050I reporting reveals what Jones bought last week, whom Jones paid last year, or information connecting this transaction to others Jones may make next year. But if

[7] *See also* Yana Kogan, Note, *The Privacy Limits of Transacting in Bitcoin*, 2022 Colum. Bus. L. Rev. 506, 513-20 (2022).

Jones pays using crypto, the transaction itself becomes part of Jones's permanent, searchable transaction history. *See* Yaga, *Blockchain Technology Overview* at 2-3, 13-17. That history is public yet reveals zero *identities*, because the transaction occurs via pseudonymous addresses. If identities and addresses are later linked, anyone can search for other transactions involving the payor—and anyone can also use readily available analytical tools "to deduce a user's other addresses and transactions." *Carman*, 112 F.4th at 393.[8] Because of the inherent differences between the two, § 6050I supplies that missing link for crypto, but not for cash.

Second, crypto transactions themselves "do not require the disclosure of information about a [payor]'s identity" to a reporter.[9] Yet § 6050I takes for granted that the reporter can identify who a payment is "from." § 6050I(b)(2)(A). That is a sensible assumption for cash, where transactions usually occur between two people in a physical exchange. It is not a sensible assumption for crypto, where

[8] *See United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020) ("Federal agents used an outside service to analyze the publicly viewable Bitcoin blockchain and identify a cluster of Bitcoin addresses controlled by the Website."); Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, in Proceedings of the 2013 Internet Measurement Conference 127, 127 (2013), https://perma.cc/XE6G-UYKG (discussing "heuristic clustering," a method that can "group Bitcoin wallets based on evidence of shared authority").

[9] U.S. Gov't Accountability Off., GAO-23-105346, *Blockchain in Finance* at 7 (2023), https://perma.cc/LQZ5-C4KQ.

transactions flow through the internet. Even so, § 6050I requires the reporter to identify the "person from whom" the assets were received, § 6050I(b)(2)(A), and to demand the payor's personal, identifying information, *id.* A recurring crypto address can suggest a repeat payor, much as a familiar face can reveal a repeat cash customer. But a payor can transact through different addresses. *See Carman*, 112 F.4th at 393. Section 6050I thus pressures crypto reporters to obtain and retain identifying information from *all* payors just in case any one payor's related transactions later aggregate above $10,000. § 6050I(a); *see* Form 8300, Part I. For cash, reporters ordinarily must obtain that personal information only from payors who actually cross the threshold, because in the face-to-face exchanges for which § 6050I was designed, reporters can recognize repeat payors.

Third, not all crypto transactions have the simple, bilateral structure that § 6050I assumes. Section 6050I and its implementing rules contemplate a familiar transaction: Jones hands cash to Smith, who "receives" it "from" Jones and can recognize whether later payments are "related." 26 U.S.C. § 6050I(a)–(b); 26 C.F.R. § 1.6050I-1(b), (c)(7)(ii). Crypto transactions often do not share these attributes. A single crypto transaction, for example, may combine the transaction itself plus

separate "rewards" and "transaction fees" denominated in the same asset.[10] Other transactions involve "smart contracts," which are programs deployed on a blockchain that execute according to predefined rules and can "automatically send funds to other accounts." Yaga, *Blockchain Technology Overview* at 32. All these complicate determinations about who a payment is "from." Further, blockchain networks validate and store transactions across many computers instead of just a single physical place, thus complicating § 6050I's exception for an "entire transaction" that "occurs outside the United States." 26 U.S.C. § 6050I(c)(2). Here again, physical cash is highly dissimilar. Physical currency passes from one person to another, does not rely on transaction fees or rewards, plays no role in smart contracts, and always occupies a definite, physical location at a given time.

These differences show why applying § 6050I to crypto does far more than just extend an old statute to a new method of payment. In short, because a § 6050I return for crypto can connect a real-world identity to a searchable, public transaction history, the Fourth Amendment consequences of compelling that return are vastly different from those involving § 6050I returns for cash.

[10] Paul Tierno, Cong. Rsch. Serv., R47425, *Cryptocurrency: Selected Policy Issues* at 8 (2025), https://perma.cc/3CEQ-83Z9.

II. The government conducts a search, thus implicating the Fourth Amendment, when it "accesses" § 6050I crypto returns.

By requiring reporters to collect and share the information from § 6050I, the government conducts a Fourth Amendment search. The forced collection is government action (Part II.A), any information so collected is protected under the Fourth Amendment (Part II.B), and searches of both the payor and the reporter occur when the government first acquires this information, notwithstanding the government's later intended use cases or the third-party doctrine (Part II.C).

A. Section 6050I conscripts reporters to collect information for the government.

The intrusive collection that § 6050I compels is government action and "trigger[s]" Fourth Amendment protections. *United States v. Miller*, 982 F.3d 412, 422 (6th Cir. 2020). "Although the Fourth Amendment does not apply to a search . . . effected by a private party *on his own initiative*, [it] protects against such intrusions if the private party acted as an instrument or agent of the Government." *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989) (emphasis added). The "'compulsion'" that § 6050I imposes leaves no room for the government to sidestep the Fourth Amendment here. *Miller*, 982 F.3d at 422 (citation omitted).

Section 6050I directs every material step of the data collection that feeds into a § 6050I return. It requires a reporter to obtain the payor's name, address, and

taxpayer-identification number; combine that information with the amount, date, and nature of the transaction; and then submit a return to the government. § 6050I(a)–(b). The implementing regulations add more: a reporter must "verify" the payor's identity, file the return within fifteen days, and retain a copy for five years. 26 C.F.R. § 1.6050I-1(e)(1)–(3). The reporter must also attest to the return under penalty of perjury, 26 U.S.C. § 6065, and civil and criminal penalties compel reporters to comply, *id.* §§ 6721, 7203. Absent § 6050I's application to crypto, reporters would do none of this on their "own initiative." *Skinner*, 489 U.S. at 614.

Reporters' status as private individuals does not weaken the government action at issue. For example, the Sixth Circuit treated an apartment manager's search as attributable to the government when officers prompted the search and the manager, "independent of his interaction with the officers, had no reason or duty" to undertake it. *United States v. Hardin*, 539 F.3d 404, 420 (6th Cir. 2008). Similarly, *Skinner* recognized government action under regulations that merely authorized private testing, because the government "did more than adopt a passive position" and displayed "encouragement, endorsement, and participation." 489 U.S. at 615-16. Section 6050I goes further, requiring payors to comply with the demand, requiring data collection, prescribing how the data can

be shared, and punishing payors and reporters for noncompliance. *See* § 6050I(f). This more than "suffice[s] to implicate the Fourth Amendment." *Id.* at 616.

B. Payors and reporters have both a reasonable expectation of privacy and a property interest in this information.

Crypto users have a reasonable "'expectation[] of privacy'" in the identity-linked transaction information that § 6050I compels reporters to collect and share with the government. *Chatrie*, 146 S. Ct. at 2205-06 (citation omitted). An expectation is protected when an individual "'seeks to preserve something as private'" and that expectation is "'one that society is prepared to recognize as reasonable.'" *Id.* at 2206 (citation omitted). Both crypto payors and crypto reporters readily satisfy each element of this test.

First, both payors and reporters in fact seek to preserve their identity-linked transaction information as private. The Sixth Circuit has already observed that these very Plaintiffs "enjoy the privacy and anonymity that cryptocurrency transactions provide." *Carman*, 112 F.4th at 391. Empirical research shows the same. In one peer-reviewed study, 70.69% of survey respondents rated transaction

anonymity "extremely" or "very" important for crypto transactions.[11] As some respondents explained: "*I expect no one realizes my identity although everyone can see the transaction* on the blockchain" and "It's completely a private thing."[12]

Courts, too, have recognized that "transactions through decentralized, peer-to-peer transactions . . . 'maintain [the] high level of privacy' associated with the blockchain." *Harper v. Werfel*, 118 F.4th 100, 110 (1st Cir. 2024) (citation omitted). And although some courts have held that there is no "privacy interest" in information *already* present on a blockchain, *Gratkowski*, 964 F.3d at 312, even those cases say nothing about the *separate* information that § 6050I compels—because none of that information resides on a blockchain. *See supra* p.7. Thus, "[i]n all, a sophisticated blockchain user can *reasonably expect not to be identified* absent highly intricate efforts by an unusually sophisticated attacker or spy."[13]

---

[11] Simin Ghesmati et al., *User-Perceived Privacy in Blockchain*, in *Financial Cryptography and Data Security* 164, 167 (2022) (for a non-paywalled version of this paper, see here at page 4: https://perma.cc/VX4E-VUM5).

[12] *Id.* (emphasis in original; alteration adopted).

[13] Paul Belonick, *Transparency Is the New Privacy: Blockchain's Challenge for the Fourth Amendment*, 23 Stan. Tech. L. Rev. 114, 135 (2020), https://perma.cc/M45E-ETDY (emphasis added). Of course, as Plaintiffs have explained, the information supplying an identity *linkage* is not all that carries a privacy interest. *See* MSJ at 19. Names, addresses, and especially social security numbers all involve expectations of privacy even apart from the linkages they allow to transaction histories. *See id.*

Second, the expectation is reasonable. To begin, Executive Order 14178 declares that crypto plays a "crucial role in innovation and economic development" and makes it federal policy to protect access to public blockchains, including the ability "to transact with other persons without unlawful censorship[] and to maintain self-custody of digital assets."[14] The President's Working Group on Digital Asset Markets likewise "supports civil liberties protections surrounding privacy and the ability of individuals to privately transact on public blockchains," because "privacy is . . . critical to enabling the increased use of digital assets for payments as individuals may not want to publicly disclose every purchase of goods or services or allow salary payments or other private transactions to be tracked."[15] Even a Treasury report focused on combating illicit uses recognizes that "lawful users" rely on blockchains to "enable financial privacy" and "to protect sensitive information on personal wealth, business

[14] *Strengthening American Leadership in Digital Financial Technology*, Exec. Order No. 14178, 90 Fed. Reg. 8647, 8647 (Jan. 23, 2025), https://perma.cc/3AD9-58PW.

[15] President's Working Group on Digital Asset Markets, *Strengthening American Leadership in Digital Financial Technology* at 111 (2025), https://perma.cc/UF3E-RUHR.

payments, or charitable donations."[16] These official judgments are strong evidence that separating one's identity from lawful blockchain activity serves reasonable and publicly accepted interests in financial privacy for crypto transactions.

Separately, payors and reporters also have a property interest in their identity-linked transaction information. The Fourth Amendment's property-based protections are independent of and "do not rise or fall with the *Katz* formulation." *United States v. Jones*, 565 U.S. 400, 406 (2012); *see id.* (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) for the "'reasonable expectation of privacy'" test). Applying that rule to the digital sphere, Justice Gorsuch has explained that property interests protect an individual's rights to "enjoy, manage, alter, dispose, and exclude others from what [in *Chatrie*] amounted to an electronic diary or map of his travels." *Chatrie*, 146 S. Ct. at 2221 (Gorsuch, J., concurring in the judgment). Crypto users exercise all those core rights over the private link between themselves and their blockchain activity. They create and control their blockchain addresses, decide whether to reveal those addresses, and ordinarily may exclude others from viewing the information that can connect those addresses to their identities. *See*

[16] U.S. Dep't of the Treasury, *Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets* at 8 (Mar. 2026), https://perma.cc/2H9D-LG4A.

Carman, 112 F.4th at 392-93. Intrusions on those rights can reveal a "map" of a person's transaction history. *Chatrie*, 146 S. Ct. at 2221 (Gorsuch, J., concurring in the judgment). The Sixth Circuit has likewise recognized that "the protection of private property extended to letters, papers, and documents," and that opening digital files may constitute a "trespass to chattels" and thus "an illegal search." *Miller*, 982 F.3d at 432-33 (citations and internal quotation marks omitted). Section 6050I strips crypto users of that control by forcing them to surrender their private information and forcing reporters to turn that information over to the government.

C. Under *Chatrie*, a search of this protected information occurs when the government demands and gains "access" to it.

The government conducts a search when it "invade[s] th[e] expectation" of privacy that payors have in their identity-linking information "and thus conduct[s] a search[] when [it] *acquire*[*s*] that information." *Chatrie*, 146 S. Ct. at 2206 (emphasis added). *Chatrie* itself began with the rule that "governmental 'intrusion into [a] private sphere generally qualifies as a search.'" *Id.* at 2205 (quoting *Carpenter v. United States*, 585 U.S. 296, 304 (2018)).[17] In other words, a

[17] *Chatrie* involved a three-stage "geofence" warrant issued to Google after a bank robbery. 146 S. Ct. at 2199. Google first produced anonymized location data for cell phones that were near the crime scene when the crime occurred, then supplied broader (but still anonymized) records for a narrowed group, then identified a small group of users. *Id.* at 2202. The Supreme Court held that law

search occurs when the government demands and then gains "*access to* a category of information otherwise unknowable." *Carpenter*, 585 U.S. at 312 (emphasis added). That is, the acquisition itself is a search. By requiring reporters to collect and reveal identities, § 6050I effects such an acquisition. That conclusion accords with *Chatrie*'s broader command that "no government official should have free access to the most closely kept aspects of [Americans'] lives." 146 S. Ct. at 2205.

The Sixth Circuit uses the same rule. For example, a search occurs when the government "attempt[s] to find something or to *obtain* information." *Kanuszewski v. Michigan Dep't of Health & Human Servs.*, 141 F.4th 796, 809 (6th Cir. 2025) (emphasis added) (quoting *Jones*, 565 U.S. at 408 n.5). Similarly, "if government agents compel an [internet service provider] to *surrender* the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search." *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (emphasis added). Thus, the conduct at issue in *Kanuszewski* did not amount to a search only because it failed to actually "reveal any information to the government." 141 F.4th at 809. Section 6050I returns are the polar opposite because they *do* reveal

---

enforcement had "conduct[ed] a search under the Fourth Amendment" when they acquired the protected location records and remanded for the Fourth Circuit to decide issues involving probable cause and particularity. *Id.* at 2215-16.

protected, personally identifying information to the government. *See supra* p.8. That is the precise Fourth Amendment theory that the Sixth Circuit held is ripe in this case: that "the initial information transmitted to the government is entitled to Fourth Amendment protection" and that "even the mere disclosure of a specific transaction to the government implicates" the Fourth Amendment "regardless of any further steps taken by the government." *Carman*, 112 F.4th at 405.

The government's later ability to *use* the information—that is, to analyze, link, and share the returns—is still relevant here, but because it exacerbates an existing constitutional violation, not because it creates one. As this Court has indicated, those later uses affect "the extent of the burden on [the Plaintiffs'] constitutional rights, and whether that burden is appropriately tailored to the government's interests." Order on Motion to Compel at 9 (Dkt. 67). But those later uses are irrelevant to determining whether a search occurred. "Whether something is a search does not depend on what it finds." *Chatrie*, 146 S. Ct. at 2212. That's because the initial access "must be either a search or not regardless" of the information it yields. *Id.* If an investigation's results do not bear on whether a search occurred, how those results are later used also cannot control the determination of whether a search occurred. Nor does the specific content or later

usage of § 6050I returns change the rule. "Where the Fourth Amendment applies, it applies regardless of 'the quality or quantity of information' the government obtains." *Id.* at 2210 (quoting *Kyllo v. United States*, 533 U.S. 27, 37 (2001)).[18]

Finally, the third-party doctrine does not reduce § 6050I returns to anything less than a Fourth Amendment search. That doctrine arose from information "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," *United States v. Miller*, 425 U.S. 435, 442 (1976), and telephone numbers "voluntarily conveyed" to a phone company to connect calls, *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (citation omitted). Voluntariness is absent here because § 6050I imposes civil and criminal penalties for noncompliance. *See* §§ 6721, 7203. Crypto transactions require anonymous blockchain addresses, but they do not require the personally identifying information that § 6050I compels. *See supra* p.7. Instead, this additional information is required only because of § 6050I. Further, even mere exposure to a third party does not eliminate Fourth Amendment protection. *See Chatrie*, 146 S. Ct. at 2213 ("cell phone location

[18] *See* Orin S. Kerr, *The Fourth Amendment After Chatrie* at 25 (Aug. 5, 2026) (unpublished), https://perma.cc/A5PU-LLL2 ("*Chatrie* takes the longstanding principle that the reasonableness of a search does not depend on what is found—in particular, that finding evidence doesn't make the search legal ex post—and imports it instead into *whether an act is a search at all*." (emphasis added)).

information is not truly 'shared' as one normally understands the term" because "cell phones and the services they provide are such a pervasive and insistent part of daily life" (cleaned up)). Thus, under *Chatrie* and other precedent, a search occurs when the government accesses § 6050I returns.

III. The searches that § 6050I authorizes violate the Fourth Amendment.

Section 6050I's searches violate the Fourth Amendment because they occur without the warrant that the Fourth Amendment requires, and no exception justifies them (Part III.A). These searches also implicate First Amendment associational interests and thus demand "scrupulous exactitude" (Part III.B), and § 6050I's vagueness further compounds their unreasonableness (Part III.C).

A. Because the government conducts a search when it accesses this information, it must obtain a warrant.

The Fourth Amendment's warrant requirement governs the searches that § 6050I authorizes. "'Searches conducted outside the judicial process, without prior approval by a judge or a magistrate judge, are per se unreasonable subject only to a few specifically established and well-delineated exceptions.'" *City of Los Angeles v. Patel*, 576 U.S. 409, 419 (2015) (quoting *Arizona v. Gant*, 556 U.S. 332, 338 (2009)) (cleaned up); *see Riley v. California*, 573 U.S. 373, 382 (2014) (similar). Section 6050I disregards every one of the safeguards that warrants guarantee. It requires

no probable cause, no individualized suspicion, no particularity, and no prior review by a judge. Instead, the government obtains identity-linked information whenever the reporting threshold is met. 26 U.S.C. § 6050I(a)–(b). Thus, for this collection to be lawful absent a proper Fourth Amendment warrant, "'[t]he government bears the burden of demonstrating an exception to the warrant requirement'" that justifies § 6050I. *Mockeridge v. Harvey*, 149 F.4th 826, 835 (6th Cir. 2025) (quoting *Taylor v. City of Saginaw*, 922 F.3d 328, 334 (6th Cir. 2019)). It cannot meet that burden here.

First, the government cannot replace the warrant requirement with a freestanding reasonableness inquiry. Without a warrant, "a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley*, 573 U.S. at 382. The government therefore cannot defend § 6050I merely by arguing that the information in a return is useful, or that demanding these returns serves important policy goals, or that those policy goals outweigh payors' privacy interests. Instead, because "acquir[ing]" the information is a search, the ordinary warrant rule controls unless an exception applies. *Chatrie*, 146 S. Ct. at 2206. Congress cannot create constitutional exceptions via a statute, even one that is part of the Tax Code, or by labeling the information a "return." *See Yin v. California*, 95

F.3d 864, 871 (9th Cir. 1996) ("Otherwise, Congress . . . could eliminate basic Fourth Amendment protections and effectively amend the Constitution in the process by enacting statutes authorizing particular searches . . . .").

Second, although the warrant requirements for cash returns (if any) are not at issue here, *see* MSJ at 25, the constitutionality of traditional § 6050I returns for cash does not answer whether § 6050I's separate crypto searches are lawful. *California Bankers Association v. Shultz* helps show why. *See* 416 U.S. 21, 65 (1974). There, the Supreme Court upheld domestic cash-reporting requirements against banks' Fourth Amendment challenge, emphasizing that the banks "already possesse[d] or would acquire in [their] own interest" that data. *Id.* at 67. But the Court did not reach the customers' Fourth Amendment challenge, because they lacked standing. *Id.* at 69. Standing is already present here. *Carman*, 112 F.4th at 410. Regardless, § 6050I returns for crypto involve a qualitatively different kind of search: they link a payor's identity to a blockchain history and thereby expose transactions never subject to § 6050I. *See supra* p.8. *Shultz* did not consider, much less approve, such searches.[19] So this Court can hold that the warrant requirement applies here without questioning whether it would apply to § 6050I cash returns.

[19] Indeed, the concurring Justices in *Shultz* warned that "[a] significant extension of the regulations' reporting requirements . . . would pose substantial

Third, no categorical Fourth Amendment exception justifies § 6050I's searches. For example, the administrative-search doctrine does not fit, because § 6050I applies across ordinary transactions, including peer-to-peer transactions, not within a single "'closely regulated' . . . category of businesses." *Patel*, 576 U.S. at 424 (citation omitted). Nor can the special-needs doctrine sustain § 6050I against Plaintiffs' facial challenge. That doctrine requires a need "'beyond the normal need for law enforcement.'" *Chandler v. Miller*, 520 U.S. 305, 306 (1997) (citation omitted). But § 6050I returns are expressly available for a wide variety of criminal, regulatory, intelligence, and other ordinary investigative purposes. *See* 26 U.S.C. § 6103(l)(15); 31 U.S.C. § 5311. In other words, they are part and parcel of ordinary law enforcement, not some special instance of it. And because this kind of "law enforcement involvement always serves some broader social purpose," treating it as a special need would allow "virtually any nonconsensual suspicionless search" to evade the warrant rule. *Ferguson v. City of Charleston*, 532 U.S. 67, 84 (2001).

Finally, fact-specific exceptions that may independently authorize a specific search cannot defeat this facial challenge. *See* MSJ at 17-18. *Patel* holds that "the

---

and difficult constitutional questions" because "the reports . . . touch upon intimate areas" and "[f]inancial transactions can reveal much about a person's activities, associations, and beliefs." 416 U.S. at 78-79 (Powell, J., concurring).

proper focus of the constitutional inquiry is searches that the law actually authorizes, not those for which it is irrelevant." 576 U.S. at 418. So, even if consent, exigent circumstances, or an independently issued warrant were to separately allow the government to acquire this information in some instances, § 6050I would "do no work" there, and those circumstances would "not involve actual applications of the statute." *Id.* at 419. That makes those instances irrelevant to this facial challenge. The analytical universe instead consists of searches wherein the government gains access *because* § 6050I commands disclosure.

Because the government cannot meet its burden to show that any Fourth Amendment exception justifies § 6050I, the searches that § 6050I authorizes are, as to crypto, subject to the ordinary warrant requirement. Yet § 6050I requires neither a warrant nor probable cause before the government obtains payors' protected information. These warrantless searches are per se unreasonable under the Fourth Amendment.

B. Because the searches implicate First Amendment activity, the Fourth Amendment applies with "scrupulous exactitude."

Section 6050I's indiscriminate searches implicate the First Amendment, too, because identity-linked blockchain information can expose crypto payors' and reporters' political, religious, charitable, and other protected, expressive

associations. *See supra* p.7. Plaintiffs have explained how § 6050I violates the First Amendment. *See* MSJ at 12-17. Regardless, the underlying First Amendment interest *also* requires courts to apply the Fourth Amendment's warrant requirement with "scrupulous exactitude." *Zurcher*, 436 U.S. at 564 (cleaned up).

The First Amendment protects associational privacy. *See Pleasant View Baptist Church v. Beshear*, 78 F.4th 286, 302 (6th Cir. 2023). As such, "[c]ompelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective . . . restraint on freedom of association." *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958). In particular, the First Amendment protects against compelled disclosure even to just the government itself: "It does not make a difference in these cases if there is no disclosure to the public." *Americans for Prosperity Found. v. Bonta*, 594 U.S. 595, 598 (2021). Section 6050I invades that protected interest. Therefore, as the Sixth Circuit recognized in holding that Plaintiffs' associational theory is ripe, § 6050I's disclosure regime can "directly mandate the reporting of expressive associations." *Carman*, 112 F.4th at 406.

For this Fourth Amendment facial challenge, then, the analysis requires special care, because "[w]here the materials sought to be seized *may* be protected by the First Amendment, the requirements of the Fourth Amendment must be

applied with 'scrupulous exactitude.'" *Zurcher*, 436 U.S. at 564 (quoting *Stanford*, 379 U.S. at 485) (emphasis added). Here, that means a "particularly exacting" analysis of the two Fourth Amendment requirements at issue above: whether the government's compelled acquisition of identity-linked transaction information constitutes a "search," and, if so, whether that search satisfies the warrant requirement. *Bray v. Planned Parenthood Columbia-Willamette Inc.*, 746 F.3d 229, 236 (6th Cir. 2014). Thus, any doubt about whether § 6050I's compelled access is a search should account for the associational information that a return can allow the government to uncover. *See supra* p.8. And because that access is a search, the analysis must guard against diluting the ordinary warrant requirement and against allowing the government to meet anything less than showing an exception applies. *See Zurcher*, 436 U.S. at 564.

C. Section 6050I's vagueness compounds its unreasonableness.

Because § 6050I's text sets some boundaries on the warrantless searches it authorizes, any uncertainty in those boundaries is relevant to the Fourth Amendment analysis. *Cf. Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (explaining that a search must be "carefully tailored to its justifications" and cannot become a "wide-ranging explorat[ion]"). To be sure, *Carman* held that Plaintiffs'

independent vagueness claim was not yet ripe because it depends on hypothetical applications that could be clarified in future rulemaking. 112 F.4th at 401-03. But *Carman* did not hold that § 6050I's terms are clear; it expressly acknowledged that "plaintiffs could be ultimately correct that *certain* provisions of § 6050I could be vague." *Id.* at 403. Those arguments are relevant to the "search" analysis, too, because the broader the searches that § 6050I authorizes, the starker the Fourth Amendment violation. This is not to say that § 6050I would be constitutional if it were interpreted narrowly. *See Chatrie*, 146 S. Ct. at 2210 ("Where the Fourth Amendment applies, it applies."). But it is to say that any vagueness which could expand § 6050I's boundaries thereby compounds the violation.

Section 6050I's boundaries are uncertain in several basic ways. It does not explain which crypto transfers are "related," who is the "person from whom" assets are received (*e.g.*, when a smart contract causes the transfer), or when "receipt" occurs for jointly controlled addresses. *See* 26 U.S.C. § 6050I(a), (b)(2)(A); 26 C.F.R. § 1.6050I-1(b), (c)(7)(ii), (e)(3)(ii); *Carman*, 112 F.4th at 403. No matter what those commands mean for cash, they will predictably induce crypto reporters to collect and report more information—earlier, from more crypto payors, and across more crypto transactions than a clear statute would require. As a result, § 6050I's

vagueness compounds the unreasonableness of the warrantless search regime that itself already violates the Fourth Amendment. *See Carman*, 112 F.4th at 403.

CONCLUSION

Plaintiffs' motion for summary judgment should be granted.

Dated: August 27, 2026

Respectfully submitted.

/s/ Joshua P. Morrow

Joshua P. Morrow (*pro hac vice*)
LEHOTSKY COHN LLP
7500 Rialto Blvd., Suite 1-250
Austin, TX 78735
(512) 693-8350
josh@lehotskycohn.com

Counsel for Amicus Curiae