November 3, 2022

Via Electronic Submission

Scott Rembrandt
Deputy Assistant Secretary
U.S. Department of the Treasury
Office of Terrorist Financing and Financial Crimes
1500 Pennsylvania Avenue, NW
Washington, DC 20220

RE: Request for Comment – "Ensuring Responsible Development of Digital Assets" (87 FR 57556)

Dear Mr. Rembrandt:

The Independent Community Bankers of America ("ICBA")[1] welcomes the opportunity to provide feedback on the U.S. Treasury Department's ("Treasury") Request for Comment on Ensuring Responsible Development of Digital Assets.

ICBA and its members appreciate Treasury's engagement with the banking industry and the American public to fulfill the directives outlined in President Biden's Executive Order on Ensuring Responsible Development of Digital Assets (the "Request").[2] Community banks are committed to providing products and services that enable their customers and communities to benefit from advances in financial technology. Hence, ICBA welcomes the opportunity to engage with policymakers to assess the illicit finance concerns of the digital assets market.

---

[1]*The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.*

With nearly 50,000 locations nationwide, community banks constitute roughly 99 percent of all banks, employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding nearly $5.9 trillion in assets, over $4.9 trillion in deposits, and more than $3.5 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org

[2] President Joseph R. Biden, Jr., "Executive Order on Ensuring Responsible Development of Digital Assets" (March 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

Community banks are at the forefront of responsible innovation in financial services as they seek new ways to serve their customers and provide technologies and experiences that support the 21st century economy. Advocates for digital assets - ranging from cryptocurrencies like bitcoin to various tokenized assets - represent that they can provide new ways to increase speed, efficiency, and transparency in financial services for consumers and businesses. However, we are alarmed by the growing use of cryptocurrencies to facilitate ransomware, money laundering, sanctions evasion, and other criminal activity. Additionally, ICBA has serious concerns about the potential for disintermediation of traditional financial services by stablecoins and decentralized finance ("DeFi") - a result which could negatively impact and disrupt the nation's financial system as a whole.

Executive Summary

ICBA closely monitored significant events in the crypto markets this year, especially the catastrophic failure of the algorithmic stablecoin TerraUSD. Community bankers are increasingly alarmed by the risks presented by digital assets, including scams, misrepresentations to consumers, and a growing potential for these digital assets to threaten the financial stability of the traditional banking sector. ICBA worked with its members to solicit feedback for this response, and we have identified the following as the most critical areas for the Treasury Department to consider as it examines the challenges posed by the use of digital assets for illicit activities:

- Broader use of cryptocurrency, without accompanying regulation or oversight, allows financial crimes and threats to national security to proliferate. Therefore, protecting national security and implementing anti-crime measures should be primary drivers of cryptocurrency policymaking and regulation.

- ICBA and its members support cross-agency collaboration to establish a clear regulatory framework for digital assets.

- ICBA believes that stablecoin issuance should be limited to insured depository institutions to address serious risks to financial stability, consumer protection, and national security.

- ICBA calls upon regulators to move swiftly on a comprehensive framework that will address the shadow banking activities of unregulated platforms to protect the financial system.

- ICBA urges Treasury to give appropriate weight to our staunch opposition to a Central Bank Digital Currency ("CBDC").

- A CBDC would not yield benefits more effectively than alternative methods in the market today. Creating a CBDC would introduce risks without providing benefits to households, businesses, and the overall economy.

Background

Soon after the launch of bitcoin in 2009, bad actors quickly realized how the technology could be used to evade detection from law enforcement and regulators and conduct illicit activities in dark corners of the web. Among the first to explore cryptocurrency's illicit uses was Dread Pirate Roberts, otherwise known as Ross Ulbricht, who used bitcoin to facilitate payments on the dark web marketplace called Silk Road.[3] Although law enforcement succeeded in their efforts to shut down Silk Road, new threats continue to emerge as developers create new methods to obscure cryptoasset transactions and cybercriminals become more experienced with their use. In the years since, bad actors have found novel ways to use cryptoassets for illicit activities, including the recent claims that Chinese spies used the privacy wallet known as Wasabi Wallet to obfuscate bitcoin payments.[4] Americans are frequently targeted by a range of crypto-related scams that have added up to more than $1 billion in losses since last year.[5] Unfortunately, this year appears to be on track to set a new record for losses due to an increased number of attacks against DeFi protocols.

ICBA and community banks are increasingly alarmed by the growing use of cryptoassets for various unlawful activities. From processing ransomware payments to laundering money, the rapid acceleration of the digital asset ecosystem challenges the current legal and regulatory structures and processes to monitor, detect, and prosecute criminal activity. These actions can result in real harm to the people and communities that community banks serve, as evidenced the Colonial Pipeline cyberattack last May that disabled critical infrastructure and triggered severe gas shortages on the east coast.[6]

ICBA and its members have devoted considerable time and resources to studying the cryptoasset technologies to consider the potential benefits and risks. ICBA has been an active participant in policymaker debates on Capitol Hill, as demonstrated by our recent letter to the House Financial Services Committee that expressed community bankers' concerns about potential stablecoin

---

[3] David Adler, *Fordham Journal of Corporate & Financial Law*, "Silk Road: The Dark Side of Cryptocurrency" (February 21, 2018), https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/#_edn4.

[4] Tom Robinson, Elliptic, "Chinese Spies Used Wasabi Wallet Mixer to Pay Bitcoin Bribes to FBI Double Agent" (October 24, 2022), https://hub.elliptic.co/analysis/chinese-spies-used-wasabi-wallet-mixer-to-pay-bitcoin-bribes-to-fbi-double-agent/.

[5] Emma Fletcher, Federal Trade Commission, "Reports Show Scammers Cashing in on Crypto Craze" (June 3, 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

[6] Joe Carroll, Andres Guerra Luz, and Jill R. Shah, *Bloomberg*, "Gas Stations Run Dry as Pipeline Races to Recover From Hacking" (May 8, 2021), https://www.bloomberg.com/news/articles/2021-05-09/u-s-fuel-sellers-scramble-for-alternatives-to-hacked-pipeline.

legislation.[7] ICBA also provided statements to Congress urging lawmakers to oppose the creation of a CBDC.[8]

ICBA Comments

Through its extensive community bank network, ICBA frequently engages its members to evaluate how community banks are exploring digital assets to address customer needs and learn more about how digital assets may impact the future of financial services. The following comments reflect their concerns about the risks of digital assets and their questions about the lack of regulatory clarity:

1. Digital assets present numerous significant threats, including financial crimes and risks to financial stability. Illicit activities fueled by cryptoassets, like ransomware, have impacted community bank customers.

2. Decentralized Finance (DeFi) presents new opportunities for bad actors to engage in illicit activities and avoid the scrutiny of traditional, regulated financial intermediaries. ICBA supports efforts by policymakers to study these novel risks and take steps to prevent the rise of a shadow banking system that can pose risks to consumers, the financial system, and U.S. national security.

3. Community bankers are opposed to the United States issuing a digital dollar or CBDC. The risks far outweigh the uncertain and unproven benefits cited by CBDC advocates. A CBDC threatens to disintermediate community banks, thus raising the risk of serious economic consequences.

What are the illicit finance risks related to non-fungible tokens?

Non-fungible tokens ("NFTs") are digital tokens that signify ownership of digital or physical property, including artwork, songs, or even membership with an organization. Individuals can trade NFTs on a variety of online platforms in exchange for other cryptocurrencies or fiat currency. The greatest risk posed by non-fungible tokens ("NFTs") is the lack of a regulatory framework or constraints, and the increased criminal attraction to the technology. The Treasury Department identified in a report earlier this year several risks unique to NFTs, including the

[7] Independent Community Bankers of America, Letter to the House Committee on Financial Services ,"Re: Community Bank Perspective on Stablecoin Legislation" (July 22, 2022), https://www.icba.org/docs/default-source/icba/advocacy-documents/letters-to-congress/letter-on-stablecoin-legislation.
[8] Independent Community Bankers of America, Statement submitted to United States Senate, "Central Bank Digital Currency: Significant Risks Must Preclude Adoption," (May 26, 2022), https://www. icba.org/docs/default-source/icba/advocacy-documents/testimony/hearing-statement-on-central-bank-digital-currency.pdf.

ease with which one can self-launder assets and royalty models that incentivize rapid sales.[9] The report also said that NFT platforms "may be considered virtual asset service providers (VASP) by FATF and may come under FinCEN's regulations."[10] However, as more criminals seek to exploit the current loopholes and use NFTs for money laundering, ICBA recommends that FinCEN consider issuing specific guidance about this emerging technology and its threats.

ICBA also recognizes that NFTs may qualify as investments and be subject to securities laws and regulations; therefore, it is essential for regulators to continue their efforts to collaborate on a comprehensive regulatory approach.

What are the illicit finance risks related to decentralized finance (DeFi) and peer-to-peer payment technologies?

Cryptocurrencies have a long history of being used for criminal and illicit activity and undermining law enforcement. Criminals frequently use cryptocurrencies to launder funds, hijack computer systems with malware to surreptitiously mine cryptocurrency, and to facilitate payments for illegal goods and services. Anonymity-enhanced cryptocurrencies, or cryptocurrencies designed to evade scrutiny and cloak users in greater secrecy, are utilized by fraudsters around the world for a variety of criminal actions.

Broader use of cryptocurrencies has expanded financial crime risk by creating cyber vulnerabilities which produce opportunities for adversaries to use digital assets to advance efforts that threaten national security and harm American businesses. For example, the Axie Infinity attack was attributed to North Korean hackers known as the Lazarus Group.[11] Although the federal government has targeted some crypto platforms that aid North Korean cybercriminals, such as the Office of Foreign Assets Control's sanctioning of Blender.io, North Korea remains undeterred in their efforts to use cryptocurrency to evade sanctions to seek funding for the Kim regime and its weapons programs.[12] In June 2022, the Lazarus Group conducted another significant heist with an attack against Horizon Bridge that yielded $100 million in ether, USD Coin, Dai, and other assets.[13] These attacks suggest that adversarial nation-states will continue to circumvent traditional financial systems through the use of cryptocurrencies or other digital assets.

---

[9] Department of the U.S. Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art" (February 2022), https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf.
[10] Ibid.
[11] Aaron Schaffer, *The Washington Post*, "North Korean hackers linked to $620 million Axie Infinity crypto heist" (April 14, 2022), https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/.
[12] United States Department of the Treasury, Press Release, "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.
[13] Carly Page, *TechCrunch*, "North Korean Lazarus hackers linked to $100M Harmony bridge theft" (June 30, 2022), https://techcrunch.com/2022/06/30/north-korea-lazarus-harmony-theft.

Additionally, cryptocurrencies are frequently used to facilitate money laundering, terrorist financing, and other financial crimes. American citizens are regularly targeted by scammers and cybercriminals who use cryptocurrency as their preferred method for ransomware or other scam related payments, such as romance scams or fraudulent investment schemes. In June, the Federal Trade Commission ("FTC") revealed that almost 46,000 Americans lost more than $1 billion to cryptocurrency scams since the start of 2021,[14] and that nearly $600 million was lost to crypto investment scams and romance scams claimed another $185 million.[15]

These attacks and scams, combined with the laundering of digital assets through decentralized exchanges and mixers, such as Tornado Cash, continue to complicate law enforcement's efforts to stop cybercriminals and recover users' stolen assets. Mixers are centralized or decentralized services "that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination."[16] While mixers are designed to provide privacy in cryptocurrency transactions, they are used by cybercriminals to conceal the source of funds.

These challenges should not be underestimated as policymakers consider the future of digital assets and how to counter their potential use for illicit activities. Community banks are responsible actors that work with regulators and law enforcement to investigate and mitigate financial crimes. If digital assets are going to play a role in the future financial system, then all participants must be held to the same high standards and work to curtail the ability of bad actors to scam consumers and commit other financial crimes.

What additional steps should the United States government take to more effectively deter, detect, and disrupt the misuse of digital assets and digital asset service providers by criminals?

The U.S. government should implement a robust identification process for all digital asset stakeholders and projects. The Travel Rule could be used as a basis to execute an identification framework. Currently, the Travel Rule requires institutions processing virtual currency transactions valued at $3,000 or more to pass on and retain certain identifying information – including names, addresses, and account numbers – of both transaction counterparties to the next financial institution in the transaction chain.[17] Creating a new requirement for all non-bank digital asset players which removes or substantially reduces the threshold for digital assets could significantly help to deter, detect, and disrupt criminal activity in this space.

---

[14] Lesley Fair, Federal Trade Commission, "Reported crypto scam losses since 2021 top $1 billion, says FTC Data Spotlight" (June 3, 2022), https://www.ftc.gov/business-guidance/blog/2022/06/reported-crypto-scam-losses-2021-top-1-billion-says-ftc-data-spotlight.

[15] Ibid.

[16] United States Department of Justice, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework* (October 2020), https://www.justice.gov/archives/ag/page/1326061/download.

[17] Travel Rule 31 CFR § 1010.410(f) and Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies FIN-2019-G001, May 9, 2019.

Are there specific areas related to AML/CFT and sanctions obligations with respect to digital assets that require additional clarity?

There are several statutory and regulatory requirements under the Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") framework that need to be further developed and clarified. Additional development and clarity are needed in the areas of: Know Your Customer ("KYC") and Know Your Transaction ("KYT"), customer due diligence, enhanced due diligence, determining the beneficial owners of a digital asset, suspicious activity identification and reporting, and responsibilities of each party involved in the digital asset ecosystem.

What regulatory changes would help better mitigate illicit financing risks associated with digital assets?

Financial institutions are required to have vigorous Bank Secrecy Act/Anti-Money Laundering controls in place. ICBA supports ongoing efforts by policymakers to harmonize regulations to ensure similar strong oversight of cryptocurrency service providers. Comprehensive guidance should address the risks associated with digital assets and clarify regulatory and compliance expectations pertaining to customer identification, monitoring, and reporting for all participants.

What additional steps should the U.S. government consider to combat ransomware?

The battle against ransomware involves much more than detecting or preventing ransom payments paid with cryptocurrency. ICBA recognizes the value of cross-industry training and partnerships with critical government agencies to educate bankers about ransomware to strengthen organizational defenses. ICBA is encouraged by recent government actions addressing ransomware and other cyberthreats to the financial services industry. In particular, the Cybersecurity and Infrastructure Security Agency's ("CISA") recent "Stop Ransomware" campaign provides critical infrastructure with important resources tools and resources to fight ransomware. Providing the private sector with actionable intelligence is crucial to preventing serious attacks, particularly those involving cryptocurrencies. The more information about potential threats the government can get in the hands of security practitioners, the more secure the financial services ecosystem will be. ICBA strongly supports industry initiatives such as the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), which facilitates public and private sector sharing of cyber threat and vulnerability information.

Additionally, cross-sector sharing is critical to fully combatting ransomware attacks. ICBA recommends that Treasury continue to work collaboratively with CISA and other critical infrastructure sectors to ensure cross-sector information sharing can be as efficient as possible.

What additional steps should the U.S. government consider to address the illicit finance risks related to mixers and other anonymity-enhancing technologies?

Mixers essentially operate as money transmitters which require regulatory reporting and monitoring obligations. Yet as the Action Plan lays out, "they may deliberately operate in a non-compliant manner to make it more difficult for regulators and law enforcement to trace illicit funds."[18] Given the likelihood of mixers being used in a criminal manner, mixers and all other anonymity-enhancing technologies should be labeled high risk.

What steps should the U.S. government take to effectively mitigate the illicit finance risks related to DeFi?

DeFi seeks to permit users around the world to access a variety of financial products and services, without having to rely on intermediaries like banks or broker-dealers. While proponents market these capabilities as a way to bring financial services to underserved communities or address other issues, these same capabilities also offer cybercriminals countless ways to avoid the scrutiny of regulated entities and circumvent sanctions programs.

As an example, Tornado Cash remains available for bad actors to use, even though the government sanctioned Tornado Cash on August 8, 2022 after it helped to launder more than $7 billion in assets since 2019.[19] As of mid-October, there was still approximately $172 million in total value locked in Tornado Cash.[20] Within the past few weeks, the individuals behind several high-profile exploits, such as the TempleDAO exploit and the BitKeep hack, quickly funneled stolen cryptoassets to Tornado Cash.[21] However, Tornado Cash is not the only protocol that can help bad actors engage in illicit activities with digital assets. In the wake of Treasury's sanctions against Tornado Cash, some hackers have turned instead to automated market maker protocols like Curve's 3pool. By using the 3pool, a hacker can deposit stablecoins into a smart contract and then withdraw a different type of stablecoin, thereby limiting the ability for issuers to freeze stolen assets.[22] In September 2022, the attacker who targeted the Wintermute market marker, used this approach by transferring $114 million in USDT and USDC stablecoins.[23]

---

[18] United States Department of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* (September 20, 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf. (Action Plan)
[19] United States Department of the Treasury, Press Release, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash" (August 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.
[20] Harsh Notariya and Ryan James, *BeInCrypto*, "Crypto Hackers Continue to Use Tornado Cash Despite US Treasury Sanctions" (October 17, 2022), https://beincrypto.com/hackers-continue-to-use-tornado-cash-despite-sanctions/.
[21] Shalini Nagarajan, *Blockworks*, "TempleDAO Hacked Funds Deposited to Tornado Cash" (October 17, 2022), https://blockworks.co/templedao-hacked-funds-deposited-to-tornado-cash/; Tim Hakki, *Decrypt*, "BitKeep Hacker Moves $1M in Binance Coin Through Tornado Cash" (October 18, 2022), https://decrypt.co/112305/bitkeep-hacker-moves-1m-binance-coin-through-tornado-cash.
[22] Curve Finance, "Depositing into the Tri-Pool" (Accessed October 24, 2022), https://resources.curve.fi/lp/deposit-faqs.
[23] Shalini Nagarajan, *Blockworks*, "Wintermute Whacked by $160M Hack Exploiting Known Vulnerability" (September 20, 2022), https://blockworks.co/wintermute-whacked-by-160m-hack-exploiting-known-vulnerability/.

Like virtually all DeFi protocols, interacting with the 3pool does not require any implementation of customer identification regulations, such as BSA's know your customer rules. Users simply connect a wallet and decide which stablecoins to add to the liquidity pool. As noted in the Treasury Department's recent report on digital assets and illicit activity, "DeFi services often lack AML/ CFT or other processes to identify customers or suspicious activity and allow layering of proceeds, or the separation of the criminal proceeds from their origin, to take place instantaneously and pseudonymously."[24] These troubling facts speak to a more significant issue with which regulators must contend: the growth of decentralized finance.

ICBA encourages regulators to collaborate on a comprehensive approach to prevent the rise of a shadow banking system filled with unregulated, decentralized platforms that pose risks to consumers, the financial system, and U.S. national security. To that end, ICBA and its members welcome Treasury's plan to study the use of DeFi for illicit activities and release a report next February. We also support efforts by the Financial Stability Board to complete similar studies so that bankers and policymakers have a complete understanding of the potential financial stability implications for the continued development of decentralized financial services. Community banks are the foundation of their communities' economic activities, and these connections will continue to have meaning even as the digital economy expands and new opportunities develop. We encourage policymakers to consider the vital role of community banks as they debate the future of digital assets—Main Street still matters in the 21st century economy.

How can Treasury maximize public-private and private-private information sharing on illicit finance and digital assets?

Communication and cooperation are critical to an effective working partnership among the government, law enforcement, digital asset stakeholders. In addition to "bilateral engagement, to include information sharing and capacity building, as appropriate, to support countries in implementing the international AML/CFT standards,"[25] Treasury, and law enforcement entities, can maximize information sharing by establishing relationships with organizations, subject matter experts, or hackers specializing in digital assets tracking and security. These relationships could allow for more targeted information sharing and intelligence of emerging trends, patterns, threats and vulnerabilities; serve as educational tools for federal regulators and law enforcement; and help inform overall AML/CFT and sanctions policies, requirements. and programs. Section 314(a)[26] and section 314(b)[27] of the USA Patriot Act are current information-sharing tools upon which to build.

[24] United States Department of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* (September 20, 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf. (Action Plan)
[25] Ibid p.9
[26] USA PATRIOT Act of 2001 (P.L. 107-56)
[27] Ibid.

How can the U.S. Department of the Treasury, in concert with other government agencies, improve guidance and public-private communication on AML/CFT and sanctions obligations with regard to digital assets?

In concert with other government agencies, Treasury can improve guidance and communication with regard to digital assets by partnering with organizations, subject matter experts, or hackers specializing in digital assets tracking and security. This partnership could give Treasury and other government agencies insight into intelligence pertaining to trends, patterns, and typologies, which can then be disseminated to digital asset stakeholders on a regular basis. Such information from Treasury and government agencies can be used by stakeholders to incorporate into risk assessments and overall AML/CFT and sanctions programs. Treasury can look no further then within its own agency on ways to improve guidance and communication as FinCEN is currently required by Congress to issue AML/CFT Priorities[28] and Threat Pattern and Trend Information[29] to covered entities. Both guidance documents could be used as models as it relates to digital assets.

How can Treasury most effectively support the incorporation of AML/CFT controls into a potential U.S. CBDC design?

ICBA strongly believes policymakers should not proceed with creation of a CBDC without explicit statutory authorization and oversight from Congress. In testimony before the Senate Banking Committee, Chairman Jerome Powell said that before proceeding to develop a CBDC the Federal Reserve would "want very broad support in society and in Congress and ideally that would take the form of authorizing legislation as opposed to a very careful reading of ambiguous law."[30] While we appreciate the Chairman's commitment to a continued dialogue, we do not believe that the authority for the Federal Reserve to issue a CBDC exists under current law. ICBA also urges Congress to consider the many risks and concerns raised above and not authorize the creation of CBDC.

[28] Issued pursuant to Section 6101(b)(2)(C) of the Anti-Money Laundering Act of 2020 (AMLA) FinCEN, after consulting with OFAC, relevant state financial regulators, and relevant law enforcement and national security agencies, is required to issue government wide priorities for anti-money laundering and countering the financing of terrorism. The AMLA was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021)

[29] Issued pursuant to Section 6206 of AMAL which requires FinCEN to periodically publish threat pattern and trend information obtained from financial institutions' Suspicious Activity Reports.

[30] "The Semiannual Monetary Report to the Congress," United States Senate Committee on Banking, Housing, and Urban Affairs (July 15, 2021) (Testimony of the Hon. J. Powell).

Conclusion

ICBA and its members appreciate the opportunity to comment on the Treasury's request for comment. We believe that any federal regulatory framework for digital assets must protect the nation's financial system from unsound risks and criminal activity, must protect consumers from misrepresentations and must preserve the separation of banking and commerce. We look forward to working with the Treasury and with the Administration as it considers the future of digital assets and develops policies that will enable community banks and their customers to benefit from advances in financial technology without sacrificing the health of the broader economy. If you have questions or require additional information about ICBA's statements, please contact me at (202) 821-4427 or by email at Brian.Laverdure@icba.org.

Sincerely,

/s/

Brian Laverdure, AAP
Vice President, Payments and Technology Policy