REGULATING CRYPTOCURRENCY: A COMPARATIVE ANALYSIS OF U.S. AND EU APPROACHES

Xander Xueyang Peng[*]

I. INTRODUCTION

The rise of cryptocurrency during the 2020 global pandemic attracted the attention of lawmakers around the world. Although the U.S. legal system has struggled to grapple with innovative

[*] Senior Notes Editor, Cardozo International & Comparative Law Review (Volume 7); J.D. Candidate, Benjamin N. Cardozo School of Law (2024). I would like to extend my gratitude to my Note Advisor, Jessica Roth, for her insightful feedback and guidance; my colleagues on the CICLR for their diligent work in preparing this Note for publication; and my mentor, Sam Amir Toossi, whose inspiration was instrumental in shaping the topic.

technologies, U.S. policymakers from all branches of government have expressed concerns that cryptocurrency could be a significant avenue for committing white-collar crimes.[1]

Cryptocurrency is primarily known for its decentralized structure,[2] appealing to consumers who prefer a system without government involvement. The blockchain technology that underpins most cryptocurrency means that every transaction is permanently logged, which can be traced and viewed through a public ledger.[3] Tracing illegal transactions back to actual individuals can be particularly challenging for pertinent government agencies, however.[4] Moreover, since cryptocurrency transactions bypass traditional financial systems and institutions that possess well-established compliance programs, the prevailing apprehension that cryptocurrencies can be leveraged for white-collar crimes, such as sanctions evasion and money laundering, has merit.[5]

On March 9, 2022, President Biden enacted an Executive Order on Ensuring Responsible Development of Digital Assets, explicitly enumerating "sanctions evasion" and "money laundering" as challenges posed by digital assets like cryptocurrencies.[6] However, following the 2022 downfall of FTX, the world's preeminent digital asset exchange platform, U.S. Securities and Exchange Commission ("SEC") Commissioner Gary Gensler persisted in his belief that his "regulation by enforcement" approach can aptly address crypto-related calamities.[7]

1 Letter from Elizabeth Warren, Mark R. Warner, Sherrod Brown & Jack Reed to Janet Yellen, Sec'y of the Dep't of the Treasury (Mar. 2, 2022), https://www.warren.senate.gov/imo/media/doc/2022.03.01%20Letter%20to%20Treasury%20re%20OFAC%20crypto%20sanctions%20enforcement.pdf [https://perma.cc/CQ9T-5XVE].

2 *See* Ephrat Livni & Eric Lipton, *Crypto Banking and Decentralized Finance, Explained*, N.Y. TIMES, https://www.nytimes.com/2021/09/05/us/politics/cryptocurrency-explainer.html [perma.cc/M7XA-3T7D] (Nov. 1, 2021).

3 *See Protect Your Privacy*, BITCOIN, https://bitcoin.org/en/protect-your-privacy [https://perma.cc/N4AH-RHHJ] (last visited Sept. 2, 2022).

4 *See* John Bohannon, *Why Criminals Can't Hide Behind Bitcoin*, SCIENCE (Mar. 9, 2016), https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin.

5 *Id.*

6 87 Fed. Reg. 40881 (Aug. 8, 2022).

7 Squawk Box, *SEC Chair Gary Gensler on FTX Fallout: Investors Need Better Protections in Crypto*, CNBC (Nov. 10, 2022, 8:48 AM), https://www.cnbc.com/video/2022/11/10/sec-chair-gary-gensler-on-ftx-fallout-investors-need-better-protections-in-crypto.html [https://perma.cc/GC2K-ZWZT].

The crypto industry's dearth of legal safeguards has precipitated substantial losses, predominantly borne by retail digital asset investors. For instance, the Federal Trade Commission ("FTC") reported that consumers lost more than $1 billion to cryptocurrency-related fraud in 2022.[8] This regulatory void incentivized white-collar criminal activities. Merely a few months after the FTC's revelation, FTX vanished, taking more than $1 billion in client funds with it.[9] Sam Bankman-Fried, the founder and CEO of FTX, subsequently faced indictment on charges of fraud, money laundering, and violations of campaign finance laws.[10]

This Note compares the crypto asset-related legal frameworks of the European Union and the United States. As U.S. regulators grapple with the rapidly evolving cryptocurrency landscape, the European Union recently promulgated a more comprehensive regulatory scheme detailing the oversight and regulation of crypto assets.[11] Within this framework, the European Union specifies which agencies possess the authority to initiate prosecutions for crimes involving these digital assets.[12] Unlike the European Union, which has rules specifically designed for crypto assets, the United States regulates crypto assets by applying extant securities regulations, resulting in diverse agencies overseeing related sectors. For example, the Office of Foreign Asset Control ("OFAC") has furnished enforcement guidance pertaining to sanction regimes that encompass cryptocurrency.[13] Concurrently, the Financial Crimes Enforcement Network ("FinCEN") formulates rules

8 *CFTC Commissioner on FTX Fallout, Crypto Regulation Outlook*, COINDESK (Nov. 10, 2022), https://www.coindesk.com/video/cftc-commissioner-on-ftx-fallout-crypto-regulation-outlook/ [https://perma.cc/UZ5K-KHNA].

9 Angus Berwick, *Exclusive: At Least $1 Billion of Client Funds Missing at Failed Crypto Firm FTX*, REUTERS (Nov. 13, 2022, 5:00 PM), https://www.reuters.com/markets/currencies/exclusive-least-1-billion-client-funds-missing-failed-crypto-firm-ftx-sources-2022-11-12/.

10 Press Release, U.S. Att'y's Off., S. Dist. of N.Y., United States Attorney Announces Charges Against FTX Founder Samuel Bankman-Fried (Dec. 13, 2022), https://www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried [https://perma.cc/6Q44-YN2K].

11 *See* Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, COD (2020) 265 (May 3, 2023), https://data.consilium.europa.eu/doc/document/PE-54-2022-INIT/en/pdf [https://perma.cc/F22Q-LYE3].

12 *Id.* at 441.

13 *See* OFF. OF FOREIGN ASSETS CONTROL, SANCTIONS COMPLIANCE GUIDANCE FOR THE VIRTUAL CURRENCY INDUSTRY (Oct. 2021), https://ofac.treasury.gov/media/913571/download? [https://perma.cc/ZZA4-FVSS].

and compliance standards to buttress anti-money laundering efforts.[14] Additionally, the Department of Justice ("DOJ") steps in to levy criminal charges in the wake of crypto-related white-collar crimes.[15]

Part II summarizes the general legal paradigm of economic sanctions and anti-money laundering ("AML") as it relates to fiat currency. Specifically, it identifies the EU and U.S. agencies vested with the authority to enforce pertinent regulations. The overarching objective is to underscore the significance of maintaining the efficacy of the extant sanctions and AML legal infrastructures in the European Union and the United States when they are extended to encompass crypto assets.

Part III explores the strategies that the European Union and the United States employ to regulate economic sanctions associated with crypto assets. While the United States leans toward strict liability standards when imposing civil penalties on firms that breach sanctions, this method fails to deter sanction evasion via cryptocurrency, primarily because crypto users can often conceal their transactions. In contrast, the European Union mandates that crypto asset payment service providers furnish a comprehensive list of personal data about their users. Even though this rule is met with resistance and sparks controversy, especially among major crypto platforms, the European Union's approach to cryptocurrency regulation effectively addresses the fundamental challenge.

Part IV examines the European Union's and the United States' strategies for enforcing anti-money laundering regulations concerning crypto assets. It highlights how the United States, by attempting to equate cryptocurrency with fiat currency regarding anti-money laundering, neglects passing specific laws addressing pseudo-anonymity, the distinct trait of crypto assets. Conversely, the European Union's updated regulation mandates that crypto businesses gather and reveal information related to both the initiator and the recipient of the crypto asset transfers they manage. This Part underscores that the primary hurdle in countering crypto crimes is the issue of traceability, a challenge rooted in the pseudo-anonymous nature of cryptocurrencies. Transactions between two self-hosted wallets become almost indiscernible.

14 *Frequently Asked Questions,* U.S. TREASURY FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/frequently-asked-questions [https://perma.cc/2QNC-5PVM] (last visited Mar. 3, 2023).

15 *Crypto Enforcement*, CRIM. DIV., U.S. DEP'T OF JUST., https://www.justice.gov/criminal/criminal-fraud/crypto-enforcement [https://perma.cc/7JQF-CV2M] (last visited Apr. 24, 2024).

Part V, after a comparative analysis of recent enforcement actions by various agencies in the European Union and United States, advocates for the U.S. government to implement more structured and rigorous regulations for the cryptocurrency industry. This Part provides an overview of the three bills introduced in the U.S. Congress in July 2023. It promotes the adoption of these three bills, emphasizing that regulations should mandate comprehensive know-your-customer ("KYC") procedures applicable to all U.S. blockchain-based platforms. Despite its potential to spark controversy, this Note posits that a stringent customer identification system will serve as an effective deterrent against crypto crimes and enhance protection for cryptocurrency users.

II. BACKGROUND

A. Economic Sanction

Restrictive measures or economic sanctions are pivotal instruments within the European Union's Common Foreign and Security Policy ("CFSP") framework, which aims to uphold the European Union's core values, interests, and security imperatives.[16] The development of sanctions involves different actors in the EU Council. The European External Action Service ("EEAS") assists the High Representatives in fulfilling their mandate and has an active role in preparing, maintaining, and reviewing sanctions.[17] Concurrently, the European Commission proffers proposals and collaborates with the High Representatives to draft regulations.[18] As its decisions are binding on the Member States, implementation and enforcement of EU sanctions is the responsibility of those states, which must assess whether there has been a breach of the sanction and take adequate steps.[19]

Similarly, economic sanctions are a preferred instrument for the U.S. government to influence the strategic choices of foreign entities

16 *European Union Sanctions*, EUR. UNION EXTERNAL ACTION (Oct. 7, 2021), https://www.eeas.europa.eu/eeas/european-union-sanctions_en [https://perma.cc/P5SB-LWVB].

17 *Id.*

18 *Id.*

19 *Id.*

that threaten the United States' interests.[20] The United States employs sanctions to curtail customary trade and financial relations with specified and targeted groups.[21] For example, in the wake of Russia's aggression against Ukraine, the United States and the European Union swiftly retaliated with a barrage of sanctions targeting specific Russian individuals and organizations with the aim of debilitating Russia's economy.[22] The "anonymous" characteristic of cryptocurrency, however, immediately prompts concerns about Russia's potential to exploit crypto in circumventing these sanctions.[23]

The Office of Foreign Assets Control ("OFAC") within the U.S. Department of the Treasury derives its sanction-enforcement authority from multiple federal statutes, particularly the International Emergency Economic Powers Act ("IEEPA").[24] OFAC enforces sanctions by preventing prohibited transactions, which are defined as "trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute."[25] Pursuant to the IEEPA, the President, during times of national emergencies, has the power to block or confiscate foreign assets that fall under U.S. jurisdiction.[26] In addition to these functions, OFAC also publishes a list of Specially Designated Nationals ("SDNs"). Entities and individuals named on this list are prohibited from conducting business with U.S.-based financial institutions.[27] Recently, OFAC has added several individuals and crypto exchanges implicated in

20 *See Basic Information on OFAC and Sanctions*, US DEP'T OF THE TREASURY, OFF. OF FOREIGN ASSETS CONTROL, https://ofac.treasury.gov/faqs/topic/1501 [https://perma.cc/H4PB-7WSU] (last visited Jan. 27, 2023).

21 *Id.*

22 *FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia*, THE WHITE HOUSE (Apr. 6, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/ [https://perma.cc/KE9G-8MU3].

23 William Alan Reinsch & Andrea Leonard Palazzi, *Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia*, CSIS (Dec. 20, 2022), https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia [https://perma.cc/HR8T-PG7W].

24 Kian Meshkat, *Navigating U.S. Economic Sanctions*, CAL. LAWS. ASS'N (Jan. 2023), https://calawyers.org/international-law/navigating-u-s-economic-sanctions/ [https://perma.cc/S8JH-4UD4].

25 *Basic Information on OFAC and Sanctions*, *supra* note 20.

26 *See* 50 U.S.C. § 1702 (1977).

27 *See Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, U.S. DEP'T OF THE TREASURY, OFF. OF FOREIGN ASSETS CONTROL, https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists [https://perma.cc/VZK9-5C4G] (Jan. 31, 2024).

laundering illicit proceeds to its list.[28] Economic sanction has emerged as a foremost diplomatic tool of engagement, serving multiple purposes, including deterring undesirable actions, imposing economic penalties, compelling rehabilitation, or inducing behavioral change in the targeted nation, entity, or individual.[29] Therefore, all U.S. citizens and permanent resident aliens, irrespective of their geographical location; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches are required to comply with OFAC regulations.[30]

Both the European Union and the United States recognize the efficacy of sanctions as a tool. However, the swift evolution and widespread adoption of cryptocurrency—a decentralized system—introduces a unique avenue for evading sanctions, presenting obstacles to effective enforcement.[31] While tactics for evading sanctions can differ significantly, the overarching aim of sanction evasion is often to shield assets from regulatory oversight or bypass asset freezes when procuring restricted materials. This Note aims to examine and compare existing OFAC enforcement measures with EU regulations, as well as propose potential cryptocurrency regulations in the United States.

B. Anti-Money Laundering

The European Union introduced the first anti-money laundering directive in 1990 to prevent the financial system's exploitation through money laundering.[32] Over the following three decades, the European Union regularly refined its framework to ensure a consistent approach to AML legislation within the single market and protect the financial system.[33] The EU Anti-Money Laundering Directives ("AMLDs") are periodically promulgated by the European Parliament for

28 *See* Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group (Mar. 2, 2020), https://home.treasury.gov/news/press-releases/sm924 [https://perma.cc/WBJ3-NYWD].

29 Jonathan Masters, *What Are Economic Sanctions?*, COUNCIL ON FOREIGN RELS. https://www.cfr.org/backgrounder/what-are-economic-sanctions [https://perma.cc/S2MN-G64E] (Aug. 12, 2019, 8:00 AM).

30 *Basic Information on OFAC and Sanctions*, *supra* note 20.

31 Reinsch & Palazzi, *supra* note 23.

32 *EU Context of Anti-Money Laundering and Countering the Financing of Terrorism*, EUR. COMM'N, https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en [https://perma.cc/RB7W-M5Q5] (last visited Jan. 31, 2024).

33 *Id.*

implementation by the member states.[34] Shortly after issuing the 5th Directive, the European Union further bolstered its anti-money laundering regime by fully implementing the 6th Directive ("6AMLD") in June 3, 2021.[35] These two Directives bear particular significance for the crypto industry, as the European Union's anti-money laundering regulations were expanded to encompass cryptocurrency wallet service providers and crypto-to-fiat exchanges operating within the European Union.[36] Additionally, the 6AMLD increased the minimum prison sentence for money laundering offenses from one year to four years and authorized judges to impose fines on individuals found guilty of money laundering.[37]

While movies and TV shows often depict money laundering as the act of cleansing illicitly gained funds from criminal endeavors, U.S. federal statutes encompass a broader array of money laundering activities. The most important statute is 18 U.S.C. § 1956, which criminalizes certain money laundering and tax evasion activities that involve the proceeds stemming from underlying crimes.[38] As articulated by the Supreme Court in *Cuellar v. United States*, section 1956's prohibition on the international transportation of illicit proceeds with the intent of concealing the source or ultimate location is restricted to concealment that is a purpose rather than an attribute of the transportation.[39] Furthermore, 18 U.S.C. § 1957 prohibits engaging in monetary

34 *See id.*

35 *The Perfect Storm: EU's 6th Anti-Money Laundering Directive Raises Regulatory Risk with a Broader Definition of Money Laundering & Extended Criminal Liability*, LEXISNEXIS (Nov. 21, 2022) [hereinafter *The Perfect Storm*], https://www.lexisnexis.com/blogs/gb/b/compliance-risk-due-diligence/posts/the-perfect-storm-eu-s-6th-anti-money-laundering-directive-raises-regulatory-risk-with-a-broader-definition-of-money-laundering-extended-criminal-liability [https://perma.cc/6SFP-PU8X]; Luděk Niedermayer & Paul Tang, *Proposal for a Directive on the Mechanisms to Be Put in Place by the Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Repealing Directive (EU) 2015/849*, EUR. PARLIAMENT LEG. TRAIN SCHEDULE (Mar. 20, 2024), https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-6th-directive-on-amlcft-(amld6) [https://perma.cc/KS92-D8ZL]; *see also* COMPLYADVANTAGE, LOOKING AHEAD TO THE 6TH ANTI MONEY LAUNDERING DIRECTIVE (2020), https://www.antiriciclaggiocompliance.it/app/uploads/2020/08/Looking-ahead-the-6th-Anti-Money.pdf [https://perma.cc/M4R7-GXQJ].

36 *Crypto-Assets, Wallets, Exchanges and 6AMLD*, COMPLYADVANTAGE, https://complyadvantage.com/insights/crypto-assets-wallets-exchanges-6amld/ [https://perma.cc/F9HA-9XWE] (May 4, 2022).

37 *The Perfect Storm*, *supra* note 35.

38 18 U.S.C. § 1956(a).

39 Cuellar v. United States, 553 U.S. 550, 565 (2008).

transactions involving "criminally derived property" worth more than $10,000.[40] The Travel Act (18 U.S.C. § 1952) criminalizes traveling in or utilizing foreign commerce to disburse proceeds or facilitate certain illicit activities.[41] Money laundering offenses are met with stringent penalties, which often include extended prison sentences and the seizure of assets associated with or traceable to the laundering activity.[42]

The first major anti-money laundering legislation in the United States was the 1970 Bank Secrecy Act ("BSA") which mandates that banks report cash deposits exceeding $10,000, identify individuals conducting these transactions, and retain records of the transactions.[43] Consequently, the primary emphasis of the BSA was on Suspicious Activity Reports ("SARs"), which are reports that a financial institute and its associated business must file whenever they detect potential money laundering or fraud.[44] The global attention to anti-money laundering increased in 1989 when various countries and international entities established the Financial Action Task Force ("FATF"), whose mission was to formulate international standards to prevent money laundering.[45]

The Anti-Money Laundering Act ("AMLA") of 2020 represented the most comprehensive revamp of U.S. AML regulations, addressing the emerging threats introduced by technological advancements.[46] The Act requires the Financial Crimes Enforcement Network ("FinCEN") to promulgate regulations setting standards for such financial institutions, outlining the measures they should take to assess their compliance with BSA requirements.[47] Significantly, the AMLA expanded the

40 18 U.S.C. § 1957(a).

41 18 U.S.C. § 1952(a).

42 *See* 18 U.S.C. §§ 1956(b), 1957(b).

43 Jackie Wheeler, *The Bank Secrecy Act Turns 50: Five Decades of Anti-Money Laundering in the US*, JUMIO (Oct. 26, 2020), https://www.jumio.com/bank-secrecy-act-turns-50/ [perma.cc/6XP8-W6CL].

44 *BSA Timeline*, U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act/bsa-timeline [perma.cc/4K7E-FGXS] (last visited Nov. 18, 2023).

45 *The Financial Action Task Force*, U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/international/financial-action-task-force [perma.cc/LUN4-HSGR] (last visited Nov. 18, 2023).

46 *Four Takeaways on BSA/AML Reform Under the Anti-Money Laundering Act of 2020*, THOMSON REUTERS (Aug. 9, 2021), https://legal.thomsonreuters.com/en/insights/articles/4-takeaways-on-bsa-aml-reform [perma.cc/3K3K-V5PJ].

47 U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM NATIONAL

BSA's definition of "financial institution" to encompass businesses involved in the exchange or transmission of cryptocurrency.[48]

The AMLA complements the BSA, building upon its foundational requirements by placing a greater emphasis on risk identification and management, rather than just reporting suspicious activities to regulatory bodies.[49] The AMLA entrusts FinCEN—a key U.S. agency spearheading anti-money laundering efforts—with the responsibility of equipping financial institutions with insights into prevalent financial crime trends and patterns.[50] The Act also mandates that FinCEN periodically release summaries detailing how Suspicious Activity Reports have been beneficial to law enforcement initiatives.[51]

The European Union's recent stance on cryptocurrency AML suggests a more rigorous approach than the United States'. The European Union strongly emphasizes ensuring the traceability of crypto asset transactions, demanding the same level of scrutiny as conventional money transfers.[52] It mandates that crypto asset service providers validate that the source of the asset is not under sanctions and does not contain money laundering risks.[53] These regulations also encompass transactions between non-custodial (un-hosted) wallets and custodial (hosted) wallets managed by crypto assets service providers ("CASPs").[54] Whenever transactions between a CASP's hosted wallet and an un-hosted wallet exceed €1000, the CASP must authenticate the identity associated with the un-hosted wallet.[55]

Both the United States and the European Union are heavily invested in regulating money laundering. The penalties for money laundering offenses imposed by U.S. federal criminal statutes are severe,

PRIORITIES 3 (2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

48 *Id.* at 1 n.5.

49 *Id.* at 1.

50 William M. Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 6102, 134 Stat. 3387, 4552 (2021).

51 *Id.* § 6202 (amending 31 U.S.C. § 5318(g))

52 Press Release, European Parliament, Crypto Assets: Deal on New Rules to Stop Illicit Flows in the EU (June 29, 2022, 9:24 PM), https://www.europarl.europa.eu/news/en/press-room/20220627IPR33919/crypto-assets-deal-on-new-rules-to-stop-illicit-flows-in-the-eu [https://perma.cc/5XLU-JTM9].

53 *Id.*

54 *Id.*

55 *Id.*

sometimes exceeding the punishments for their underlying crimes.[56] Under the AMLA, FinCEN is responsible for devising regulations and setting compliance benchmarks, ensuring that financial institutions adhere to the standards set by the BSA.[57] To grasp the current U.S. AML regulations concerning cryptocurrency, this Note will examine U.S. enforcement actions and judicial interpretations related to cryptocurrency, contrasting them with the EU regulations that aim to mitigate crypto money laundering.

III. SANCTION

A. The European Union's Actions on Sanctions

Sanctions are instrumental for the European Union in furthering the objectives of the Common Foreign and Security Policy ("CFSP").[58] Similar to the United States, the European Union enforces sanctions to safeguard human rights, preserve territorial integrity, prevent the proliferation of nuclear weapons, and address other concerns.[59] The European Union draws its sanctions from two primary sources. Firstly, as member of the United Nations, EU Member States are required to implement binding resolutions passed by the UN Security Council under Chapter VII of the UN Charter.[60] Secondly, the European Union can implement autonomous measures independent of UN Security Council resolutions to further its unique interests.[61] Such measures are often invoked when the UN Security Council fails to achieve consensus.[62] While individual EU Member States may introduce national sanctions to further their own foreign policy objectives,[63] these instances are relatively uncommon.

Following the Russian invasion of Ukraine in 2022, the European Union's most widely used and essential type of sanction against

56 *See generally* U.S. SENT'G COMM'N, QUICK FACTS (2019), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Money_Laundering_FY19.pdf [https://perma.cc/XK5N-7AH9].

57 *See* Wheeler, *supra* note 43.

58 *See European Union Sanctions*, *supra* note 16.

59 *Id.*

60 *Id.*

61 *Id.*

62 *Id.*

63 *Commission Opinion, of 8.11.2019 on the Compatibility of National Asset Freezes Imposed by Member States with Union Law*, COM (2019) 8007 final (Aug. 11, 2019).

Russia has been asset freezing.[64] An EU asset freeze consists of two main components.[65] First, the European Union ensures that all funds and economic resources owned by the designated entities or individuals are immobilized.[66] Second, it forbids third parties from providing funds or economic resources, whether directly or indirectly, to listed entities.[67]

The European Union has consistently acknowledged and regulated nontraditional assets as part of financial instruments by adopting a broad definition of "funds" and "economic resources." Specifically, Article 1(g) of Council Regulation 269/2014 categorizes "funds" as encompassing all types of financial assets and benefits.[68] It describes "economic resources" as any asset potentially convertible into funds, goods, or services.[69] While cryptocurrencies are not explicitly mentioned in this definition, on October 6, 2022, the European Union introduced its eighth sanctions package against Russia, which explicitly forbids all transactions of "crypto-asset wallets, accounts, or custody services" with Russia or Russian persons, regardless of the wallet's value.[70]

Equating traditional payment service providers with crypto asset service providers is a predominant theme in Markets in Crypto-Assets ("MiCA"), a landmark crypto asset regulation.[71] Reflecting the disclosure requirements for traditional payment service providers, the European Union mandates that crypto asset service providers gather and reveal user information on the originator and beneficiary of the crypto asset transfers they facilitate.[72] This user information includes the

64 *See EU Sanctions Against Russia*, EURO. COUNCIL, https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/ (last visited Feb. 21, 2023).

65 *Commission Opinion*, *of 19.6.2020 on Article 2 of Council Regulation (EU) No. 269/2014*, at 4, COM (2020) 4117 final (June 19, 2020).

66 *Id.* at 1.

67 *Id*.

68 *See* Council Regulation (EU) No. 269/2014, Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine, art. 1(g), 2014 O.J. (L 78) 6.

69 *Id.* art. 1(d).

70 European Commission Press Release IP/22/5989, Ukraine: EU Agrees On Eighth Package Of Sanctions Against Russia (Oct. 6, 2022).

71 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, 2023 O.J. (L 150) 40 [hereinafter Regulation (EU) 2023/1114].

72 *See* Regulation (EU) 2023/1113, of the European Parliament and of the Council of 31 May 2023 on InformationAccompanying transfers of Funds and Certain

originator's name, distributed ledger address, crypto asset account number, residential address, official personal document number, identification number, and their date and place of birth.[73] The European Union introduced the famous "travel rule" as part of a provisional agreement on the proposals to strengthen the European Union's anti-money laundering and counter-terrorism financing rules, which were presented by the Commission on July 20, 2021.[74] The "travel rule" aims to ensure financial transparency in crypto asset exchanges by updating the regulations concerning information that accompanies fund transfers to include transfers of crypto assets.[75] As the name suggests, the "travel rule" requires the complete set of originator information, gathered by the crypto asset service providers, to "travel" with the crypto assets transfer, irrespective of the amount.[76]

Acknowledging the pseudo-anonymity and rapid transaction capabilities of crypto assets, this regulation asserts that all crypto transactions, irrespective of their amounts and whether they are domestic or international, are subject to the same requirements.[77] However, the decentralized nature of the blockchain technology that underlies cryptocurrencies allows users to move crypto assets without the intervention of a third-party payment service provider. Consequently, this pivotal regulation is only relevant for transactions involving crypto asset service providers.[78] In other words, if a transaction happens between two self-hosted wallets, it remains pseudo-anonymous; this means that, while the transaction is visible on the public ledger, the personal details of both the sender and the recipient remain concealed.

B. The United States' Sanctioning Actions

The regulatory landscape for digital assets continues to evolve, and recent enforcement actions by OFAC indicate a growing emphasis on ensuring sanctions compliance within the cryptocurrency sector.

Crypto-Assets and Amending Directive (EU) 2015/849, 2023 O.J. (L 150) 1 [hereinafter Regulation (EU) 2023/1113].

73 *Id.* at 19.

74 *See* Press Release, Eur. Council, Anti-Money Laundering: Provisional Agreement Reached on Transparency of Crypto Asset Transfers (June 29, 2022, 11:00 PM), https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [https://perma.cc/6UKP-666X].

75 *Id*.

76 *Id.*

77 *See id.*

78 *See id.*

Such emphasis includes taking actions against individuals and entities that have utilized cryptocurrency for illicit activities. For example, on March 2, 2020, OFAC sanctioned two Chinese nationals involved in laundering cryptocurrency stolen by a North Korean state-sponsored organization, Lazarus Group.[79] In 2018, Lazarus used a cyber-attack to steal $250 million worth of virtual currencies from a cryptocurrency exchange.[80] Two Chinese individuals received about $100 million and layered the funds in transactions to transfer $1.4 million worth of Bitcoin into prepaid iTunes gift cards.[81] More recently, on March 23, 2022, Lazarus carried out the largest virtual currency heist in history—worth almost $620 million—from a blockchain project linked to an online game.[82] OFAC immediately sanctioned virtual currency mixer Blender.io, which Lazarus used to process over $20.5 million of the illicit proceeds.[83]

OFAC clarifies that sanctions compliance obligations apply equally to transactions involving cryptocurrency and traditional currency.[84] Although OFAC has taken only two enforcement actions regarding cryptocurrency, each reflects how the department analyzes relevant factors to calculate a final civil monetary penalty. On December 30, 2020, OFAC entered into a $98,830 settlement with BitGo, Inc. for apparent violations of multiple sanctions programs related to digital currency transactions.[85] BitGo is a technology company based in California that offers non-custodial secure digital wallet management services.[86] Since 2015, BitGo processed 183 cryptocurrency transactions, totaling $9,127.79, on behalf of individuals who were located in sanctioned jurisdictions.[87] The base civil monetary penalty

79 *See Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, *supra* note 27.

80 *Id.*

81 *Id.*

82 *See* Press Release, U.S. Dep't of the Treasury, U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768 [https://perma.cc/HUG3-3HKV].

83 *Id.*

84 OFF. OF FOREIGN ASSETS CONTROL, *supra* note 13, at 1.

85 *See Settlement Agreement Between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitGo, Inc.*. U.S. DEP'T OF THE TREASURY, OFF. OF FOREIGN ASSETS CONTROL (Dec. 30, 2020), https://ofac.treasury.gov/recent-actions/20201230_33 [https://perma.cc/GFS3-BXPQ].

86 *Id.*

87 Enforcement Release, Dep't of the Treasury, OFAC Enters into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs

applicable in this matter was $183,000, but the settlement amount of $93,830 reflected OFAC's considerations of the totality of circumstances.[88] OFAC considered aggravating factors which included that BitGo had reason to know the location of these users based on IP addresses associated with the login devices and failed to voluntarily self-disclose the apparent violations.[89] OFAC also considered mitigating factors, such as BitGo's implementation of remedial measures, cooperation with OFAC's investigations, and retroactive screening of all users.[90]

On February 18, 2021, OFAC announced its second enforcement action related to cryptocurrency—a $507,375 settlement with BitPay, Inc., a technology company based in Atlanta, Georgia.[91] BitPay offers a payment processing platform for merchants to accept cryptocurrency as payment for goods and services.[92] While BitPay had location and IP information on customers in sanctioned jurisdictions, it failed to prevent them from engaging in $129,000 worth of cryptocurrency transactions on its platform.[93] Although BitPay has implemented sanctions compliance controls since 2013, the deficiencies in its compliance programs served as aggravating factors.[94] However, OFAC also considered remedial measures taken by BitPay, which largely reduced the base civil monetary penalty from $2,255,000 to $507,375.[95]

These two recent enforcement actions concerning cryptocurrency highlight OFAC's adherence to a strict liability standard when imposing civil monetary penalties. While blockchain technology ensures that every transaction is publicly and permanently recorded, users can still maintain partial anonymity. Consequently, companies in the

Related to Digital Currency Transactions (Dec. 30, 2020), https://ofac.treasury.gov/media/50266/download?inline [https://perma.cc/QTL4-8XH4].

88 *Id.*

89 *Id.*

90 *Id.*

91 *Settlement Agreement Between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitPay, Inc.*, U.S. DEP'T OF THE TREASURY, OFF. OF FOREIGN ASSETS CONTROL (Feb. 18, 2021), https://ofac.treasury.gov/recent-actions/20210218 [https://perma.cc/D2Z9-2KMG].

92 *Id.*

93 Enforcement Release, Dep't of the Treasury, OFAC Enters into $507,375 Settlement with BitPay, Inc. for Apparent Violations for Multiple Sanctions Programs Related to Digital Currency Transactions (Feb. 18, 2021), https://ofac.treasury.gov/media/54341/download?inline [https://perma.cc/EG8A-9RZY].

94 *Id.*

95 *Id.*

cryptocurrency sector might face liability, even if they are unaware that individuals in sanctioned regions are utilizing their services.

While OFAC handles the civil enforcement of sanctions violations, the DOJ is tasked with pursuing criminal violations. Under the IEEPA, a person can face criminal liability if they willfully engage in, attempt to engage in, conspire to commit, or aid or abet in the commission of an unlawful act.[96] In the wake of the massive sanctions placed on Russia, the DOJ has underscored its dedication to prosecuting willful sanctions violators by establishing the interagency Task Force KleptoCapture.[97]

The DOJ stated that part of KleptoCapture's mission is to "target[] efforts to use cryptocurrency to evade U.S. sanctions, launder proceeds of foreign corruption, or evade U.S. responses to Russian military aggression."[98] The DOJ's announcement of the task force not only indicates that numerous U.S. and international institutions with Russian clientele will be under intense scrutiny for sanction compliance, but also signifies that there will be criminal repercussions for those who circumvent sanctions.

On April 25, 2022, for example, the DOJ charged two European citizens with conspiring with a U.S. citizen to assist North Korea in evading U.S. sanctions by providing them with cryptocurrency and blockchain technology services.[99] According to court documents, Cao De Benos, the founder of the Korean Friendship Association, partnered with Christopher Emms, a cryptocurrency businessman, to jointly organize a cryptocurrency conference.[100] Two individuals presented blockchain technology and stated that the technology made it "possible to transfer money across any country in the world regardless of what sanctions or any penalties that are put on any country."[101] The DOJ also charged Virgil Griffith, who developed and funded cryptocurrency infrastructure in North Korea, with assisting sanction

96 50 U.S.C. § 1705(c).

97 *See* Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture (Mar. 2, 2022), https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture [https://perma.cc/BQW4-6W5U].

98 *Id.*

99 *See* Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Two European Citizens Charged for Conspiring with a U.S. Citizen to Assist North Korea in Evading U.S. Sanctions (Apr. 25, 2022), https://www.justice.gov/opa/pr/two-european-citizensCr-charged-conspiring-us-citizen-assist-north-korea-evading-us-sanctions [https://perma.cc/S5F9-Z3E9].

100 *Id.*

101 *Id.* (quoting Christopher Emms's own sales pitch).

evasion. A District Court Judge for the Southern District of New York sentenced him to over five years in prison and fined him $100,000.[102]

C. U.S. Court Opinions on Sanctions

While the U.S. executive branch appears determined to target parties that evade sanctions via cryptocurrency, OFAC's enforcement actions so far have been limited to settlements with cryptocurrency companies. As such, the executive branch's perspective on the relationship between cryptocurrency and sanctions enforcement has not yet faced scrutiny in an adversarial process.

On May 13, 2022, the U.S. District Court for the District of Columbia offered its perspective, affirming that the DOJ is authorized to press criminal charges against individuals who utilize cryptocurrency to circumvent U.S. sanctions.[103] U.S. Magistrate Judge Zia Faruqui explicitly stated that the court will substantially defer to OFAC's guidance.[104] In particular, the court cited precedent to indicate its "greater degree of deference than the *Chevron* standard" when reviewing OFAC's decisions.[105] While quoting OFAC's compliance guidance, Judge Faruqui emphasized that "sanctions compliance obligations *apply equally* to transactions involving virtual currencies and those involving traditional fiat currencies."[106]

This judgment not only validates the DOJ's efforts to criminally pursue sanctions violators, but it also marks the first instance in which federal courts have endorsed this type of enforcement. As Deputy Attorney General Lisa Monaco aptly stated, "sanctions [are] the new FCPA."[107] Monaco emphasized that sanctions enforcement is no

---

102 *See* Press Release, U.S. Dep't of Just., Off. of Pub. Affs., U.S. Citizen Who Conspired to Assist North Korea in Evading Sanctions Sentenced to over Five Years and Fined $100,000 (Apr. 12, 2022), https://www.justice.gov/opa/pr/us-citizen-who-conspired-assist-north-korea-evading-sanctions-sentenced-over-five-years-and [https://perma.cc/9TSU-FJY2].

103 *In Re:* Criminal Complaint, No. 22-mj-067-ZMF, 2022 WL 1573361, at *4 (D.D.C. May 13, 2022).

104 *Id.* at *3.

105 *Id.* (quoting Zarmach Oil Servs., Inc. v. U.S. Dep't of the Treasury, 750 F. Supp. 2d 150, 156 (D.D.C. 2010)).

106 *Id.* at *2 (quoting OFF. OF FOREIGN ASSETS CONTROL, *supra* note 13, at 1).

107 *Deputy Attorney General Lisa O. Monaco Delivers Keynote Remarks at 2022 GIR Live: Women in Investigations*, U.S. DEP'T OF JUST. OFF. OF PUB. AFFS. (June 16, 2022), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-remarks-2022-gir-live-women [https://perma.cc/87PW-Y7TE].

longer just the concern for banks and financial institutions.[108] Rather, sanctions enforcement is expected to grow dramatically, which follows the path of the meteoric rise of FCPA enforcement in the late 2000s.[109]

This case record is sealed, and the court redacted the name of the defendant and the sanctioned country at issue.[110] Nevertheless, since the court published the opinion on its website, it serves as a cautionary note. This signals that the judiciary concurs with the executive branch, including the DOJ and OFAC, that cryptocurrency falls under the purview of sanctions regulations. As Judge Faruqui stated in his opinion, "The Department of Justice can and will criminally prosecute individuals and entities for failure to comply with OFAC's regulations, including as to virtual currency."[111]

D. Sanctions: Compare and Contrast

Both the European Union and the United States prioritize the regulation of crypto asset payment service providers. Recognizing that blockchain technology inherently promotes decentralization, they are confronted with the issue that crypto users are normally anonymous.[112] Typically, only users who have registered their details on crypto asset payment service platforms can be identified and, consequently, subjected to governmental regulation.[113]

However, within the sanctions regime, the United States appears willing to apply a strict liability standard when imposing civil penalties on blockchain companies, which are not limited to crypto asset payment service providers.[114] Therefore, these blockchain-based companies should implement risk-based compliance programs that include OFAC-recommended know-your-customer programs that identify customers, monitor transactions, and mitigate risks while self-disclosing any potential violations. It remains unclear whether OFAC's enforcement action and compliance guidance are sufficient to detect and

108 *Id.*

109 *Id.*

110 *In Re: Criminal Complaint*, 2022 WL 1573361, at *1 n.1.

111 *Id.* at *4.

112 *See* Tad Simons, *Why the Crypto Economy Needs Stricter Anti-Fraud Protocols and Other Regulations*, THOMSON REUTERS (Oct. 11, 2022), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/crypto-anti-fraud-regulations/ [https://perma.cc/83HZ-6CCA].

113 *Id.*

114 *See* OFF. OF FOREIGN ASSETS CONTROL, *supra* note 13, at 6.

combat crypto use for sanction evasion. On March 2, 2022, Senator Elizabeth Warren (D-MA) wrote a letter to Treasury Secretary Janet Yellen inquiring into the Department's progress enforcing and monitoring sanctions compliance in the cryptocurrency sector.[115] In that letter, Senator Warren expressed her concern that OFAC "has not developed sufficiently strong and effective procedures for enforcement in the cryptocurrency industry."[116]

Senator Warren's concerns are mirrored in a report from the Congressional Research Service. This report highlights several potential tactics that Russia might employ to circumvent measures set by exchanges, including the use of anonymity-enhanced cryptocurrencies, un-hosted wallets, chain-hopping, and the utilization of mixers and tumbling services.[117] The report acknowledges that not all of these practices are deemed illegal and several are already encompassed within current regulatory frameworks.[118] However, these practices further obscure transactions from their associated real-world individuals, thereby increasing the challenges for relevant government agencies to identify wrongdoers.

Unlike OFAC's broad and somewhat ambiguous requirements for customer identification, new EU regulations mandate that crypto asset payment service providers disclose a comprehensive and detailed set of personal information about their users.[119] When the United States formulates its version of crypto-asset regulation, it should take inspiration from the European Union's model by demanding such detailed personal information from providers. For instance, by mandating the disclosure of users' country and address, OFAC could block users in sanctioned jurisdictions from using cryptocurrency to sidestep sanctions. By requiring an official identification document, OFAC could effectively prevent sanctioned individuals from using cryptocurrency to, directly or indirectly, access their frozen assets.

Notably, the European Union's "travel rule," which mandates that the complete set of the originator's personal information accompany the crypto-asset transfer, irrespective of the transaction amount, has garnered significant attention from crypto-asset payment service

115 Letter from Elizabeth Warren, Mark R. Warner, Sherrod Brown & Jack Reed to Janet Yellen, Sec'y of the Dep't of the Treasury, *supra* note 1.

116 *Id.* at 4.

117 For a detailed explanation of each practice, see KRISTEN E. BUSCH & PAUL TIERNO, CONG. RSCH. SERV., IN11920, RUSSIAN SANCTIONS AND CRYPTOCURRENCY 1-2 (2022).

118 *Id.* at 2.

119 *See generally* Regulation (EU) 2023/1113, *supra* note 72.

providers.[120] The foremost challenge in implementing this rule occurs when transactions take place between two self-hosted wallets without the involvement of crypto-asset payment service providers. To link a transaction to a real person, that individual's information must be documented within the transaction, essentially establishing a traceable "starting point."[121] Transactions between two self-hosted wallets, also known as peer-to-peer ("P2P") exchanges, are analogous to direct cash exchanges for items in person. However, the scale of crypto transactions can far exceed these direct cash exchanges. Thus, while current technology struggles to track such transactions, one viable approach to combat sanctions evasion and money laundering could be to bar corporations that handle sensitive materials (such as military equipment, nuclear substances, and other sanctioned commodities) from utilizing self-hosted wallets. If these sellers or corporations employ crypto-asset payment service providers, the burden then shifts to these service providers to execute rigorous know-your-customer measures to proficiently identify the self-hosted wallet buyers.

This travel rule contains no exception, however.[122] Critics question the efficacy of this requirement and express concerns over the safeguarding of data privacy.[123] It is anticipated that the Court of Justice of the European Union ("CJEU") will soon evaluate whether the travel rule represents an excessively broad surveillance mechanism for personal data.[124] U.S. regulators must weigh the benefits against potential costs when considering the adoption of European Union's crypto travel rule.

120 *See* Press Release, Eur. Council, Anti-Money Laundering: Provisional Agreement Reached on Transparency of Crypto Asset Transfers, *supra* note 74.

121 John Reed Stark, *Crypto-Traceability: Don't Believe The Hype*, LINKEDIN (Nov. 8, 2022), https://www.linkedin.com/pulse/crypto-traceability-dont-believe-hype-john-reed-stark/ [https://perma.cc/AG42-NURX].

122 *See* Press Release, Eur. Council, Anti-Money Laundering: Provisional Agreement Reached on Transparency of Crypto Asset Transfers, *supra* note 74 (noting that "the new agreement requires that the full set of originator information travel with the crypto-asset transfer, regardless of the amount of crypto assets being transacted").

123 Mikołaj Barczentewicz, *Why the EU's Rushed 'Travel Rule' for Crypto Should Be Struck Down*, COINDESK, https://www.coindesk.com/layer2/2022/07/25/why-the-eus-rushed-travel-rule-for-crypto-should-be-struck-down/ (May 11, 2023, 12:48 PM).

124 *Id.*

IV. ANTI-MONEY LAUNDERING

A. The European Union's Approach

In June 2023, the European Union passed a new regulation—Markets in Crypto-Assets ("MiCA")—to protect consumers against some of the risks associated with investment in crypto assets.[125] However, the rules do not affect crypto tokens without issuers, like bitcoin,[126] though trading platforms will need to warn consumers about the risk associated with the transactions in crypto assets.[127] Crypto asset service providers must abide by strong requirements to protect consumers' wallets[128] and be liable in case they lose investors' crypto assets.[129]

MiCA requires that the European Securities and Markets Authority ("ESMA"), in cooperation with the European Banking Authority ("EBA"), maintain a public register of non-compliant crypto asset service providers.[130] Crypto-asset service providers whose parent companies are based in countries on the European Union's high-risk list for anti-money laundering activities or on its list of non-cooperative jurisdictions for tax purposes, will be mandated to carry out intensified verifications in alignment with the EU AML framework.[131] Crypto providers likely disfavor MiCA because the regulation holds providers liable if they lose investors' crypto assets.

On June 29, 2022, despite the pending status of the proposals to strengthen the EU's anti-money laundering and counter-terrorism financing rules, presented by the Commission on July 29, 2021 ("EU AML/CTF rules of 2021"), negotiators from the Council Presidency and the European Parliament reached a provisional agreement on a proposal to update the rules on information accompanying fund transfers.[132] This update extended the scope of the travel rule in wire

125 *See* Regulation (EU) 2023/1114, *supra* note 71.

126 *See* Press Release, Eur. Parliament, Crypto Assets: Deal on New Rules to Stop Illicit Flows in the EU (June 29, 2022, 9:24 PM), https://www.europarl.europa.eu/news/en/press-room/20220627IPR33919/crypto-assets-deal-on-new-rules-to-stop-illicit-flows-in-the-eu [https://perma.cc/T2HP-YL8J].

127 Regulation (EU) 2023/1114, *supra* note 71, art. 66, ¶ 3.

128 *Id.* art. 37, ¶ 6(c).

129 *Id.* art. 75, ¶ 8.

130 *Id.* art. 141.

131 *Id.* art. 141(i).

132 *See* Press Release, Eur. Council, Anti-Money Laundering: Provisional Agreement Reached on Transparency of Crypto Asset Transfers (June 29, 2022), https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-

transfers to include transfers of crypto assets, ensuring increased financial transparency in crypto asset exchanges.[133]

The European Union obligates crypto asset service providers to collect and disclose information about the originator and the beneficiary of crypto asset transfers, mirroring the disclosure requirement present in fiat currency payment service providers.[134] This new travel rule would require crypto firms to report suspicious transactions to regulators,[135] aiming to aid in the crackdown on illicit money activities.[136]

MiCA and the revised Transfer of Fund Rules (Regulation (EU) 2023/1113) impose accountability on crypto asset service providers. The EU approach ensures customers' interests are being protected and incentivizes crypto companies to proactively comply with the strict regulations.

B. The United States' Approach

As outlined, FinCEN, a U.S. government agency, oversees matters related to money laundering, fraud, and other financial crimes. The AMLA grants FinCEN the authority to establish compliance regulations and standards aimed at combating money laundering activities.[137] FinCEN has sought comments on amendments to the travel rule, which involves collecting and sharing information concerning the senders and recipients of cryptocurrency transactions.[138]

FinCEN's recent enforcement actions on crypto asset service providers underscore its classification of virtual currency exchanges within the same regulatory framework as traditional money

laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [https://perma.cc/AW3Z-6EZH].

133 *Id.*

134 Regulation (EU) 2023/1113, *supra* note 72, ¶ 2.

135 *Id.* ¶ 47.

136 *See EU Backs Crypto Anti-Money Laundering Rules*, REUTERS (June 29, 2022, 6:55 PM), https://www.reuters.com/technology/eu-backs-crypto-anti-money-laundering-rules-crack-down-dirty-money-2022-06-29/ [https://perma.cc/ZHS9-JRDB].

137 LIANA W. ROSEN & RENA S. MILLER, CONG. RSCH. SERV., R47255, THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN): ANTI-MONEY LAUNDERING ACT OF 2020 IMPLEMENTATION AND BEYOND 23 (2022) (citing 31 U.S.C. § 5318A).

138 *See* Press Release, Fin. Crimes Enf't Network, Agencies Invite Comment on Proposed Rule Under Bank Secrecy Act (Oct. 23, 2020), https://www.fincen.gov/news/news-releases/agencies-invite-comment-proposed-rule-under-bank-secrecy-act [https://perma.cc/3G6P-N9A2].

transmitters.[139] On April 18, 2019, FinCEN imposed penalties on a peer-to-peer virtual currency exchange for contravening anti-money laundering regulations.[140] Eric Powers, who operated as a peer-to-peer exchanger of convertible virtual currency, was subject to a civil money penalty by FinCEN due to his failure to register as a money service business ("MSB").[141] Powers engaged in a significant number of suspicious transactions involving illicit darknet activities without submitting Suspicious Activity Reports ("SARs").[142] Additionally, he provided services to customers without implementing measures to ascertain their identities, the legitimacy of the funds, or whether they stemmed from unlawful sources.[143]

On October 19, 2020, FinCEN imposed a civil money penalty of $60 million on Larry Dean Harmon, the creator of Helix and Coin Ninja, a convertible virtual currency mixer.[144] This action was taken due to Harmon's violations of the Bank Secrecy Act and its associated regulations.[145] The company promoted its services on the darknet, offering customers a means to make anonymous payments for items such as drugs, firearms, and child pornography.[146] Helix managed a substantial volume of activity, encompassing over 1,225,000 transactions, more than $311 million in transfers, and at least 356,000 bitcoin transactions.[147]

The BSA requires financial institutions (including crypto exchangers) to proactively identify and manage risks of money laundering.[148] On August 10, 2021, FinCEN disclosed that it assessed a $100 million penalty against BitMEX, an unregistered future commission

139 *See* Press Release, Fin. Crimes Enf't Network, FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws(Apr. 18, 2019), https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money [https://perma.cc/N4J2-QD7W].

140 *See id.*

141 *Id.*

142 *Id.*

143 *Id.*

144 *See* Press Release, Fin. Crimes Enf't Network, First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws [https://perma.cc/ACP9-QKVA].

145 *Id.*

146 *Id.*

147 *Id.*

148 *AML Crypto: An AML Checklist For Cryptocurrency Exchanges*, ALESSA (Aug. 15, 2023), https://alessa.com/blog/aml-crypto-checklist/ [https://perma.cc/5KS8-3GDF].

merchant ("FCM"), for willful violation of the BSA.[149] BitMEX, one of the earliest and most prominent exchanges for convertible digital currency derivatives, neglected to establish adequate anti-money laundering and customer identification programs.[150] It also failed to report supicious activities, thereby exposing the U.S. financial system to significant risks.[151]

As detailed in Part II, the AMLA strengthens the obligations outlined in the BSA. In addition to requiring financial institutions to report suspicious activities to government authorities, the AMLA mandates that these institutions recognize and mitigate risks.[152] It also compels FinCEN to furnish financial institutions with information concerning financial crime trends and patterns.[153] Additionally, the AMLA requires FinCEN to periodically release a condensed overview of information related to SARs that have proven valuable to law enforcement efforts.[154] Recent enforcement actions indicate FinCEN's uniform treatment of cryptocurrency and traditional fiat currency under the AMLA.

On February 8, 2022, the DOJ underscored its determination to prosecute individuals employing cryptocurrency as a tool for executing white-collar offenses, when it unveiled indictments and filed charges against Ilya Lichtenstein and Heather Morgan. Lichtenstein and Morgan were accused of participating in a conspiracy to launder cryptocurrency that was stolen during the 2016 breach of Bitfinex.[155] Law enforcement seized over $3.6 billion in cryptocurrency linked to that hack.[156] In the press release following the arrest, the DOJ emphasized that it could follow money through the blockchain, and that it will not "allow cryptocurrency to be a safe haven for money

149 *See* Press Release, Fin. Crimes Enf't Network, FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act (Aug. 10. 2021), https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures [https://perma.cc/C6PF-7XDS].

150 *Id.*

151 *Id.*

152 31 U.S.C. § 310(d)(5)(B)(ii).

153 *Id.* at § 310(d)(5).

154 *Id.* at § 310(l)(2)(A).

155 *See* Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency (Feb. 8, 2022) [hereinafter DOJ Press Release, Two Arrested for Alleged Conspiracy], https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency [https://perma.cc/7K87-U8CP].

156 *Id.*

laundering."[157] Nevertheless, it is crucial to highlight that, in this instance, the DOJ effectively linked the illicit transactions to actual individuals. As detailed previously, although every transaction is permanently recorded and publicly accessible on the blockchain, law enforcement needs a "starting point" to trace unlawful transactions back to real individuals. In this case, Bitfinex served as the DOJ's "starting point." By meticulously tracking all the illicit transactions resulting from the hack, the DOJ successfully identified the participants involved in the money laundering scheme.[158] The DOJ was aided by a previous FBI shutdown of a darknet market called AlphaBay and the proliferation of anti-money laundering and know-your-customer protocols in the United States.[159]

C. U.S. Court Opinions on Money Laundering

In *United States v. Decker*, the defendant laundered money by utilizing the dark web, which permits vendors, working with unidentified marketplace administrators, to launder illicit proceeds through crypto transactions that conceal the funds' main metdata.[160] An analysis of the defendant's financial records showed that he had a bitcoin account and that most of his incoming bitcoin transactions within Coinbase originated from dark web markets.[161] The defendant "also admitted that he then [used] LocalBitcoins, a bitcoin exchange . . . to exchange bitcoin for fiat currency."[162]

To be guilty of money laundering in violation of 18 U.S.C. § 1956, a defendant must have:

> (1) knowingly conducted a 'financial transaction,' (2) which he knew involved funds that were the proceeds of some form of unlawful activity, (3) where the funds involved in the financial transaction in fact were the proceeds of a 'specified unlawful activity,' and (4) that the defendant engaged in the financial transaction knowing that the transaction was designed in whole or in part to conceal or disguise the nature,

157 *Id.*

158 Andrew R. Chow, *Inside the Chess Match that Led the Feds to $3.6 Billion in Stolen Bitcoin*, TIME (Feb. 10 2022, 7:55 AM), https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/ [https://perma.cc/7SVY-JCX8].

159 *Id.*

160 United States v. Decker, 832 Fed. Appx. 639, 643 (11th Cir. 2020).

161 *Id.* at 644.

162 *Id.* at 649.

> location, source, ownership, or control of the proceeds of such unlawful activity.[163]

The court in *Decker* found that the evidence was sufficient to satisfy all four elements and that the defendant laundered money.[164]

There are three key takeaways from this case. First, the court made it clear that courts will treat cryptocurrency the same as traditional fiat currency in matters pertaining to money laundering.[165] Second, the court rejected the defendant's assertion that the mere utilization of bitcoin fails to establish concealment, which is the fourth element of money laundering.[166] The court also stated that the utilization of bitcoin as a form of currency in itself does not necessarily imply involvement in a financial transaction linked to illegal undertakings.[167] The element of "concealment" may be met, however, when outgoing crypto transactions are consistently directed to a peer-to-peer exchange that is frequently utilized to obscure the source of crypto funds.[168] This obscurity is accomplished by anonymously trading crypto for fiat currency.[169] Lastly, in this case, the crucial "starting point" of the illegal activity occurred when the defendant sold drugs to an undercover DEA agent via the dark web.[170] Law enforcement initially identified the perpetrator and followed the trail of unlawful transactions, leading it to the records of the P2P exchange.[171] This suggests that numerous instances of money laundering through cryptocurrency might evade detection due to potential absence of suitable "starting points" from which law enforcement might initiate its investigations.

D. Flaws in U.S. Regulation

Though both the DOJ and the judicial branch have demonstrated their dedication to prosecuting crypto criminals engaged in money laundering through cryptocurrency, this commitment alone may be

163 *Id.* (citing United States v. Tarkoff, 242 F.3d 991, 994 (11th Cir. 2001)).
164 *Id.*
165 *See id.*
166 *Decker*, 832 Fed. Appx. at 649-50.
167 *Id.*
168 *Id.* at 650.
169 *Id.*
170 *Id.* at 643.
171 *Id.* at 643-44.

insufficient. "[F]ollow[ing] money through the blockchain"[172] can become significantly more intricate when individuals use P2P exchanges, which operate without a central intermediary or authority to facilitate asset transfers or collect customer information. Suppose that, unlike the defendant in *United States v. Decker*, a crypto criminal disguised their entire identity and did not attract law enforcement's attention. In this situation, P2P exchanges pose a formidable challenge to tracking unlawful activities, not solely due to the absence of a clear "starting point," but also because they render compliance with the Bank Secrecy Act nearly impossible. The rapid advancement of Web3, characterized by a decentralized and open internet structure featuring token-based economics, introduces a genuine risk of employing P2P exchanges to evade central intermediaries, such as traditional crypto exchange platforms, in money laundering endeavors.

Nevertheless, a clear conclusion can be drawn from the recent fraudulent and criminal cases involving crypto and the many unlawful actions undertaken by unidentified criminals that have long evaded detection. The United States' existing crypto regulations are inadequate, as they fail to safeguard consumers and prevent criminal activities.

V. AN IDEAL REGULATORY FRAMEWORK

A. U.S. Legislative Efforts on Crypto in 2023

The crypto industry in the United States is in dire need of comprehensive regulations that can alleviate investor concerns by establishing a clear position for cryptocurrencies within the U.S. financial framework and by outlining the specific roles each regulatory agency plays in the oversight. The United States has thus far relied on enforcement actions by various agencies to regulate the industry. However, these expansive and forceful enforcement efforts have inefficiently safeguarded investors and consumers and the absence of regulatory clarity has prompted established crypto enterprises to contemplate relocating outside the United States.[173]

172 DOJ Press Release, Two Arrested for Alleged Conspiracy, *supra* note 155.

173 *See* Sheila Chiang, *Ripple CEO Says More Crypto Firms May Leave U.S. Due to "Confusing" Rules*, CNBC (May 18, 2023, 1:35 AM), https://www.cnbc.com/2023/05/18/ripple-ceo-says-more-crypto-firms-may-leave-us-due-to-confusing-rules.html [https://perma.cc/YC5N-QC5Z].

As a result, three major fronts have emerged in U.S. crypto legislation in 2023.[174] Firstly, the Financial Innovation and Technology for the 21st Century Act ("FITA"), proposed by the House Committee on Agriculture and Financial Services, is a legislative effort focused on overseeing the cryptocurrency sector.[175] This bill aims to establish clear criteria for distinguishing whether a cryptocurrency should be categorized as a security or a commodity.[176] It also seeks to extend the regulatory scope of the Commodity Futures Trading Commission ("CFTC") over the cryptocurrency industry, concurrently providing clarification regarding the jurisdiction of the SEC.[177] Secondly, an Amendment concerning Crypto Asset Anti-Money Laundering was affixed to the National Defense Authorization Act of 2024 ("NDAA"),[178] though it was not ultimately enacted. This Amendment mandated that the Secretary of the Treasury formulate examination standards for crypto assets. The Amendment would facilitate the evaluation of how businesses adhere to sanctions requirements and prevent money laundering.[179] Notably, the Amendment mandated that the Secretary of the Treasury "establish a risk-focused examination and review process for financial institutions" to assess the "adequacy of reporting obligations and ani-money laundering programs" and "[c]ompliance . . . with anti-money laundering . . . requirements."[180] Lastly, the Blockchain Regulatory Certainty Act ("BRCA") clarifies that a blockchain service is not a money transmitter or a financial institution, unless it has control over digital assets "to which a user is

174 *See* Press Release, Fin. Servs. Comm., House Financial Services Committee Reports Digital Asset Market Structure, National Security Legislation to Full House for Consideration (July 26, 2023), https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=408940 [https://perma.cc/TB4L-ZN93].

175 *See* Financial Innovation and Technology for the 21st Century Act, H.R. 4763, 118th Cong. (2023).

176 *Id.*

177 *Id.*

178 *Lummis, Gillibrand Urge Inclusion of Bipartisan Amendment to Prevent Use of Crypto Assets in Illicit Transactions in Final NDAA*, CYNTHIA LUMMIS (Oct. 23, 2023), https://www.lummis.senate.gov/press-releases/lummis-gillibrand-urge-inclusion-of-bipartisan-amendment-to-prevent-use-of-crypto-assets-in-illicit-transactions-in-final-ndaa/ [https://perma.cc/3GH2-Q857] (this amendment did not ultimately make the NDAA's final cut).

179 National Defense Authorization Act for Fiscal Year 2024, H.R. 2670, 118th Cong. §§ 1099AAA, 1099BBB (2023), https://www.congress.gov/bill/118th-congress/house-bill/2670/text/eas (as reported by the Publishing Office on July 7, 2023, as "Engrossed Amendment Senate," including the Senate's proposed amendments).

180 *Id. at* 1099AAA.

entitled under the blockchain service . . . created, maintained, or disseminated by the blockchain developer."[181]

B. What the Regulation Ought to Be

This Note highly recommends adoption of FITA. The Note underscores the limitations of the SEC's "regulation by enforcement" approach, which falls short of adequately safeguarding consumers. Moreover, U.S. agencies' extensive enforcement actions have failed to reassure crypto companies and deterred them from conducting operations within the United States. FITA's significance lies in its capacity to address this challenge by establishing definitive jurisdiction for cryptocurrency regulation in the United States. This initial step is crucial in mitigating the uncertainty that causes anxiety among crypto companies and investors.

Though the AML Amendment was not enacted, Congress should pass an AML Amendment-like statute. In order to effectively counter white-collar crimes associated with cryptocurrencies, U.S. regulations need to address the challenge of traceability within the cryptocurrency realm. The AML Amendment to the NDAA aligns with the approach taken by the European Union by compelling crypto enterprises to establish compliance programs encompassing know-your-customer procedures. This strategy aims to enhance accountability and ensure adherence to regulatory standards within the crypto industry.[182]

Although OFAC imposes civil penalties on crypto companies that violate sanctions, with more severe penalties for those lacking a functional compliance program, OFAC does not currently require crypto companies to enforce KYC protocols. Implementing rigorous identity verification procedures during both registration and transactions can establish crucial "starting points" for law enforcement to successfully track illicit transactions. The European Union's "travel rule" further mandates that every transaction is associated with the identities of the parties involved. Nonetheless, unlike conventional financial systems and institutions, the decentralized nature of crypto platforms presents

181 Blockchain Regulatory Certainty Act, H.R. 1747, 118th Cong. § 2(a) (2023).

182 *See* Senate Amendment 712 to National Defense Authorization Act for Fiscal Year 2024, S. 2226, 118th Cong. (2023-2024), https://www.congress.gov/amendment/118th-congress/senate-amendment/712/text. The Amendment sought to enhance compliance with Subchapter II of Chapter 53 of Title 31, which, among other things, requires any financial institution that issues or sells monetary instruments, as prescribed by the Secretary, in amounts or denominations of $3,000 or more, to identify the individual involved. *See* 31 U.S.C. § 5325 (a).

challenges for safeguarding user information and privacy. U.S. regulators must evaluate whether existing privacy laws and technology are equipped to shield users' personal data from potential unauthorized access or theft.

The adoption of BRCA is advisable, but it should not restrict the application of KYC requirements. Instead, these requirements should be expanded to encompass Web3 and other blockchain-backed platforms and vendors. While BRCA states that only blockchain services holding digital assets should be regulated as financial institutions, it is important to recognize that cryptocurrency holds value not only in fiat currency but also in various blockchain-based commodities and platforms. Therefore, Congress should not confine KYC requirements solely to financial institutions.

Mandating KYC during customer onboarding and transactions will establish a trail of "starting points" for transactions on the platform and transactions on P2P exchanges. Requiring KYC for transactions would prevent anonymous crypto criminals from spending illicit funds or converting them into fiat currency. Current technology may not be capable of identifying two self-hosted wallets engaging in crypto asset exchanges via P2P, as their identities are not recorded on the blockchain. However, if KYC requirements are imposed on all blockchain-based platforms, crypto criminals will be identified by law enforcement or their unlawful funds will remain "frozen" in self-hosted wallets that refrain from interacting with any blockchain-based platforms.

Indeed, identity verification and KYC protocols play a pivotal role in preemptively curbing cybercriminal activities. Through both customer due diligence and extended customer due diligence measures, these processes establish essential layers of prevention. Legislation must obligate companies to implement stringent sanction screening for high-risk individuals and Politically Exposed Persons, who have a higher risk for potential involvement in money laundering. Where customers originate from sanctioned regions, legislation should require companies to decline transactions unless they can validate both the purchaser's and payer's identities. This approach reinforces the importance of accountability, security, and legality in financial transactions.

To ensure consumer protection against fraud and embezzlement, U.S. regulations should enforce upgrades in security systems for crypto platforms and companies. These enhancements should encompass features that alert users to potential hacking risks, including phishing attacks, and enable the reporting of suspicious transactions

to relevant government bodies. Additionally, imposing strict liability on crypto platforms and companies in civil cases of customer asset loss would reinforce accountability and encourage robust security measures, contributing to a safer and more secure environment for cryptocurrency users.

VI. CONCLUSION

The cryptocurrency frenzy that gained momentum in 2020 subsided within a mere two years, marked by the significant downturn known as "the crypto crisis" and the subsequent collapse of the world's largest cryptocurrency exchange.[183] Nevertheless, cryptocurrency platforms have remained havens for cybercriminal activities over the past few years. A report from the blockchain analytics firm Chainalysis in 2022 disclosed that approximately $900 million were laundered through decentralized finance ("DeFi") protocols in 2021, showcasing an astonishing increase of 1,964% from the previous year.[184] Illicit addresses received $14 billion during 2021, having increased almost twofold from the previous year.[185]

Following the 2008 financial crisis, Satoshi Nakamoto developed Bitcoin.[186] Nakamoto's philosophy is to create a decentralized currency that opts out of state-controlled financial systems, so it can be stable and immune to financial crises.[187] In 2022, sustained and heightened inflation compelled the Federal Reserve to embark on a vigorous campaign of interest rate hikes. This move triggered significant selloffs in cryptocurrencies and other high-risk assets.[188] The sharp decline in crypto prices led to the collapse of multiple crypto companies.[189] This is a far cry from Nakamoto's original dream—cryptocurrency not only fails to be immune from economic downturn, but it also requires government regulations to regain consumers' trust.

183 Candice Choi, *Crypto Crisis: A Timeline of Key Events*, WALL ST. J., https://www.wsj.com/articles/crypto-crisis-a-timeline-of-key-events-11675519887 (June 6, 2023, 10:32 AM).

184 CHAINALYSIS, THE 2022 CRYPTO CRIME REPORT 12 (Feb. 2022), https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf [https://perma.cc/FU2C-BMA8].

185 *Id.* at 3.

186 Julie Pinkerton, *The History of Bitcoin, the First Cryptocurrency*, U.S. NEWS & WORLD REP. (Mar. 21, 2024, 2:51 PM), https://money.usnews.com/investing/articles/the-history-of-bitcoin [https://perma.cc/75VP-JAHH].

187 *See id.*

188 *Id.*

189 *Id.*

The growing global appeal of cryptocurrencies attracts both legitimate customers and malicious actors. Cryptocurrency, like any form of finance, is built on the foundation of trust. For it to maintain its value over time, it must operate within a secure legal framework. While the European Union has enacted stringent regulations to oversee the crypto industry, the United States predominantly depends on enforcement actions by regulatory agencies. However, the considerable rise in crypto-related criminal activities in recent years has proven the U.S. approach inadequate.

Cryptocurrency criminals leverage the decentralized nature of blockchain to shield themselves through pseudonymous transactions. Even if law enforcement manages to identify these criminals, the immense cost of analyzing billions of transactions on a public ledger remains a substantial challenge. This Note advocates for the passage of the Financial Innovation and Technology for the 21st Century Act, a statute similar to the AML Amendment within the National Defense Authorization Act, and the Blockchain Regulatory Certainty Act. Additionally, this Note underscores the necessity of imposing KYC requirements on all blockchain-based platforms and vendors. While this may depart from Nakamoto's vision of a "government-less" blockchain, a well-regulated blockchain industry is crucial to safeguard crypto users and ensure the continued relevance of cryptocurrency in the future.