Crypto
Council for
Innovation

BY U.S. MAIL AND ELECTRONIC SUBMISSION

Himamauli Das
Acting Director, Financial Crimes Enforcement Network
Policy Division
P.O. Box 39
Vienna, VA 22183

February 13, 2022

RE: FinCEN Docket No. FINCEN-2021-0008, Response to FinCEN's Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime

Dear Acting Director Das,

The Crypto Council for Innovation ("CCI") appreciates the opportunity to comment on the Financial Crimes Enforcement Network's ("FinCEN") request for information ("RFI") regarding ways to "streamline, modernize, and update the anti-money laundering and countering the financing of terrorism ("AML/CFT") regime of the United States,"[1] specifically with respect to the Bank Secrecy Act and its implementing regulations (collectively, the "BSA").[2]

CCI is an alliance of crypto industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the cryptocurrency industry, including Andreesen Horowitz, Block (formerly Square), Coinbase, Fidelity Digital Assets, Paradigm, and Ribbit Capital. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of crypto to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI and its members stand ready and willing to work with FinCEN and other government agencies to accomplish these goals to ensure that the most transformative innovations of this generation and the next are anchored in the United States.

I. Introduction and Overview

CCI welcomes FinCEN's interest in modernizing AML/CFT regulation and strongly believes that the technological revolution of the last decade has made the current moment a unique opportunity to reexamine how the United States counters the threat of financial crime and to explore new ways to deploy technology to address emerging threats. Specifically, as

---

[1] Press Release, FinCEN, *FinCEN Seeks Comments on Modernization of U.S. AML/CFT Regulatory Regime* (Dec. 14, 2021), https://www.fincen.gov/news/news-releases/fincen-seeks-comments-modernization-us-amlcft-regulatory-regime; Review of Bank Secrecy Act Regulations and Guidance, 86 Fed. Reg. 71,201 (Dec. 15, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-15/pdf/2021-27081.pdf.

[2] The BSA is codified at 31 U.S.C. § 5311 *et seq.*, and the BSA implementing regulations are codified at 31 C.F.R. § 1010, *et seq.*

FinCEN embarks on the process of modernizing the BSA, it should consider how to harness the innovation that blockchain and other new technologies facilitate to accomplish the objectives of the BSA in novel ways that make law enforcement investigations more efficient while also better protecting individuals' security and privacy.

We commend FinCEN for embracing innovative approaches to financial crime compliance in a number of ways over the last several years. Embracing innovative approaches will undoubtedly lead to the provision of more, and better, financial products and services to a greater number of people, and, in turn, to broader financial inclusion and economic empowerment. By encouraging novel approaches to regulation, instead of imposing duplicative reporting requirements that focus on collecting sensitive personal data,[3] FinCEN can better protect privacy, make law enforcement efforts more effective, and ensure that the United States is not left out of the next generation of innovation in financial services.

Two areas offer particularly fertile ground for reevaluating the traditional approaches to AML/CFT activity: (i) how government and the private sector can identify and mitigate financial crime risk while bringing more people into the financial system; and (ii) the ways in which financial institutions verify customer identities.

Threat Identification. From the adoption of the BSA in 1970, the U.S. AML/CFT framework was grounded in the recognition that the private sector has important perspectives on, and an important role to play in identifying, illicit finance risks. The statute therefore imposed recordkeeping and reporting requirements that would facilitate the provision of information from financial institutions to the government under specified circumstances. Indeed, the main objective of the BSA was to require banks "to maintain prudent practices with respect to identification of their customers, reporting of unusual cash transactions, and general recordkeeping,"[4] in order to provide information that is "highly useful" to "criminal, tax, or regulatory investigations" or to "intelligence or counterintelligence activities."[5] With respect to blockchain-based transactions, however, much of this data is *already* publicly available. Thus, a new paradigm of compliance should focus on creating mechanisms for the public and private sectors to leverage technology to *utilize* this publicly available information – rather than requiring duplicative, burdensome reporting.

While a paradigm of threat identification grounded in financial institution recordkeeping and reporting requirements is important, in an era where cryptocurrency transactions take place over public ledgers, there are more effective ways for the public and private sectors to identify and mitigate risk. Specifically, instead of a model of threat identification focused solely on investigating individuals and groups through subpoenas or other requests for specific records held by financial institutions (much of which may already be publicly available on the blockchain), the threat identification paradigm in blockchain-based environments should focus

---

[3] *See* Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 3,897 (proposed Jan. 15, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2021-01016.pdf.

[4] 115 Cong. Rec. 36,769, 36,770 (Dec. 3, 1969) (statement of Rep. Patman).

[5] 31 U.S.C. § 5311(1).

on the identification of typologies, tactics, and techniques of financial crime based on blockchain data. These efforts can leverage the comparative advantages of the private sector in blockchain and data analytics, and the government's comparative advantages in threat-related intelligence, to develop typologies and risk indicators that can be broadly disseminated throughout the industry to enhance threat identification and suspicious activity reporting, particularly by smaller financial institutions in the blockchain ecosystem.

Identity Management. Similarly, the Treasury Department came, over time, to impose requirements under the BSA for financial institutions to verify the identities of their customers.[6] These requirements mandate that every financial institution at which a customer opens an account collect and verify the same information previously collected and verified by every other financial institution at which the customer holds an account, causing costly duplication of effort. New technologies and methodologies for verifying and managing identity can make this process more effective and more efficient, opening the financial services industry to a broader range of actors that can deliver services to new individuals and communities, including those historically excluded from the financial sector because established institutions have not been able or willing to serve them. These new methods could potentially protect customer information more effectively and provide ways to verify identity for those who may lack access to traditional government issued IDs (or whose information is not available in the commercial databases typically used to verify identity). They could also reduce the amount of personal information potentially vulnerable to release in the event of a breach, thus protecting privacy and security. FinCEN and the federal banking regulators have begun the process of encouraging financial institutions to embrace innovation in identity management,[7] but work should continue to encourage accelerated innovation in this space.

---

[6] *See* Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090 (May 9, 2003), https://www.govinfo.gov/content/pkg/FR-2003-05-09/pdf/03-11019.pdf, and Customer Identification Programs for Broker-Dealers, 68 Fed. Reg. 25,113 (May, 9, 2003), https://www.govinfo.gov/content/pkg/FR-2003-05-09/pdf/03-11017.pdf (requiring banks and broker-dealers, respectively, to implement reasonable procedures to verify the identity of any person seeking to open an account, maintain records of the information used to verify the person's identity, and determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations).

[7] *See, e.g.*, Board of Governors of the Federal Reserve System ("FRB"), Federal Deposit Insurance Corporation ("FDIC"), FinCEN, National Credit Union Administration("NCUA"), and Office of the Comptroller of the Currency ("OCC"), Interagency Statement on Sharing Bank Secrecy Act Resources (Oct. 3, 2018), https://www.fincen.gov/sites/default/files/2018-10/Interagency%20Statement%20on%20Sharing%20BSA%20Resources%20-%20%28Final%2010-3-18%29%20%28003%29.pdf; FRB, FDIC, FinCEN, NCUA, OCC, Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018), https://www.fincen.gov/sites/default/files/2018-12/Joint Statement on Innovation Statement (Final 11-30-18)_508.pdf; Press Release, FinCEN, *FinCEN to Host Innovation Hours Program Workshop on Digital Identity Services and Technologies* (Aug. 31, 2021), https://www.fincen.gov/news/news-releases/fincen-host-innovation-hours-program-workshop-digital-identity-services-and#:~:text=WASHINGTON%E2%80%94The%20Financial%20Crimes%20Enforcement,that%20undermine%20the%20integrity%20and; Press Release, FinCEN, *FDIC and FinCEN Launch Digital Identity Tech Sprint* (Jan. 11, 2022), https://www.fincen.gov/news/news-releases/fdic-and-fincen-launch-digital-identity-tech-sprint.

A. *Technology and the Current Moment*

It is particularly important for FinCEN, and the broader U.S. regulatory community, to take up this work now because we sit today at the convergence of two significant developments.

First, cryptocurrencies, and blockchain-based technology more broadly, are disrupting a wide and expanding range of economic activity. Born in the aftermath of the financial crisis, cryptocurrencies and the blockchain represent the simple but powerful idea that individuals should be able to store value and engage in economic exchange without having to use only centralized institutions to execute transactions. Because blockchain-based transactions are recorded on public ledgers, the paradigm of recordkeeping and reporting established by the BSA can be supplemented by enhanced analysis of publicly available blockchain transactional data to identify and curtail illicit activity. These approaches could complement the identity verification measures already taken by banks and other exchanges at the on and off ramps that bridge the cryptocurrency and fiat currency worlds. Compliance capabilities have also benefited from significant technological advancements in recent years. In particular, the rise of data analytics and artificial intelligence (along with related applications like machine learning and natural language processing) has improved general AML compliance potential.[8]

Second, similar technological developments can be used to manage and verify identities more securely, obviating the need to create large repositories of personally identifiable information ("PII") at financial institutions that can be hacked or misused, empowering customers, and increasing the efficiency and effectiveness of identity verification throughout the financial sector.

The economic impact of meeting this technological moment will be significant. By the end of 2022, the number of crypto users is expected to break one billion for the first time,[9] and the rise of cryptocurrency is poised to improve the lives of underprivileged communities. The World Bank reports that close to one-third of adults, 1.7 billion people, remain unbanked,[10] and cryptocurrency has already demonstrated the potential to change this landscape for the better. Crypto's lower barriers to entry and "low cost, nearly instantaneous, borderless, peer-to-peer transfers of actual value,"[11] creates an unparalleled opportunity to bolster financial inclusion by helping underserved communities worldwide access the financial system.

---

[8] *See* Financial Action Task Force (FATF), Opportunities and Challenges of New Technologies for AML/CFT (July 2021), https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.

[9] *Global Crypto Owners Near 300 Million, Predicted to Hit 1 Billion by the End of 2022*, Crypto.com (Jan. 19, 2022), https://blog.crypto.com/global-crypto-owners-near-300-million-predicted-to-hit-1-billion-by-the-end-of-2022.

[10] *See* World Bank, Financial Inclusion, Overview, https://www.worldbank.org/en/topic/financialinclusion/overview#1 (last visited Feb. 10, 2022).

[11] Andreesen Horowitz, The web3 Landscape at 10 (Oct. 2021), https://a16z.com/wp-content/uploads/2021/10/The-web3-Readlng-List.pdf.

Underbanked communities in the United States, particularly those comprising minority populations, have shown a particular interest in crypto,[12] a trend recently recognized by the Acting Comptroller of the Currency, Michael Hsu. When describing crypto's appeal to these communities, Hsu noted the fact that "37 percent of the underbanked indicated they own cryptocurrency, compared to 10 percent of the fully banked."[13] Several members of Congress have also recently remarked on cryptocurrency's ability to bring traditionally underbanked individuals into the financial system.[14] For many of these underbanked and minority communities, the traditional financial system has generally not been tailored to their financial needs.[15] In comparison, cryptocurrency, with its decentralized infrastructure and ease of access, provides a much-needed alternative for these individuals to take control of their financial present – and future.[16] Crypto therefore has the potential to democratize finance and expand access and ownership opportunities for these individuals and communities.

While the United States has been at the forefront of many of these developments, the current uncertain regulatory climate that developers face in the U.S. is poised to drive overseas

---

[12] *See e.g.*, Silvia Foster-Frau, *Locked Out of Traditional Financial Industry, More People of Color Are Turning to Cryptocurrency*, Wash. Post (Dec. 1, 2021), https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa-37fe-11ec-9bc4-86107e7b0ab1_story.html; Kori Hale, *Why Black Investors Seemingly Prefer Cryptocurrencies Over Traditional Stocks*, Forbes (Aug. 10, 2021), https://www.forbes.com/sites/korihale/2021/08/10/why-black-investors-seemingly-prefer-cryptocurrencies-over-traditional-stocks/?sh=16d66c906839.

[13] Michael J. Hsu, Acting Comptroller, OCC, *Remarks Before the BritishAmerican Business Transatlantic Finance Forum Executive Roundtable: "The Future of Crypto-Assets and Regulation"* (Jan. 13, 2022), https://www.occ.treas.gov/news-issuances/speeches/2022/pub-speech-2022-2.pdf.

[14] *See e.g.,* Sam Sutton, *Four Takeaways From the House Stablecoin Hearing*, PoliticoPro (Feb. 8, 2022) ("Several Republicans and some Democrats urged caution against cracking down on privately backed digital tokens that have become a resource for underbanked communities. New York Democratic Reps. Ritchie Torres and Gregory Meeks noted that Black and Hispanic communities have moved more quickly to embrace crypto and decentralized finance platforms as a form of financial services."); Kollen Post, *What We Learned at Congress' Much-Anticipated Summit of Crypto Execs,* The Block (Dec. 8, 2021), https://www.theblockcrypto.com/post/126866/what-we-learned-at-congress-much-anticipated-summit-of-crypto-execs ("[S]everal Democrats who entered the committee this year seemed more interested in crypto's potential positive impacts. Rep. Ritchie Torres asked the witnesses how stablecoins could help the large immigrant population in his district in the South Bronx facilitate cheaper remittances.").

[15] Samuel Haig, *Minority Communities Are Investing in Crypto to Escape Financial Discrimination*, Cointelegraph (Aug. 17, 2021), https://cointelegraph.com/news/minority-communities-are-investing-in-crypto-to-escape-financial-discrimination.

[16] Cryptocurrency also has the potential to reduce the cost of remittances, especially low-value remittances, the average cost of which the World Bank has pegged at 6.3%. *See* World Bank, Remittance Prices Worldwide, Quarterly, Issue 39, at 5 (Sept. 2021), https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q321.pdf. Technologies such as Celo, which offers a consumer-facing mobile application that integrates with a native stablecoin platform, enables remittances to be confirmed in seconds and securely transferred, allowing for faster, cheaper, and more energy efficient cross-border transactions. *See* Evan Kereiakes, *Rethinking Remittances with Blockchain Technology and Celo*, Celo Blog (May 28, 2020), https://medium.com/celoorg/rethinking-remittances-with-blockchain-technology-720c978084d4.

the next generation of blockchain-based applications. Indeed, because of the inherently global nature of blockchain technology, this risk is particularly acute in the cryptocurrency context. Regulation that is not sensitive to the unique dynamics of cryptocurrency, combined with the "de-risking" of U.S. financial institutions in developing regions, can also have a significant impact on U.S. national security as U.S. companies become less predominant in the cryptocurrency space.[17]

Specifically, as described in this letter, productive relationships between crypto financial institutions and law enforcement agencies are critical to mitigating financial crime risk, but those relationships, and the exchanges of information they facilitate, may be put at risk if crypto financial institutions move offshore. This is because crypto financial institutions are required to collect information about their customers both at onboarding and throughout the lifecycle of the customer relationship. Law enforcement agencies can combine this information, obtained with subpoenas or other forms of lawful process, with information obtained from the blockchain to identify specific perpetrators of illicit activity. To the extent crypto financial institutions move overseas, the ability of U.S. law enforcement agencies to obtain expediently the pieces of the puzzle that cannot be obtained from public blockchains will likely be reduced commensurately, to the detriment of the U.S. law enforcement and national security communities. Just as the U.S. benefits from the fact that large global telecommunications, Internet, and social media companies are headquartered here, U.S. law enforcement—and thus the American people—will lose out if cryptocurrency financial institutions leave the United States or are never established here in the first place.

The absence of U.S. firms from the cryptocurrency payments space can also leave voids that could be filled by other payments technologies, like China's Digital Yuan project, which has the potential to fundamentally reshape the global payments ecosystem in a way that will undoubtedly be detrimental to U.S. interests.

In the face of global competition, U.S. regulators have an opportunity to counteract these trends, and help realize the promise of crypto. While the economic benefits of keeping cryptocurrency companies in the United States are obvious, it is also a tremendous advantage to U.S. national security and law enforcement to ensure that the cutting edge of innovation remains in this country.

B. *The AMLA, Public-Private Partnerships, and Identity Management*

Congress recognized the potential for technology to transform the U.S. AML/CFT regime in the Anti-Money Laundering Act of 2020 ("AMLA").[18] Title LXII of the AMLA in particular focuses on modernizing the AML/CFT system—the topic of this RFI—and contains several sections relating to leveraging technology and innovation to improve the effectiveness and

[17] ClearingHouse, A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement (Feb. 2017), https://bpi.com/wp-content/uploads/2018/07/20170216_tch_report_aml_cft_framework_redesign.pdf.

[18] The AMLA is contained in Div. F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, Div. F, 134 Stat. 3388, 4547 (2021).

efficiency of the current AML/CFT framework.[19] We encourage FinCEN to capitalize on this pivotal moment and reimagine how to conduct core BSA activities consistent with the spirit of the statute and the possibilities that now exist.

In Part II of this comment letter, we focus on how FinCEN and the private sector can develop novel mechanisms of threat identification, which go beyond recordkeeping and reporting requirements, and leverage public and private resources to develop typologies and risk indicators of financial crime that can be disseminated throughout the industry. In Part III, we explain why FinCEN should encourage the adoption of novel approaches to identity management. Collectively, these approaches can reduce financial crime risk while better protecting customer privacy.

In the half-century since the adoption of the BSA, the U.S. AML/CFT regime has evolved to adapt to changing threats and changing opportunities. By leveraging technology to improve threat identification, and adopting novel approaches to identity management, the U.S. can set the tone for how governments and transnational bodies manage financial crime risk globally for the next generation.

II. FinCEN Should Foster Innovative Frameworks to Identify and Mitigate Financial Crime Risk Related to Blockchain-Based Transactions.

The original intent of the BSA of 1970 was to mitigate money laundering risk by instituting a set of preventative measures that put financial institutions on the front lines of the fight against financial crime. At the outset of the statutory regime, the BSA centered on ensuring banks maintained the requisite records to provide information that is "highly useful" to government investigations and that banks submitted reports on otherwise-ephemeral cash transactions. The BSA has since been refreshed periodically to address new threats through new mechanisms of a regime fundamentally grounded in recordkeeping and reporting; examples include formal Suspicious Activity Report ("SAR") requirements and, after 9/11, Sections 314(a) and 314(b) of the USA PATRIOT Act.

The explosive growth of cryptocurrencies marks another inflection point and can facilitate a new, and improved, mechanism to identify and mitigate financial crime risk. Specifically, because blockchains are generally public and reveal transaction histories, it is possible to analyze those transactional records to identify typologies of high-risk behavior, specific high-risk addresses, risk indicators, and the tactics and techniques that illicit actors use

[19] *See e.g.,* AMLA, § 6207 (adding a Subcommittee on Innovation and Technology to the BSAAG to advise FinCEN and other federal and state regulators on how to most effectively encourage and support technological innovation in the area of AML/CFT and reduce any obstacles to innovation that may arise from existing regulations); *id.* § 6208 (establishing Bank Secrecy Act Innovation Officers to advise public and private sector stakeholders on innovative methods, processes, and new technologies that may assist with AML/CFT compliance and provide technical assistance and guidance regarding their implementation); *id.* § 6209 (requiring standards by which financial institutions must test the new technologies); *id.* § 6210 (requiring FinCEN to conduct an analysis of the impact of the new technologies on financial crimes compliance); *id.* § 6211 (establishing a global financial crimes tech symposium focused on how the new technologies can be used to more effectively combat financial crimes and other illicit activities).

to launder ill-gotten funds (like the ways in which ransomware actors "hop" among multiple blockchains to attempt to hide the proceeds of their criminal activity)[20] on the basis of publicly available information,[21] while mitigating impacts on privacy.

Private sector actors are generally well-positioned to leverage their expertise in blockchain analytics to identify this activity and can combine it with specific intelligence from government agencies about threats to ensure the work is maximally impactful. Working together, government and the private sector can develop typologies of illicit activity that can be shared among a broad range of participants in the blockchain ecosystem to ensure that even smaller financial institutions can have up-to-date information to identify and prevent emerging illicit threats. And, importantly, because this kind of preventive risk management is less dependent on recordkeeping and reporting, it poses fewer privacy challenges. SARs remain a vital law enforcement tool, and we envision a regime to complement and support SARs by sharing threat typologies and risk indicators widely across members of the blockchain industry subject to the BSA to help ensure those SARs are impactful by permitting financial institutions to situate the activity they are seeing in the context of broader threats.

The power of blockchain data to provide information about transactions is especially noteworthy when viewed in light of recent proposals to expand the scope of suspicionless reports like Currency Transaction Reports ("CTRs") to require reporting of certain transactions between cryptocurrency exchanges and self-hosted wallets.[22] Traditional CTRs may have been appropriate when they related exclusively to cash transactions, information about which would have been lost if not captured contemporaneously. But, as described in this letter, much of the information about transaction histories that would have been required by recent proposals to expand CTR requirements, such as the date and time, amount, source and destination wallet address of transactions, and transaction hash, is *already* available on blockchains.[23] This

---

[20] This practice is often referred to as "chain hopping"—a practice often used by illicit actors to obfuscate the origin of their funds by converting one cryptocurrency into a different cryptocurrency at least once before moving the funds to another service or platform. *See* FinCEN, Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 (Oct. 2021), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

[21] For example, the Statement of Facts released in connection with the two arrests made for an alleged conspiracy to launder cryptocurrency stolen during the Bitfinex hack in 2016 includes a number of statements about the government's reliance on public blockchain data to identify the alleged perpetrators. U.S. Dep't of Justice, Statement of Facts at 2 & n.7 (Feb. 7, 2022), https://www.justice.gov/opa/press-release/file/1470211/download ("U.S. authorities traced the stolen funds on the BTC blockchain," which is "a public transaction ledger that includes a record of every BTC transaction that has ever occurred").

[22] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83,840 (proposed Dec. 23, 2020) ("NPRM"), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf; *see also* 86 Fed. Reg. 3,897 (Jan. 15, 2021) (reopening comment period) ("January NPRM"), https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2021-01016.pdf; 86 Fed. Reg. 7,352 (Jan. 28, 2021) (extending comment period), https://www.govinfo.gov/content/pkg/FR-2021-01-28/pdf/2021-01918.pdf.

[23] *See* Coinbase Comment, Dkt. No. FINCEN-2020-0020 (Mar. 25, 2021), https://www.regulations.gov/comment/FINCEN-2020-0020-8248.

reality means proposals to report this data to FinCEN are duplicative and unnecessary, while at the same time posing serious privacy and security risks to consumers.

To the extent recent proposals related to CTRs requested information not directly available on blockchains, like the "name and physical address of each counterparty to the transaction of the financial institution's customer,"[24] FinCEN's proposal to collect and retain that data in large government repositories, as opposed to simply mandating that financial institutions retain those records internally, poses serious privacy and security concerns. Such concerns are especially sharp with respect to CTR requirements that would link a person's PII with their blockchain addresses, which, if accessed without authorization, could reveal their entire blockchain transaction history. That proposal also used the same $10,000 threshold for cryptocurrency CTRs without fully considering the differences between cryptocurrency and cash transactions. This makes particularly clear that simply grafting traditional recordkeeping and reporting requirements onto the blockchain is at best inappropriate – an unlawfully obtained fiat currency CTR is unlikely to reveal a customer's entire financial history, but an unlawfully leaked crypto CTR linking a person's real identity with his or her blockchain address could have significant privacy and security consequences.

In light of these concerns, FinCEN and the rest of the U.S. regulatory community should prioritize the development of systems to identify illicit financial activity that leverage the unique properties of publicly available blockchain data, instead of expanding existing reporting requirements in a manner that poses significant privacy and security concerns without commensurate benefits. Doing so will not only give law enforcement agencies better tools but will also free up compliance resources at cryptocurrency exchanges to focus on important value-added activities, like SAR investigations, and is consistent with a "risk-based approach to AML/CFT regulation" that will mark a departure from the status quo.[25]

A. *The Foundations of the Modern Recordkeeping and Reporting System*

A core insight of the BSA is that the private sector has an inherent comparative advantage in recognizing certain forms of suspicious activity. The modern AML system, where financial institutions must report certain categories of transactions through CTRs and SARs, in particular, is rooted in the idea that "the creation of a meaningful system for detection and prevention of money laundering is impossible without the cooperation of financial institutions,"[26]

---

[24] January NPRM, 86 Fed. Reg. at 3,899.

[25] Himamauli Das, Acting Director, FinCEN, *Prepared Remarks of FinCEN Acting Director Him Das, Delivered Virtually at the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference* (Jan. 13, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-him-das-delivered-virtually-american-bankers.

[26] *See* FinCEN; Proposed Amendment to the Bank Secrecy Act Regulations—Requirement of Money Transmitters and Money Order and Traveler's Check Issuers, Sellers, and Redeemers to Report Suspicious Transactions, 62 Fed. Reg. 27,900, 27,901 (proposed May 21, 1997) (finalized on Mar. 2, 2000), https://www.govinfo.gov/content/pkg/FR-1997-05-21/pdf/97-13303.pdf (proposing to amend the BSA regulations to require money transmitters, and issuers and sellers of money orders to report suspicious transactions to further the "creation of a comprehensive system . . . for the reporting of suspicious transactions," *id.* at 27,900).

because "it is representatives of financial institutions, rather than law enforcement, who see the money launderers first."[27] Moreover, "because money laundering transactions are designed to appear legitimate in order to avoid detection,"[28] bank "officials . . . are more likely than government officials to have a sense as to which transactions appear to lack commercial justification or otherwise cannot be explained as falling within the usual methods of legitimate commerce."[29]

Because the government understood that financial institutions were often better positioned than official agencies to identify suspicious transactions, it followed that financial institutions should be required to retain records about those transactions and to report them to the government. The specific regulatory requirements that implement this core idea and govern the private sector's role have evolved over time.

1. *BSA Recordkeeping and Reporting Requirements*

In 1970, the BSA imposed recordkeeping requirements and required the filing of reports for certain types of transactions. The statute noted that records of the identities of accountholders,[30] and of cash transactions,[31] which were by nature ephemeral, were of particular value because "[r]eports of domestic currency transactions will be quite helpful in limiting the use of secret foreign financial facilities for illegal purposes. These reports will also facilitate domestic law enforcement transactions . . . If certain cash transactions are required to be reported to the Treasury Department, law enforcement agencies, particularly in the income tax field, will have a useful tool in their investigations and proceedings. "[32]

2. *Suspicious Activity Reports*

In 1992, the Annunzio-Wylie Anti-Money Laundering Act granted the Treasury broad authority to require financial institutions to report suspicious transactions.[33] Pursuant to this authority, a "single integrated system" was created that reflected, among other things, the "mutual desire" of Treasury and financial regulators to "simplify and reduce the burdensomeness of the reporting process," while "increas[ing] the effectiveness of counter-

---

[27] FinCEN, Advisory, *Court Interprets "Safe Harbor" Provisions*, (Aug. 1, 1996), https://www.fincen.gov/resources/advisories/fincen-advisory-issue-5.

[28] 62 Fed. Reg. at 27,901; *see also* Proposed Amendment to the Bank Secrecy Act Regulations—Requirement to Report Suspicious Transactions, 60 Fed. Reg. 46,556, 46,558 (proposed Sept. 7, 1995), https://www.govinfo.gov/content/pkg/FR-1995-09-07/pdf/95-22223.pdf.

[29] 62 Fed. Reg. at 27,901.

[30] Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, § 101, 84 Stat. 1114, 1114-15 (1970).

[31] Currency and Foreign Transactions Reporting Act, § 221.

[32] 116 Cong. Rec. 16,949, 16,954 (May 25, 1970) (remarks of Rep. Patman).

[33] Annunzio-Wylie Anti-Money Laundering Act, Pub. L. No. 102-550, tit. XV, § 1517(b), 106 Stat. 3672, 4059-60 (1992).

money laundering efforts."[34] Over time, FinCEN expanded SAR requirements to other types of financial institutions, including, among others, money services businesses ("MSBs").[35]

3. *Information Sharing under 314(a) and 314(b)*

In response to the 9/11 attacks, Congress adopted the USA PATRIOT Act, aimed at combatting terrorism more effectively. Sections 314(a) and 314(b) of that statute inaugurated a new paradigm in information sharing to fight money laundering and terrorist financing. Each provision facilitates the flow of information among relevant participants in the financial ecosystem – between government and financial institutions under 314(a), and on a voluntary basis among financial institutions under 314(b).

Taken together, these components of the BSA—SAR and CTR reporting, along with 314(a) and 314(b)—establish a recordkeeping and reporting regime that originated in the context of fiat currency transactions. As noted above, however, the blockchain obviates the need for reporting on certain types of data, and as explained further below, it also opens new opportunities for government and the private sector to identify threats and risks in a way that is scalable and often immediate.

B. *The Blockchain Informational Advantage*

Certain types of reports, like high-value SARs, will always be important to the identification and mitigation of financial crime. But blockchain technology unlocks new potential forms of threat identification based on the same foundational idea that history demonstrates has always animated BSA information reporting processes: the private sector has unique insight about risks that are valuable and important to the government in combating criminal activity. In the blockchain era, it will remain the case that "[n]o system for the reporting of suspicious transactions can be effective unless information flows *from* as well as *to* the government."[36] But the ways in which public and private sector efforts leverage their comparative advantages to fight financial crime should be adapted to the unique advantages of blockchain technology.

The AML regime should therefore be augmented with structures to facilitate the identification of threat typologies and risk indicators, with an eye toward sharing them broadly to prevent financial crime. This approach would leverage the unique properties of the blockchain, on which all transactions are generally publicly available. And as cryptocurrency applications proliferate, an increasing portion of economic activity will likely take place on publicly observable blockchains. Just as in the past, where the government recognized that the private sector has the unique capacity to identify suspicious activity, hosted wallet providers and cryptocurrency exchanges, in partnership with others such as blockchain analytics firms, may today be better positioned than government to develop techniques to analyze activity on the blockchain, and to identify specific typologies of illicit activity. The government, by contrast, may have access to a broader range of information that can be used to confirm the identities of individual wallet-

[34] 60 Fed. Reg. at 46,558.

[35] *See* 31 C.F.R. § 1022.320.

[36] 60 Fed. Reg. at 46,559.

holders involved in potentially suspicious activity, and to inform an analysis of financial crime trends. Therefore, it is critical for the government to work in partnership with the private sector to establish the necessary "feedback loop[s]" for threat identification and mitigation that Acting Director Das has said is one of FinCEN's goals.[37]

There are a range of possibilities for the specific shape novel frameworks to identify and mitigate financial crime risk with respect to blockchain-based technologies could take, but below we describe key principles any such regime should embrace. A structure that leverages the strengths of the public and private sectors fueled by modern data analytics and the blockchain would be powerful and could complement existing mechanisms of information-sharing like 314(a), 314(b), and SARs, which are, by their nature, retrospective. The AMLA took an important step in the right direction by mandating the creation of a Subcommittee on Innovation and Technology in the Bank Secrecy Act Advisory Group ("BSAAG"),[38] tasked with encouraging and supporting technological innovation.[39] The statute also required the Secretary of the Treasury to convene a group of public and private sector experts "to examine strategies to increase cooperation between the public and private sectors for purposes of countering illicit finance," which can be leveraged for these purposes.[40]

C. *Threat Identification – Core Principles*

A framework for threat identification aimed at the specific challenge of identifying and mitigating financial crime risk in blockchain-based transactions should be constructed with reference to a set of core principles. These kinds of partnerships should: (i) focus on typology development and rapidly disseminate those typologies and threat indicators across the industry and to global Financial Intelligence Unit ("FIU") partners; (ii) harness the power of technology; and (iii) leverage the full range of available administrative structures.

Importantly, this kind of framework will make it easier for law enforcement agencies to engage in global investigations quickly—a significant improvement over investigative capabilities with respect to fiat currency transactions today. At present, law enforcement agencies must rely on legal processes like subpoenas to gain access to transactional records held at financial institutions. Collecting and analyzing these records takes time, even when the transactions occur domestically at financial institutions that have been identified. If transactions related to criminal activity took place through financial institutions abroad, obtaining the records through Mutual Legal Assistance Treaty ("MLAT") requests can take months or years, if they yield relevant records at all.

---

[37] Das, *supra* note 25.

[38] The BSAAG was established pursuant to Section 1654 of the Annunzio-Wylie Anti-Money Laundering Act of 1992, as a means by which the Treasury receives advice on the BSA. The Director of FinCEN serves as the chair of BSAAG and is responsible for ensuring that relevant issues are placed before the BSAAG for review, analysis, and discussion. Annunzio-Wylie Anti-Money Laundering Act, § 1564(a)-(b).

[39] AMLA, § 6207.

[40] AMLA, § 6211.

With cryptocurrency, the history of wallet addresses is available for law enforcement to analyze—and even to seize directly, as the Department of Justice recently did with the proceeds of the Bitfinex hack, unraveling "a labyrinth of cryptocurrency transactions" on the path to a significant prosecution.[41] The approach we propose in this letter also allows law enforcement to invert the typical investigative process, and start by identifying high-risk transactions on the blockchain (*e.g.*, a wallet that interacted with a known criminal network), and to work from there to identify the individuals involved in the activity. Law enforcement agencies do not need to wait for SARs to be filed to pursue bad actors. And during the course of ongoing investigations, law enforcement agents can use blockchain records to identify additional persons and entities with whom the subjects transacted, wherever in the world they may be, without waiting on MLAT requests that may or may not be granted.

These possibilities illustrate the power of devoting public and private sector resources to developing structures to fully utilize the potential of blockchain-based records, instead of imposing reporting requirements on cryptocurrency exchanges that cover records that are already available publicly.

Develop typologies that can be disseminated broadly. As noted above, core BSA structures were designed to require recordkeeping and reporting to support government investigations of individuals, entities, and networks. These requirements, especially as they relate to SARs, are and will remain important. But they should be supplemented with alternative structures that leverage unique properties of blockchains to reduce financial crime risk.

While in some circumstances these structures could be used to advance individual investigations—and, as noted above, to identify high-risk wallet addresses—these structures would be designed to create the tools to empower cryptocurrency financial institutions to more effectively identify indicators of specific types of financial crime risk. These may include typologies of criminal activity that would illustrate, for example, how bad actors use techniques like "chain-hopping" to obfuscate the links between specific crypto assets and unlawful activity.

These typologies and tools can broadly promulgate information to a wide range of actors in the crypto ecosystem so they can monitor for such activity on their networks. This approach would complement efforts to interdict the particular perpetrators of specific criminal acts and would help facilitate the development of a broad cohort of financial institutions equipped with the ability to identify and interdict illicit activity that interacts with their platforms. This approach would also permit smaller financial institutions to benefit from the work of these partnerships even if they lack the resources to participate directly. And focusing on typologies also has the salutary effect of buttressing consumer privacy because the focus would not be on collecting and reporting information about individual financial institution customers.

These kinds of partnerships can also allow rapid iteration of typology development as threats emerge, based on information that originates either with the government or with the private sector. They can also leverage FinCEN's power to connect with its global FIU partners

[41] Press Release, U.S. Dep't of Justice, *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency* (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

to expand the exchange of financial intelligence that is relevant to the development of the kinds of impactful typologies discussed here.[42]

Harness the power of technology. This type of work is enabled by the nature of the blockchain—purposefully designed to create an immutable record of transactions—which allows for open-source traceability and accountability of each transaction, regardless of the identity or location of the participants. Records of fiat currency transactions have traditionally been siloed at financial institutions, but because the transactions that take place on the blockchain are public, new tools can be used to analyze those transactions on an aggregated basis to identify typologies and threats.

In the past decade, compliance technology also has developed rapidly, with quantum leaps made in areas such as data analytics, artificial intelligence, and machine learning, which can help to better identify risks and communicate, monitor, and address suspicious activity.[43] These technologies are evolving at a rapid pace. The ideal mechanism would therefore leverage the comparative advantages of public and private to marry the government's information about threats and bad actors with the private sector's expertise in analytics, and access to additional types of information about transactions and relationships.

Leverage a range of administrative frameworks. This effort will depend not only on new substantive approaches to financial crime threat mitigation, but also on new administrative structures for doing so. FinCEN has long had the authority to grant exceptive relief from its regulations,[44] and to provide administrative rulings on the implications of proposed activity under the BSA.[45] FinCEN has also recently published a report noting that it should embark on a rulemaking process to adopt a framework to grant no-action relief.[46] And several U.S. states have developed regulatory sandboxes to help facilitate the incubation of new ways to provide

---

[42] *See* FinCEN, The Egmont Group of Financial Intelligence Units, https://www.fincen.gov/resources/international/egmont-group-financial-intelligence-units (last visited Feb. 11, 2022) (describing the Egmont Group as an international networks of FIUs designed to "improve communication, information sharing, and training coordination amongst its FIU members" and which supports its FIU members by "helping them to expand and systematize the exchange of financial intelligence and information, improve expertise and capabilities of personnel, and enable secure communication with one another").

[43] FATF, Opportunities and Challenges of New Technologies for AML/CFT (July 2021), https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.

[44] 31 U.S.C. § 5318(a)(7); 31 C.F.R. § 1010.970(a).

[45] FinCEN has the authority to issue administrative rulings interpreting regulations promulgated under the BSA pursuant to 31 C.F.R. § 1010.710. For a list of published administrative rulings, *see* FinCEN, Administrative Rulings, https://www.fincen.gov/resources/statutes-regulations/administrative-rulings (last visited Feb. 11, 2022).

[46] FinCEN, Assessment of No-Action Letters in Accordance with Section 6305 of the Anti-Money Laundering Act of 2020 (June 28, 2021), https://www.fincen.gov/sites/default/files/shared/No-Action%20Letter%20Report%20to%20Congress%20per%20AMLA%20for%20ExecSec%20Clearance%20508.pdf.

financial services.[47] One can envision the use of these authorities to create novel structures that combine features of, for example, 314(a) and 314(b) to facilitate the development and dissemination of typologies and risk indicators.

D. *Examples of Public-Private Partnerships*

There are several extant frameworks that could serve as a model for what we propose, but FinCEN should leverage the structures described above, including the BSAAG and the consultation structure required by the AMLA, to consult with industry on how to establish these kinds of mechanisms.

NCFTA. The National Cyber-Forensics and Training Alliance ("NCFTA")—a Pittsburgh-based non-profit organization focused on identifying, mitigating, and neutralizing cybercrime threats globally—is one potential model for the type of public-private partnership we envision. NCFTA was initially established by the Federal Bureau of Investigation ("FBI") in 1997 and operates through strategic alliances and partnerships with subject matter experts in the public, private, and academic sectors.[48] NCFTA focuses on enabling "near real-time"[49] information sharing among members—some of which have staff permanently located at NCFTA—and fostering close collaboration among law enforcement, the private sector, and academia.

As the FBI describes it, the NCFTA essentially works as an early-warning system that leverages the power of real-time information sharing.[50] For example, a major banking institution that discovers a new kind of malware attacking its network can disseminate that information to other NCFTA members, which can then develop strategies to mitigate the threat. FBI agents and analysts from NCFTA can also use the information to open new or support existing investigations, often in concert with law enforcement partners globally. This model encourages not only information sharing between the government and the private sector, but also among private sector partners themselves.[51] Between 2015 and 2021, NCFTA produced 26,945

---

[47] Multiple states have launched a "regulatory sandbox" for innovative financial products or services, including Arizona, Nevada, Utah, Florida, West Virginia, Hawaii, and North Carolina. *See e.g.*, Ariz. Rev. Stat. Ann. §§ 41-5601 *et seq.*; S.B. 161, 2019 Leg., 80th Sess. (Nev. 2019) (pending statutes); Utah Code Ann. §§ 13-55-101 *et seq*; Fla. Stat. Ann. § 559.952; W. Va. Code Ann. §§ 31A-8G-1 *et seq.*; Press Release, Gov. David Y. Ige, *DCCA News Release: Hawaii Launches First Sandbox for Digital Currency* (Mar. 17, 2020), https://governor.hawaii.gov/newsroom/latest-news/dcca-news-release-hawaii-launches-first-sandbox-for-digital-currency; N.C. Gen. Stat. § 169-1 *et seq*.

[48] *The NCFTA: Combining Forces to Fight Cyber Crime*, FBI News (Sept. 16, 2011), https://www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime.

[49] *See* NCFTA, About Us, https://www.ncfta.net/home-2/about-us (last visited Feb. 6, 2022).

[50] *The NCFTA: Combining Forces to Fight Cyber Crime*, FBI News (Sept. 16, 2011), https://www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime.

[51] Christopher Wray, Dir., FBI, *The FBI and the Private Sector: Battling the Cyber Threat Together* (Jan. 28, 2021), https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-battling-the-cyber-threat-together-012821.

intelligence reports and referred 4,184 cases to law enforcement, ultimately resulting in the prevention of $12.25 billion in financial losses.[52]

JMLIT. The United Kingdom's Joint Money Laundering Intelligence Taskforce ("JMLIT") is another innovative public-private partnership, established in 2015, that can serve as a reference for the type of public-private partnership we propose. JMLIT is a partnership between law enforcement and financial institutions to exchange information relating to money laundering and wider economic threats. JMLIT members include financial institutions, the Financial Conduct Authority (the United Kingdom's principal financial regulatory body), Cifas (a United Kingdom fraud prevention organization), and various law enforcement agencies.

A particularly strong feature of JMLIT is its mechanism for public-private information sharing, which is actively used by law enforcement agencies to enhance their access to financial intelligence, facilitate interagency cooperation, and enhance their understanding of the ever-evolving money laundering landscape. Through JMLIT, law enforcement agencies can obtain information from multiple sources and quickly develop a comprehensive intelligence picture.[53] While JMLIT access is only granted to certain financial institutions, it has developed alerts that are distributed to the wider industry and non-JMLIT banks have filed SARs based on information learned from these alerts.[54]

Through its Operations Group, JMLIT facilitates weekly meetings among law enforcement agencies and financial institution representatives, supporting more iterative/real-time interactions. Private sector members of JMLIT are also encouraged to refer cases to the Operations Group using an information sharing gateway which complements the mandatory obligations imposed by the SAR filing regime. Since 2015, JMLIT has supported more than 950 law enforcement investigations and contributed to more than 280 arrests and the seizures or restraints of more than £86 million. In particular, JMLIT's private sector members have identified more than 7,400 suspicious accounts and commenced more than 6,000 internal investigations.[55]

III. FinCEN Should Encourage Novel Approaches to Identity Management

Identity management is another area in which evolving technology can help accelerate changes to BSA processes. Traditionally, the core manifestation of the regulatory expectation that a financial institution must Know Your Customer ("KYC") was the Customer Identification Program ("CIP"). The policy rationale behind KYC and CIP is simple: financial institutions must know with whom they are dealing by obtaining and verifying customer information, including

---

[52] *See* NCFTA, Home, https://www.ncfta.net (last visited Feb. 6, 2022).

[53] FATF, *Mutual Evaluation Report for United Kingdom's Anti-money Laundering and Counter-terrorist Financing Measures* (Dec. 2018), https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf.

[54] *Id.*

[55] *See* National Crime Agency, NECC, Joint Money Laundering Intelligence Taskforce, https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre (last visited Feb. 11, 2022).

name, date of birth, address, and personal identification number (*e.g.*, taxpayer identification number),[56] to mitigate money laundering and terrorist financing risk.[57]

But, at present, and with some notable exceptions, financial institutions must each collect and verify this information independently on customers who establish accounts across multiple institutions. And they must do so using the same basic framework that has been in place since the advent of CIP requirements. Indeed, Congress has noted the need for "anti-money laundering, countering the financing of terrorism, and sanctions policies . . . that . . . do not unduly hinder or delay legitimate access to the international financial system for underserved individuals, entities, and geographic areas[.]"[58] The persistence of these challenges is particularly troubling given that technology has evolved significantly, and we have access to additional data and tools to verify identity efficiently and effectively.[59]

FinCEN should therefore help encourage novel approaches to identity management, including the use of blockchain technology, and the use of shared services and platforms, consistent with the forward-leaning, innovative solutions FinCEN and the FDIC are seeking to foster in their tech sprint on digital identity.[60]

Novel approach to storing and proving identifying information. FinCEN should consider encouraging the exploration of novel approaches to identity management that would permit financial institutions to meet the policy objective behind KYC and CIP requirements while allowing financial institutions to increase effectiveness and efficiency and better protect consumers' personal information.

FinCEN specifically could establish a process to evaluate the way novel mechanisms can be used to create and maintain digital identity records, including (but not limited to) the adoption of digital identity verification techniques that can use a combination of decentralized blockchain-based technologies and secure "off-chain" data repositories. Specifically, there are tools under development that can allow digital identity information to be stored securely, and that use digital markers or tokens to enable the persons whose identity information is requested to confirm for a financial institution at onboarding that their identity *has been* verified, without

---

[56] *See* 31 C.F.R. § 1020.220(a)(2)(i)(A).

[57] *See* FinCEN; Customer Identification Programs for Certain Banks (Credit Unions, Private Banks and Trust Companies) That Do Not Have a Federal Functional Regulator, 67 Fed. Reg. 48,299, 48,302 (July 23, 2002), https://www.govinfo.gov/content/pkg/FR-2002-07-23/pdf/02-18193.pdf ("Obtaining sufficient information to verify a customer's identity can reduce the risk that a bank will be used as a conduit for money laundering and terrorist financing.").

[58] AMLA, § 6215(a)(8).

[59] *See, e.g.,* FATF, Digital Identity (Mar. 2020), http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf (broad discussion of evolving technologies available to facilitate digital identity management).

[60] FDIC, FDITECH, Measuring the Effectiveness of Digital Identity Proofing for Digital Financial Services, https://www.fdic.gov/fditech/techsprints/measuring-effectiveness.html (last visited Feb. 11, 2022) ("What is a scalable, cost-efficient, risk-based solution to measure the effectiveness of digital identity proofing to ensure that individuals who remotely (i.e., not in person) present themselves for financial activities are who they claim to be?").

providing the sensitive PII itself. This provides a mechanism for a customer to control the dissemination of information about his or her identity, thus better protecting privacy, while also enabling access to financial services.[61]

There are even more novel ways of confirming identities without revealing identities that are under development through the use of zero-knowledge proofs and other sophisticated forms of encryption.[62] These technologies would allow a customer to confirm that she is who she says she is, without revealing her specific identity. Doing so would be accomplished by the customer leveraging a token or other digital marker that only she possesses that would confirm she has unique access to a particular body of identifying information that is stored in encrypted form. This approach to identity management could potentially supplement existing CIP mechanisms that require the dissemination of large amounts of PII to numerous financial institutions. And it could do so while allowing individuals to keep their PII private and safe from theft or manipulation.

With time, many of the techniques described here could also incorporate non-traditional forms of identifying information (*e.g.*, mobile device identifiers) that would facilitate access to financial services for those who may lack government-issued photo IDs. While these technologies are likely a long way away from maturity, now is the time to allow experimentation and testing of these types of products to incentivize research into how they may scale over time.

Leverage shared services and shared platforms and collaboration among financial institutions. FinCEN should also further encourage financial institutions to leverage shared services and shared platforms in conducting identity management. On October 3, 2018, FinCEN and the federal banking regulators—FRB, FDIC, NCUA, and OCC—issued the *Interagency Statement on Sharing Bank Secrecy Act Resources* (the "2018 Interagency Statement"). Congress endorsed this approach in the AMLA, expressly encouraging financial institutions to enter the types of arrangements described in the statement.[63] The 2018

---

[61] Traditionally, a user must register for an account for every service provider. Each service provider serves as the central authority for managing user identity. With novel identity management frameworks, the user can receive credentials proving identity from multiple issuers, such as government agencies, universities, and employers, and store them in a digital wallet. When a need for identity verification arises, the user can then present proofs of their identity to any company that requests it and these companies can verify the proofs are true. *See e.g.,* CAPCO, Decentralized Identity: How Digital Transformation and Distributed Ledger Technology is Disrupting KYC (2020), https://www.capco.com/-/media/CapcoMedia/Capco-2/PDFs/Decentralized_Identity_Disrupting_KYC.ashx; Darren Shou, *How Decentralized Identity Is Reshaping Privacy for Digital Identities*, Forbes (Dec. 10, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/12/10/how-decentralized-identity-is-reshaping-privacy-for-digital-identities/?sh=247c3e6e3226.

[62] Howard Wu, *How the Coming Privacy Layer Will Fix the Broken Web*, Future (June 15, 2021), https://future.a16z.com/a-privacy-layer-for-the-web-can-change-everything/; Pamela Dingle, *Advancing Privacy with Zero-Knowledge Proof Credentials*, Microsoft: Identity Standards Blog (July 22, 2020), https://techcommunity.microsoft.com/t5/identity-standards-blog/advancing-privacy-with-zero-knowledge-proof-credentials/ba-p/1441554.

[63] *See* AMLA, § 6213 ("[i]n order to more efficiently comply with the requirements of this subchapter, 2 or more financial institutions may enter into collaborative arrangements, as described in the statement entitled 'Interagency Statement on Sharing Bank Secrecy Act Resources'").

Interagency Statement was published "to address instances in which banks may decide to enter into collaborative arrangements to share resources to manage their [BSA] and [AML] obligations more efficiently and effectively."[64] FinCEN and the federal banking regulators defined collaborative arrangements as "two or more banks with the objective of participating in a common activity or pooling resources to achieve a common goal. Banks use collaborative arrangements to pool human, technology, or other resources to reduce costs, increase operational efficiencies, and leverage specialized expertise."[65] The 2018 Interagency Statement recognized that, although each financial institution faces a unique set of threats and risks, there are efficiencies to be gained by collaborating—including potentially in "reviewing and developing risk-based customer identification and account monitoring processes."[66]

More can be done, however, to build on the 2018 Interagency Statement. Regulators indicated that "[c]ollaborative arrangements as described in this statement generally are most suitable for banks with a community focus, less complex operations, and lower-risk profiles for money laundering or terrorist financing."[67] However, any financial institution that properly manages the risk of adopting an innovative approach to identity management should be able to do so, which would free resources to manage other financial crime compliance activities.

Identity management and CIP are precisely the kinds of requirements that the ideas embodied in the 2018 Interagency Statement could helpfully address because each financial institution at which a customer opens an account must collect and verify information identical to that previously collected and verified by the other financial institutions at which the customer has opened an account—a duplication of effort that can be reduced. Indeed, this type of approach to relying on data not contained at the relevant financial institution has historical precedent, as the BSA has permitted certain financial institutions to rely on the CIP of another financial institution in certain circumstances.[68] And a recent Government Accountability Office report on de-risking mandated by the AMLA noted the potential for shared KYC utilities to increase banking access for vulnerable groups, like humanitarian organizations and MSBs that cater to cross-border transfers.[69] It should be noted that FinCEN has not yet formally expanded the concept of reliance to MSBs—a category of financial institution that includes many cryptocurrency companies—but such an expansion could be warranted.

---

[64] FRB, FDIC, FinCEN, NCUA, OCC, Interagency Statement on Sharing Bank Secrecy Act Resources at 1 (Oct. 3, 2018), https://www.fincen.gov/sites/default/files/2018-10/Interagency%20Statement%20on%20Sharing%20BSA%20Resources%20-%20%28Final%2010-3-18%29%20%28003%29.pdf.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *See, e.g.,* 31 C.F.R. § 1020.220(a)(6).

[69] U.S. Gov't Accountability Office, GAO-22-104792, Bank Secrecy Act: Views on Proposals to Improve Banking Access for Entities Transferring Funds to High-Risk Countries at 29-31 (Dec. 2021), https://www.gao.gov/assets/gao-22-104792.pdf,

Customer due diligence. A final area where blockchain technology will play an important role is with respect to customer due diligence. As described above, transactional histories are generally publicly available on blockchains for analysis. It will be increasingly important for financial institutions of all types to leverage the information about transaction history that is available through blockchain forensic tools. These kinds of tools can identify transactions with high-risk counterparties or other kinds of high-risk activities and will be an indispensable component of customer due diligence on an ongoing basis.

IV. Conclusion

The last decade has witnessed unprecedented dynamism in the ways financial products and services are delivered, largely as a result of the development of blockchain technology. As FinCEN reexamines the BSA, it faces an opportunity to similarly reimagine how AML compliance processes take place. One of the core ways it can do so is by supplementing the BSA's paradigm of recordkeeping and reporting with new frameworks for the public and private sectors to identify and mitigate financial crime risks. Anchored in the comprehensive public record of transactions recorded on the blockchain, and enabled by advances in forensic tools to analyze those records, the public and private sectors have opportunities to employ novel approaches to identify and disseminate typologies of illicit finance threats. Similarly, blockchain technology and advanced cryptography have the potential to reinvent identity management and customer due diligence while protecting privacy and making those processes more effective. We look forward to continuing to collaborate with FinCEN to accomplish these shared objectives.

Respectfully submitted,

/s/ Sheila Warren

Sheila Warren

Chief Executive Officer

Crypto Council for Innovation