UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES OF AMERICA, v. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, Defendants.	Case No. 24 Cr. 82 (RMB)

BRIEF OF AMICI CURIAE DEFI EDUCATION FUND AND BLOCKCHAIN ASSOCIATION IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

Cameron T. Norris*
Daniel M. Vitagliano**
Zachary P. Grouev*
Consovoy McCarthy PLLC
1600 Wilson Boulevard, Suite 700
Arlington, Virginia 22209
(703) 243-9423
dvitagliano@consovoymccarthy.com
cam@consovoymccarthy.com
zach@consovoymccarthy.com

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

**pro hac vice applications forthcoming*
*** supervised by principals of the firm admitted to practice in Virginia*

Counsel for Amicus Curiae DeFi Education Fund and Blockchain Association

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Other Authorities

Constitutional Provisions

INTEREST OF AMICI CURIAE

DeFi Education Fund ("DEF") is a nonpartisan research and advocacy group based in the United States. DEF's mission is to advocate for sound policy for decentralized finance ("DeFi"), educate lawmakers about the technical workings and benefits of DeFi, achieve regulatory clarity for the future of the global digital economy, and advocate for individual users and developers in the DeFi space. DeFi is part of the cryptocurrency ecosystem. Among other things, DEF educates the public about DeFi through op-eds, podcasts, and print media; submits amicus briefs in cases where DeFi technology is at issue; and submits public comments on proposed rulemakings that impact DeFi.

The Blockchain Association ("BA") is the leading membership organization dedicated to promoting a pro-innovation policy environment for the digital-asset economy. BA endeavors to achieve regulatory clarity and to educate policymakers, regulators, courts, and the public about how blockchain technology can create a more secure, competitive, and consumer-friendly digital marketplace. BA represents over 120 member companies reflecting the entire breadth of the blockchain industry, including software developers, infrastructure providers, exchanges, custodians, investors, and others supporting the public blockchain ecosystem.

DEF and BA have a significant interest in this case, particularly the government's assertion, contra the plain meaning of the law and FinCEN Guidance, that 18 U.S.C. §1960 does not require the government to prove that defendants exercised control over any funds. DEF has been a leading public advocate on the scope of the money-transmitting laws as they apply to software developers, organizing congressional outreach and publishing a working paper directly addressing the "control" issue. *See, e.g.*, Tuminelli, et al., *Through the Looking Glass: Conceptualizing Control and Analyzing Criminal Liability for Unlicensed Money Transmitting Businesses Under Section 1960*, Int'l Acad. of Fin. Crime Litigators Working Paper No. 3 (Dec. 2024), perma.cc/Z6JD-QSTG; DEF, et al., *Letter to the S. Comm. on Banking, S. Comm. on the Judiciary, H. Comm. on Fin. Servs., and H. Comm. on the Judiciary* (Mar. 26, 2025), perma.cc/2B8V-W4SL (*Letter to Cong. Comms.*) (letter from DEF and signed by BA and 30+ members of the cryptocurrency ecosystem raising concerns over the effort to adopt an "unprecedented and overly expansive interpretation" of §1960). And because "under [the DOJ's] interpretation, essentially every blockchain developer could be prosecuted as a criminal," *Letter to Cong. Comms.* at 1, BA's members will be subject to serious regulatory chill if that interpretation is upheld. More broadly, DEF and BA have an interest in holding the government to its word, vindicating constitutional principles of fair notice and due process, and ensuring regulation of the cryptocurrency ecosystem that accurately reflects the realities of the technology at issue.

INTRODUCTION

The government's theory underlying Count II, which alleges that the defendants conspired to operate an unlicensed money transmitting business, rests on a novel and fatally flawed interpretation of the criminal code. *See* Indictment (Dkt. 4) at 17. To engage in "money transmitting" under 18 U.S.C. §1960(b)(2), a defendant must have been "transferring funds on behalf of the public." Although it may seem obvious, in order to transfer funds *on behalf of* a person, a defendant must first take custody of the funds and control them. But the Justice Department's theory here makes federal criminals out of software developers who do not take custody and do not exercise control of any third party's funds. These software developers simply created technology that allowed *other* people to transfer their *own* funds peer-to-peer. The government's novel theory runs counter to the plain meaning of the statute, to longstanding guidance from the Financial Crimes Enforcement Network ("FinCEN"), and to virtually every canon of construction that governs criminal cases. This Court should reject it and dismiss Count II.

SUMMARY OF ARGUMENT

Americans should have fair notice of what a law prohibits before the government enforces it against them. *See, e.g.*, U.S. Const. Art. I, §9, cl. 3 (prohibition on ex post facto laws); *Bittner v. United*

States, 598 U.S. 85, 102 (2023) (Op. of Gorsuch, J.) (reiterating the "Due Process Clause's promise" of "'fair warning'"). The government cannot silently adopt a broader reading of a criminal statute that would abrogate its own longstanding guidance, then retroactively prosecute defendants who reasonably relied on the government's prior position. *E.g.*, *Bittner*, 598 U.S. at 102-03 (Op. of Gorsuch, J.). But that is exactly what happened when the Justice Department indicted the developers of Samourai Wallet, a non-custodial software tool that allowed cryptocurrency owners to make their own peer-to-peer transactions.

Count II of the indictment relies on a novel and ill-considered legal theory that the Justice Department knew contradicts FinCEN's interpretation. *See Brady* Letter (Dkt. 86) at 7. Since 2019, FinCEN consistently told the public that, regardless of the underlying technology, an entity is not a money transmitter unless it has "total independent control over the value" being moved. *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* 15, FIN-2019-G001 (May 9, 2019), perma.cc/8M5Z-QY2D ("*Application to Certain Business Models Involving Convertible Virtual Currencies*"). Thus, "suppliers of tools (communications, hardware, or software) that may be utilized in money transmission, like anonymizing software, are … *not money transmission*." *Id.* at 20 (emphasis added). Software developers have relied on that guidance for the past six years.

But despite being warned by the agency charged with interpreting money-transmitting provisions that a "no-control-required" theory would be seriously flawed, the Justice Department did not change course. Instead, it charged Count II based on an all-consuming interpretation of §1960 that rejects FinCEN's control requirement and threatens to criminalize developers of a neutral technology used by individual users to transfer their own funds. *See* Resp. to Mot. to Dismiss (Dkt. 53) at 24, *United States v. Storm*, No. 23 Cr. 430 (KPF) (S.D.N.Y. Apr. 26, 2024) (*Storm* MTD Resp.) ("Section 1960 Does Not Require the Business to Have Control of the Funds").

That interpretation should be rejected. The plain meaning of the statute does not support the government's reading. Section 1960(b)(2) requires that funds be "transferr[ed] … *on behalf of* the public," which means the defendant must receive and control funds before he can "transmi[t]" them. (emphasis added.) Circuit precedent, dictionary definitions, and simple common sense all confirm the point. And this threshold element applies to all three of §1960(b)(1)'s definitions of the related term "unlicensed money transmitting business." Even if §1960 could be interpreted to lack a control requirement, prosecuting the defendants for following FinCEN's Guidance would violate constitutional principles of due process and fair notice. The shockwaves that the government's change in position has sent through the cryptocurrency world proves the point. Finally, adopting the government's interpretation would offend the rule of lenity, the major questions doctrine, and the separation of powers principles underlying those canons.

The Justice Department's theory of §1960 would twist a decades-old statute to criminalize broad swaths of otherwise lawful conduct and stifle a frontier industry that Congress could not have imagined itself to be regulating. For all these reasons, Count II should be dismissed.

ARGUMENT

When the text of a statute excludes conduct as not criminal, the American people should be able to rely on that plain meaning. *E.g.*, *Bittner*, 598 U.S. at 102 (Op. of Gorsuch, J.). And when the agency charged with administering a statute explains its position on government letterhead, the public should be able to take the government at its word. *FDA v. Wages and White Lions Invs.*, 145 S. Ct. 898, 917 (2025). If the government changes its mind, it can propose a rule to that effect using the procedures that Congress prescribed. *See* 5 U.S.C. §553. That way, adversely affected parties can participate in the rulemaking process and seek pre-enforcement review. §§702, 706. And if the government really wishes for an old statute to read differently today, it can always take that request to Congress. Channeling changes through the democratically accountable legislature ensures that

Americans receive fair notice. *West Virginia v. EPA*, 597 U.S. 697, 737-38 (2022) (Gorsuch, J., concurring). Count II, however, shortcuts these established procedures, contradicts the text of §1960, undermines due process and fair notice, stifles an important segment of the economy, and flouts the rule of lenity and the major-questions doctrine.

I. Count II is inconsistent with the statutory text.

Count II charges conduct—the development of non-custodial software to enable peer-to-peer financial transactions—that is outside the scope of the money-transmitting laws. This Court should dismiss it.

To convict under §1960(b)(1)(B) or (C), the government must prove that the defendant "transferr[ed] funds on behalf of the public." 18 U.S.C. §1960(b)(2). To convict under (B), the government must prove that the defendant "accept[ed]," "transmitt[ed]," or "engage[d] as a business in the transmission" of funds. 31 U.S.C. §§5330(d)(2), 5330(d)(1)(A); *accord* 31 C.F.R. §1010.100(ff)(5) (incorporated by §1960(b)(1)(B) via 31 U.S.C. §5330(d)(1)(B) and 31 U.S.C. §5313). To convict under (C), the government can prove that the defendant operated a money transmitting business that "involve[d] the transportation or transmission of funds" that the defendant knew were connected to crime. But under either theory, it must prove that the defendant "transferr[ed] funds on behalf of the public." 18 U.S.C. §1960(b)(2). To interpret this phrase, courts determine "'the statute's plain meaning.'" *United States v. Rowland*, 826 F.3d 100, 108 (2d Cir. 2016). And because the statutory terms are undefined, the Court "consider[s] 'the ordinary, common-sense meaning of the words.'" *Id.*

Under the ordinary, common-sense understanding of §1960(b)(2), a defendant cannot "transfer" funds "*on behalf of*" another person if he does not have possession and control over the funds to begin with. Someone does not "transfer," "transmit," or "accept" an object when he creates a neutral tool that other people use to move the object. For example, if someone drives his money from one place to another using a Ford Bronco, *Ford* does not "transfer," "transmit," or "accept" the money. Nor does Ford make the transfer on behalf of the driver. Likewise, the paper company that prints security envelopes so that others may safely mail checks does not "transfer," "transmit," or "accept" the checks. Nor does the paper company make the transfer on behalf of the sender. But under the Justice Department's sweeping interpretation of §1960, "there is no requirement that the transferer exercise control over the funds being transferred." *Storm* MTD Resp. at 24. The government's position here is that §1960(b)(2)'s reference to "transferring funds on behalf of the public" requires no more control than "a USB cable [that] transfers data from one device to another" or "a frying pan [that] transfers heat from a stove to the contents of the pan." *Id.* That means Ford, the paper company, and the manufacturers of a host of other neutral tools that a third-party might later use to move value are all money transmitters—an absurd proposition that Congress has never endorsed.

Second Circuit precedent supports the defendants' reading. Consider *United States v. Velastegui*, where the Court explained that "[a] money transmitting business *receives money from a customer* and then, for a fee paid by the customer, *transmits that money to a recipient* in a place that the customer designates." 199 F.3d 590, 592 (2d Cir. 1999) (emphasis added); *see also United States v. Banki*, 685 F.3d 99, 114 (2d Cir. 2012) (favorably citing *Velastegui*'s definition); *United States v. Singh*, 995 F.3d 1069, 1077 (9th Cir. 2021) (same). Or take *United States v. Bah*, where the Second Circuit explained that "[s]o long as [the defendant] (or his agents) *maintained possession of any payments*, the movement of … money across state lines would not itself violate the statute, because Section 1960 prohibits the '*transfer*' of money, not the transportation of money by an individual." 574 F.3d 106, 114 n.6 (2d Cir. 2009) (emphasis added). In other words, mere receipt of funds is not enough. *Bah* holds that, in addition to gaining possession and control, the defendant must relinquish control of the funds to complete a §1960 offense. *See id.* at 114. If taking possession of a payment and transporting it across state lines is insufficient to trigger the statute under *Bah*, it is difficult to see how developing a piece of software that never takes possession of anything could somehow turn out differently. *See* Tuminelli, et al., *Through the Looking Glass* at 12-17 (discussing *Bah* and related cases).

This Court often relies on dictionary definitions to help ascertain plain meaning, *see, e.g.*, *United States v. Broxmeyer*, 616 F.3d 120, 125 (2d Cir. 2010); *United States v. Reynoso*, 239 F.3d 143, 146-48 (2d Cir. 2000), and those definitions further prove that §1960(b)(2) refers to a subject who has possession or control over the funds being moved. To "transfer" means "to convey or remove from one place or one person to another; to pass or hand over from one to another, esp. to change over the possession or control of." *Transfer*, Black's Law Dictionary (10th ed. 2014). The noun version, *see* 31 C.F.R. §1010.100(ff)(5), means "[a]ny mode of disposing of or parting with an asset or an interest in an asset," and "every method—direct or indirect, absolute or conditional, voluntary or involuntary—of disposing of or parting with property or with an interest in property," *Transfer*, Black's Law Dictionary (10th ed. 2014). To "transmit," 31 U.S.C. §5330(d)(1), (d)(2); 31 C.F.R. §1010.100(ff)(5), means "to send or transfer (a thing) from one person or place to another," *Transmit*, Black's Law Dictionary (10th ed. 2014). And to "accept," 31 U.S.C. §5330(d)(1), (d)(2); 31 C.F.R. §1010.100(ff)(5), means "to receive (something offered) willingly," *Accept*, Merriam-Webster Online (2025). None of these actions can be taken without possession and control. Section 1960(b)(2)'s requirement that a transfer be "on behalf of" someone else further underscores the point. Providing the technology for a person to make their own transfer, without controlling the funds at issue, is not making that transfer "on behalf of" someone else.

II. Count II violates due process and fair notice.

Even if §1960 could support the government's novel interpretation, the Court should dismiss Count II. The money-transmitting charges would impose criminal liability for acts taken in reasonable reliance on FinCEN's longstanding interpretation of a statute that FinCEN is charged with administering. And under a decade of FinCEN Guidance, the defendants' conduct—developing non-custodial software with privacy-enhancing features—was well outside the scope of the money-transmitting laws. When the government undertakes an unexpected, unexplained change in position and then moves to punish those who fail to read its mind beforehand, the resulting enforcement violates due process and cannot proceed.

A. FinCEN established that non-custodial software developers are not money transmitters based on their lack of control over user funds.

In a series of publications beginning in 2013, FinCEN developed an extensive corpus applying the money-transmitting laws it administers to non-custodial software development and the cryptocurrency ecosystem. *See Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013), perma.cc/5WCK-BLGF; *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014), perma.cc/4B2Q-XKEV; *Application to Certain Business Models Involving Convertible Virtual Currencies*, *supra*, at 15. Given the fact that §1960 and the relevant Bank Secrecy Act provisions were written decades before the technological innovations of instantaneous digital asset transfers, FinCEN endeavored to apply these older laws to new technology in a way that gave forward-looking guidance to the digital-asset industry and preserved regulatory stability. And in turn, the digital-asset industry relied on FinCEN's Guidance as a trustworthy source on the federal government's position.

At the core of FinCEN's Guidance was the requirement that, in order to qualify as a money transmitter, a person must have "total independent control over the value" being moved. *Application to Certain Business Models Involving Convertible Virtual Currencies*, *supra*, at 15. Applying this requirement, FinCEN explained in 2019 that the developer of an "unhosted" cryptocurrency wallet—non-custodial "software hosted on a person's computer, phone, or other device that allow[s] the person to store [cryptocurrency] and conduct [peer-to-peer] transactions"—is not a money transmitter because the developer lacks control over user funds. *Id.* at 15-16. That control remains missing whether the non-custodial software tool offers enhanced security features, *id.* at 17 (unhosted multiple-signature wallet), or privacy-protection functionality, *id.* at 20 ("anonymizing software provider"). This control requirement, FinCEN stressed, "is not technology-dependent." *Id.* at 15.

FinCEN's Guidance remained consistent over time. In 2013, FinCEN explained that, for a person to be a money transmitter under its regulations, the person must "accep[t]" and "transmi[t]" the cryptocurrency or "engag[e] in the transfer of funds." *Application to Persons Administering, Exchanging, or Using Virtual Currencies*, *supra*, at 3 & n.10. This explanation cited FinCEN's regulations, 31 C.F.R. §1010.100(ff)(5)(ii)(A)-(F), which then excluded (and still exclude today) one who merely "[p]rovides the delivery, communication, or network access services used by a money transmitter to support money transmission services" from the definition of "money transmitter," §1010.100(ff)(5)(ii)(A). FinCEN reiterated the principle a year later when it explained, citing the same regulations, that "the production and distribution of software, in and of itself, does not constitute acceptance and transmission of value," and therefore is not money transmission, "even if the purpose of the software is to facilitate the sale of virtual currency." *Application to Virtual Currency Software Development*, *supra*, at 2. In 2019, FinCEN tripled down in an analysis of the money-transmitting laws' application to certain business models within the cryptocurrency ecosystem. *See generally Application to Certain Business Models Involving Convertible Virtual Currencies*, *supra*. From the beginning, FinCEN stressed that the 2019 Guidance was a continuation of its longstanding practice and expressly disclaimed any intention to "establish … new regulatory expectations or requirements." *Id.* at 1.

In every case, across years of guidance documents, FinCEN has drawn a distinction based on whether the provider of a software tool obtains "total independent control of … value" and thus "accepts," "transmits," and "transfers" that value. If the provider obtains control of user funds, it is a money transmitter. But if the provider merely creates a neutral tool that allows users to make peer-to-peer transactions while maintaining control of their own value, no funds are "accepted," "transmitted," or "transferred" within the meaning of the money-transmitting laws. This principle was well-understood by the public, the defendants, the cryptocurrency ecosystem, and many members of Congress to exclude non-custodial software tools like Samourai Wallet. *See, e.g.*, *Brady Letter* at 4-5; Tuminelli, et al., *Through the Looking Glass*; Van Valkenburgh, *New Tornado Cash Indictments Seem to Run Counter to FinCEN Guidance*, Coin Center (Aug. 23, 2023), perma.cc/LK4H-KUUJ; Sens. Lummis & Wyden, *Letter to Hon. Merrick Garland from Sen. Lummis & Sen. Wyden, Re: Money Transmitting Business Registration and Non-Custodial Crypto Asset Software* 1 (May 9, 2024), perma.cc/9AKY-PZRX (*Garland Letter*).

This control requirement applies equally to each clause of §1960. Money transmitting in the criminal context is no broader than money transmitting in the statutes that FinCEN directly administers. Indeed, FinCEN's regulations use near-identical terms to define money transmitting as appear in §1960(b)(2). Section 1960 defines "money transmitting" as "transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier." §1960(a), (b)(2). FinCEN's regulations define a "money transmitter" as one who "accept[s]" funds and then "transmi[ts]" that value "to another location or person by any means," or "[a]ny other person engaged in the transfer of funds." 31 C.F.R. §1010.100(ff)(5)(i)(A)-(B). And courts have recognized that money transmitting in §1960 is not a broader concept than money transmitting elsewhere in federal law. *See United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 92 & n.10 (D.D.C. 2008). Thus, FinCEN's correct position—that, to be a money transmitter, a defendant must obtain total independent control of the funds being moved— applies to federal money-transmitting law across the board, including Section 1960(b).

B. The Justice Department contradicted FinCEN without providing public notice or offering any reasoned explanation for its change in position.

Despite this clear guidance, in 2023, the Justice Department abruptly decided to contradict FinCEN, indicting several software developers under the money-transmitting laws based on a novel interpretation of what it means to "transfer" funds. These indictments were part of—what the Justice

Department now calls—a "reckless strategy of regulation by prosecution, which was ill conceived and poorly executed." *See* Blanche, Deputy Att'y Gen., *Ending Regulation by Prosecution* 1, Dep't of Just. (Apr. 7, 2025), perma.cc/986B-8TTF. Although the department "is not a digital assets regulator," these prosecutions "superimpos[ed]" a *new* regulatory framework on a large slice of the cryptocurrency ecosystem. *Id.* That framework flipped FinCEN's Guidance on its head, all without forward-looking notice to the software developers now subjected to potential criminal liability. According to the department's unprecedented and limitless theory, §1960 does not require that a defendant "take control of the funds" to qualify as a money transmitter. *See Storm* MTD Resp. at 31.

To make matters even more confusing, on April 7 of this year the Justice Department announced that it would no longer regulate by prosecution, and more specifically, no longer target ordinary registration violations including under §1960. *See Ending Regulation by Prosecution* at 1-3. The April 7 memo disavowed the department's previous course of conduct, rescinded "[a]ll previously issued policies and directives … inconsistent with" the memo, and instructed that "[o]ngoing investigations … inconsistent with the [memo] should be closed." *Id.* at 1-2. Yet this prosecution, one of the most egregious instances of the failed "strategy of regulation by prosecution," continues.[1] Underlining the serious due-process problems with the government's abrupt about-face, a recent filing confirmed that the DOJ knew (but failed to disclose) evidence that its novel "no-control-required" interpretation of §1960 was inconsistent with FinCEN's longstanding practice. *See Brady* Letter at 7.

[1] Although the DOJ recently abandoned the §1960(b)(1)(B) charge in *Storm*, it has yet to do so in this case. *See* Update Letter (Dkt. 144), *United States v. Storm*, No. 23 Cr. 430 (KPF) (S.D.N.Y. May 15, 2025). And even if it had, the update letter appears to double down on the erroneous idea that §1960(b)(2) applies differently to §1960(b)(1)(B) than the other money-transmitting provisions in §1960.

C. The government's change in position violated constitutional principles of due process and fair notice.

"A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations*, 567 U.S. 239, 253 (2012). This requirement "is essential to the protections provided by the Due Process Clause of the Fifth Amendment," *id.*, under which a conviction must fail "if the statute under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited," *United States v. Williams*, 553 U.S. 285, 304 (2008). The Supreme Court has repeatedly applied these principles to rule that a prosecution contradicting the prosecuting authority's previous public reassurance to a regulated party cannot stand. *See, e.g.*, *Raley v. Ohio*, 360 U.S. 423, 425-26 (1959); *Cox v. Louisiana*, 379 U.S. 559, 571 (1965).

While this principle does not prevent the government from making a reasoned change to a prior legal position, such changes "becom[e] a problem—a fatal one—when the Government decides to turn around and *retroactively* apply [its] new interpretation to proscribe conduct that occurred *before* the new interpretation was issued." *PHH Corp. v. CFPB*, 839 F.3d 1, 44 (D.C. Cir. 2016) (Kavanaugh, J.), *reh'g en banc granted, order vacated* (Feb. 16, 2017), *on reh'g en banc*, 881 F.3d 75 (D.C. Cir. 2018). As then-Judge Kavanaugh summarized: "When a government agency officially and expressly tells you that you are legally allowed to do something, but later tells you 'just kidding' and enforces the law retroactively against you and sanctions you for actions you took in reliance on the government's assurances, that amounts to a serious due process violation." *Id.* at 48. Thus, when an agency's prior communication with the public deprives the defendant "of fair warning as to what conduct the Government intended to make criminal … there can be no doubt that traditional notions of fairness inherent in our system of criminal justice prevent the Government from proceeding with the prosecution." *United States v. Penn. Indus. Chem. Corp.*, 411 U.S. 655, 674 (1973); *accord Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 156-57 (2012).

The Justice Department's theory of Count II violates these principles. It rejects FinCEN's control requirement altogether, arguing instead that §1960 does not require that a defendant "take control of [any] funds." *Storm* MTD Resp. at 31. Thus, according to the department and contrary to FinCEN's longstanding Guidance, the developers of non-custodial software tools like unhosted wallets are money transmitters, including projects that offer security- or privacy-enhancing features and even if they do not "take control of [any] funds." *Id.* at 24-31. For the first time, under the department's new interpretation, these software developers must register as money transmitters or else be subject to criminal prosecution.

This radical change in position was not brought on by an amendment to the money-transmitting laws. Nor did the government rely on a rule adopted after notice and comment, or even a revision to FinCEN's longstanding Guidance. Rather, the government announced its departure from FinCEN's position by indicting the developers of several non-custodial software tools for allegedly violating money-transmitting laws that FinCEN spent years assuring them were inapplicable. Though the defendants "conform[ed] their conduct to [FinCEN's] interpretatio[n]" of the law, they failed "to divine the [Justice Department's contrary] interpretatio[n] in advance." *SmithKline Beecham Corp.*, 567 U.S. at 159. The penalty for this lack of prescience? A federal criminal prosecution threatening years in prison and substantial fines. That is precisely what the Due Process Clause forbids. *See, e.g.*, *PHH Corp.*, 839 F.3d at 44, 48 (Kavanaugh, J.).

III. The legal theory underlying Count II has chilled innovation and will stifle the lawful development of non-custodial software tools.

The government's "'surprise switcheroo,'" *Azar v. Allina Health Servs.*, 587 U.S. 566, 571 (2019), shocked the cryptocurrency world. As amici, BA's members, and software developers saw firsthand, these prosecutions shattered the preexisting consensus and chilled development and innovation. They cast doubt on the legality of a wide range of software projects and exposed well-meaning developers to potentially significant criminal liability. And they have ensured that software developers and members of the cryptocurrency ecosystem cannot confidently rely on the careful and considered judgments of their regulators moving forward. *Contra* Exec. Order 14178, *Strengthening American Leadership in Digital Financial Technology*, 90 C.F.R. 8647, 8647 (Jan. 31, 2025) (adopting a policy "to support the responsible growth and use of digital assets[,] … including by providing regulatory clarity and certainty built on technology-neutral regulations"). After all, if one part of the executive branch can assure the public that an action is legal only for another to later claim that the same action was actually a serious federal crime, developers cannot afford to place themselves at risk of prosecution under the latter pronouncement by relying on the former one.

The government's abrupt contradiction of its own longstanding position has disturbing implications for software developers everywhere and, unsurprisingly, has profoundly chilled innovation. Its interpretation of the money-transmitting laws to cover non-custodial software tools generated widespread shock and alarm in the cryptocurrency world, which had long relied on the government's clear and correct guidance saying the opposite. *See, e.g.*, Van Valkenburgh, *DOJ's New Stance on Crypto Wallets is a Threat to Liberty and the Rule of Law*, Coin Center (Apr. 29, 2024), perma.cc/LV4E-F7JF; Anthony, *Samourai Charges Mark Chilling Moment for Financial Privacy*, Cato Inst. (Apr. 30, 2024), perma.cc/LFJ2-TWHA. And while the government's strategy of prosecution-by-ambush initially focused on software development in the cryptocurrency ecosystem, no limiting principle confines the department's "no-control-required" reading of §1960 to cryptocurrency or software. Rather, the provider of any neutral technology that a third-party might use to move value is now potentially subject to serious criminal liability. *See, e.g.*, DEF, et al., *Letter to White House AI and Crypto Czar* 1-2 (Apr. 7, 2025), perma.cc/HK5M-527J. Reading §1960 to sweep so broadly would give prosecutors carte blanche to "target software developers aligned with politically disfavored causes and industries" across an "incalculable" "surface area for selective prosecution." *Letter to White House AI and Crypto Czar* at 1.

The legislative branch has also sounded the alarm about the due-process implications of this jarring change in position. Congress heard testimony from concerned members of the cryptocurrency ecosystem, including amici, on the pernicious effects that would inevitably flow downstream from the Justice Department's campaign of regulation by prosecution. *See, e.g.*, Written Testimony of A. Tuminelli, *Decoding DeFi: Breaking Down the Future of Decentralized Finance, H. Comm. On Fin. Servs., Subcomm. on Digital Assets, Fin. Tech. and Inclusion* 12 (Sept. 10, 2024), perma.cc/DDE5-P4ZC. And a bipartisan group of Senators wrote Attorney General Garland to express their "grave concerns" that the "DOJ's unprecedented interpretation of [§1960] in the context of non-custodial crypto asset software services contradicts the clear intent of Congress and the authoritative Guidance of the Department of the Treasury's Financial Crimes Enforcement Network." *Garland Letter* at 1. The Senators explained that, as the defendants and amici argue here, "[t]he statutes and regulations are clear that direct receipt and control of assets are required elements of money transmission." *Id.* at 1. Thus, "non-custodial crypto service providers cannot be classified as money transmitter businesses because users of such services retain sole possession and control of their crypto assets." *Id.* at 2. "Indeed, this limiting factor is essential, otherwise a wide range of additional services such as internet service providers or postal carriers could inadvertently be caught in the definition of a money transmitting business since they routinely send, receive and process information and messages regarding payments." *Id.* at 1.

IV. Count II violates the rule of lenity and the major-questions doctrine.

Even if the Court concluded that neither §1960's plain text nor the constitutional principles of fair notice and due process resolve the interpretive question, it should still dismiss Count II. The statute is at least ambiguous on whether control is required. In such circumstances, courts rely on a series of well-known tiebreakers. Two of those rules, the rule of lenity and the major-questions doctrine, cut strongly in the defendants' favor.

Lenity. "The 'rule of lenity' is a new name for an old idea." *Wooden v. United States*, 595 U.S. 360, 388 (2022) (Gorsuch, J., concurring in the judgment). Part of the Anglo-American legal tradition running from Blackstone to Marshall and Story, lenity was initially justified by the familiar "assumption that that when Parliament intended to inflict severe punishments it would do so clearly." *Id.* Although this descriptive justification persists today, across the Atlantic "lenity came to serve distinctively American functions—a means for upholding the Constitution's commitments to due process and the separation of powers." *Id.* at 389.

The connection to due process is especially relevant to a case like this one where the charged conduct occurred in reliance on the government's previous legal position. The rule of lenity "works to enforce the [Constitution's] fair notice requirement by ensuring that an individual's liberty always prevails over ambiguous laws." *Id.*; *see also Snyder v. United States*, 603 U.S. 1, 20-21 (2024) (Gorsuch, J., concurring) (explaining that lenity and fair notice often perform similar functions in criminal cases). This "'settled usag[e]'" of the American legal system "protect[s] an indispensable part of the rule of law—the promise that [individuals] can suffer penalties only for violating standing rules announced in advance." *Wooden*, 595 U.S. at 389-91 (Gorsuch, J., concurring in the judgment). It also "minimizes the risk of selective or arbitrary enforcement, and strikes the appropriate balance between the legislature and the court in defining criminal liability." *United States v. Valle*, 807 F.3d 508, 523 (2d Cir. 2015). In the Second Circuit, when a criminal statute is ambiguous and "the Government and the defense both posit plausible interpretations[,] … the rule of lenity requires [the court] to adopt the defendant's construction." *Id.*

Lenity resolves this case for the defendants. As discussed above, the Justice Department's interpretation falls short. But even giving the government the benefit of its arguments on all those points, at least "'a reasonable doubt persists about [the] statute's intended scope,'" which is enough to trigger the rule of lenity. *Id.* (quoting *Moskal v. United States*, 498 U.S. 103, 108 (1990)).[2] And the government's disregard for due process and fair notice in its retreat from FinCEN's Guidance makes this case "a particularly appropriate candidate for the rule of lenity." *Bittner*, 598 U.S. at 102 (Op. of Gorsuch, J.). In *Bittner*, due process favored lenity because "[a] number of the government's own public guidance documents … seemingly warned" that the defendant's interpretation might be right. *Id.* Here, FinCEN's longstanding Guidance documents did much more than "seemingly war[n]" that control was required under §1960: they firmly concluded that non-custodial software developers like the defendants were not money transmitters. If [the government's own executive agency, from 2013 to 2023, was "unable to anticipate the government's current theory," there is no realistic possibility that "'the common world' had fair notice of it." *Id.* at 103 (quoting *McBoyle v. United States*, 283 U.S. 25, 27 (1931)).

Major Questions. Like the rule of lenity, the major-questions doctrine vindicates the separation of powers. *See Wooden*, 595 U.S. at 391 (Gorsuch, J., concurring in the judgment); *West Virginia*, 597 U.S. at 737-38 (Gorsuch, J., concurring). The Supreme Court has "long recognized that 'the power of punishment is vested in the legislative, not in the judicial department." *Fischer v. United States*, 603 U.S. 480, 497 (2024); *see also Wooden*, 595 U.S. at 391 (Gorsuch, J., concurring in the judgment). Likewise, "'crimes are supposed to be defined by the legislature, not by clever prosecutors riffing on equivocal language."' *Dubin v. United States*, 599 U.S. 110, 129-30 (2023) (cleaned up). To these ends, courts "affor[d] proper respect to 'the prerogatives of Congress' in carrying out the quintessentially legislative act of defining crimes and setting the penalties for them" by refusing to overread statutes to criminalize broad swathes of otherwise innocent conduct. *Fischer*, 603 U.S. at 497

[2] For example, the Justice Department conceded in *Storm* that the references to "total independent control" in FinCEN's 2019 Guidance could, for at least some kind of cryptocurrency software, be applied to determine whether the software functioned as a money transmitter. *See Storm* MTD Resp. at 32-33.

(cleaned up). Exercising interpretive restraint "places the weight of inertia upon the party that can best induce Congress to speak more clearly and keeps courts from making criminal law in Congress's stead." *United States v. Santos*, 553 U.S. 507, 514 (2008).

This case calls for the application of a "major questions lenity" rule rooted in the separation of powers. A conviction under §1960 can result in substantial criminal penalties. *See* 18 U.S.C. §1960(a) (providing for a fine and up to five years in prison). And the Justice Department's novel interpretation risks criminalizing otherwise lawful development of any neutral technology that Americans use to engage in peer-to-peer transactions. For example, the government's reading threatens to criminalize non-custodial wallets—tools that ordinary cryptocurrency owners use millions of times each month. *See, e.g.*, Matsuoka & Lazzarin, *Estimating the Number of Real Crypto Users*, a16zcrypto (Oct. 16, 2024), perma.cc/YP34-W92Y (citing a 2024 study from MetaMask, a popular non-custodial cryptocurrency wallet, reporting 30 million monthly active users). Section 1960's proper scope is also at the center of a lively policy exchange between the public and the political branches, with legislative leaders harshly criticizing the government's unexplained departure from FinCEN's Guidance. *See, e.g.*, *Garland Letter* at 1. To accept the DOJ's construction in the absence of a clear indicator in §1960's text and structure would short-circuit the political process and reward the government's "reckless" and "ill conceived" "strategy of regulation by prosecution." *Ending Regulation by Prosecution* at 1.

CONCLUSION

The Court should grant the motions to dismiss Count II.

Dated: June 5, 2025

Respectfully submitted,

<u>/s/Daniel M. Vitagliano</u>

Cameron T. Norris*
Daniel M. Vitagliano (SDNY 5856703)**
Zachary P. Grouev*
Consovoy McCarthy PLLC
1600 Wilson Boulevard, Suite 700
Arlington, Virginia 22209

**pro hac vice applications forthcoming*
*** supervised by principals of the firm admitted to practice in Virginia*

(703) 243-9423
dvitagliano@consovoymccarthy.com
cam@consovoymccarthy.com
zach@consovoymccarthy.com

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