DeFi Education Fund

October 17, 2025

Submitted via the Federal eRulemaking Portal at www.regulations.gov

U.S. Department of the Treasury
www.regulations.gov

Re: Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets, Docket No. TREAS-DO-2025-0070

DeFi Education Fund (DEF) respectfully submits these comments in response to the United States Department of the Treasury's (Treasury) "Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets," TREAS-DO-2025-0070 (RFC), and more specifically, the request for input on the various "methods, techniques, or strategies for detecting and mitigating illicit activity risks involving digital assets," including smart contract-based digital identity verification.[1] DEF enthusiastically supports Treasury's efforts to mitigate illicit activity risks in the digital asset ecosystem and support a safe and secure ecosystem, and we believe Treasury should carefully consider the risks posed by digital identity verification in smart contracts before requiring or implementing such verification through rulemaking—and focus on the implementation of strong cybersecurity solutions.

Current identification systems create centralized repositories of sensitive information (i.e., honeypots) that pose meaningful risks to consumers. Moreover, as a standalone, digital identity verification cannot reliably mitigate illicit activity risks. While evolving technologies, such as zero-knowledge proofs (ZKPs), may prevent public exposure of a user's sensitive personal information and their activities on the blockchain, privacy and cybersecurity risks remain with verifiable credential issuance.

By way of background, DEF is a non-partisan, nonprofit research and advocacy group. Our mission is to educate lawmakers about the technical workings and benefits of decentralized finance (DeFi), advocate for sound DeFi policy, and protect the rights of developers, users, and projects to freely create decentralized infrastructure and technology. DEF has no members and operates as an independent entity. We believe that DeFi has immense potential to advance

[1] *See* Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets, 89 Fed. Reg. 40148, 40149 (Aug. 18, 2025) (summarizing the RFC's purpose to solicit input on methods for detecting and mitigating illicit activity risks involving digital assets).

innovation in the world economy and that its potential can best be realized in conjunction with smart policy.

This letter has three sections:

- **Section I serves as a primer to the risks involved in digital identity verification**, explaining why privacy matters in financial transactions and with emerging technologies, such as DeFi, for both American citizens and national security.

- **Section II provides a general overview of digital identity infrastructure** and identifies the privacy and cyber risks associated with the current model of digital identity management and issuance, as well as risks associated with a digital identity footprint and the creation of honeypots of sensitive personal information.

- **Section III identifies the risks and vulnerabilities that exist in the digital asset ecosystem** and the opportunity to strengthen Treasury's cybersecurity efforts.

I. The Importance and Relevance of Privacy

Privacy is foundational to a free and open society, and to the safety and dignity of its people. It is not monopolized by criminals, as some would suggest, but a protection that is embedded in the American Constitution. There are perfectly lawful, legitimate reasons for choosing to protect one's own sensitive information, such as PII and financial transaction history, which can paint the most intimate picture of one's beliefs, associations, and activities—aspects of their lives which could lead to discrimination, harassment, or exploitation. Many Americans are justifiably concerned with how their personal information is protected within the traditional financial system and strongly believe that changes must be made to grant individuals more control over their own data.[2] This sentiment towards privacy was shared among members of Congress with the House's passing of the *Anti-CBDC Surveillance State Act*.[3]

Prior to the Information and Digital age, Americans could transact and interact with each other without being identified and profiled for profit-seeking objectives. This freedom was largely lost as our society digitized, and today some of the only ways for Americans to transact

[2] DEF & Ipsos, *Demystifying DeFi* (Aug. 2025), https://tinyurl.com/4dpxp57b (reporting that 54% of Americans surveyed feel the current financial system does not adequately protect their personal information and 56% believe changes are needed to give people more control over their personal data).
[3] H.R. 5403, 119th Cong. (2024) (Anti-CBDC Surveillance State Act) (effectively prohibiting the Federal Reserve from issuing a central bank digital currency and codifying EO 14178); Remarks of Rep. Tom Emmer, YouTube (Feb. 28, 2024), https://tinyurl.com/msjjp3fp (explaining that a CBDC would effectively "give the federal government the ability to surveil and restrict Americans' transactions and monitor every aspect of our daily lives.").

without leaving a digital footprint is to use paper currencies, hard metals, or other forms of bartering.

Privacy matters for all Americans, as it is a means for both personal and national security. Should the American people be protected in their private lives, then so too will the nation be protected from foreign adversaries that weaponize Americans' sensitive personal information. The risks associated with the existing information collection regimes and why privacy is in the interest of national security is discussed below.

A. Information Collection Risks

Information collection and retention has become the standard for most of our financial affairs. Individuals using the traditional financial system are required to provide sensitive information to identify themselves to banks and other financial institutions, and once identified, every transaction is traceable and reportable by financial institutions to reduce the risk of non-compliance with anti-money laundering (AML) laws, including the Bank Secrecy Act (BSA) and its progeny.[4]

Federal agencies that collect PII in the course of agency operations generally create a federal record[5] that must be retained pursuant to federal statute or an Executive Order,[6] and the agency must not dispose of it except pursuant to the National Archives and Records Administration's (NARA) approved disposition schedule.[7]

---

[4] *See Bank Secrecy Act (BSA)*, FinCEN, https://tinyurl.com/mtbv5jsj (stating that under the BSA, financial institutions are required to identify and verify the identity of their customers, keep records of cash purchases and negotiable financial instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and report suspicious activity that might signify money laundering or tax evasion); *History of Anti-Money Laundering Laws*, FinCEN, https://tinyurl.com/37wehvwk (describing how, since the BSA's passage, its scope has expanded with the enactment of the Money Laundering Control Act (1986), the Annunzio-Wylie Anti-Money Laundering Act (1992), the Money Laundering Suppression Act (1994), and the USA PATRIOT Act (2001)).

[5] 44 U.S.C. § 3301(a)(1)(A) (defining "records"); Office of Mgmt. & Budget, Circular A-130, *Managing Information as a Strategic Resource*, at 17(h) (July 28, 2016), https://tinyurl.com/ycy9r49b (explaining that OMB Circular A-130 establishes general policy for federal information management and requiring agencies to "maintain all records with PII" according to NARA-approved retention or disposition schedules).

[6] *See* 44 U.S.C. § 3101 ("The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities"); 5 U.S.C. § 552a(e)(1) ("Each agency that maintains a system of records shall—(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President").

[7] 44 U.S.C. § 3303a(a), (d) (providing that the Archivist of the United States, acting through NARA, determines which federal records warrant continued preservation or disposal based on their administrative, legal, research, or other value, after notice for public comment in the Federal Register).

Additionally, pursuant to the PATRIOT Act of 2001, Treasury was required to "prescribe regulations setting forth the minimum requirements for financial institutions and their customers regarding the identity of the customer" that applied to the "opening of an account at a financial institution."[8] These regulations are now known as Customer Identification Programs (CIPs), which set forth requirements for financial institutions to comply with upon opening accounts for new customers.[9]

Subsequently, individuals face new risks and vulnerabilities: information collection and retention has created honeypots of data that have been compromised throughout American history. Of note, PII was the most stolen data source globally in 2024.[10]

Financial institutions are regular targets of cyber criminals. For example, Capital One and JP Morgan Chase were both targets of large scale data compromises from cyber attacks that resulted in millions of customers' sensitive personal information being stolen. Specifically, in 2019, Capital One experienced a data breach affecting 100 million Americans and 6 million Canadians, which compromised consumers' personal information such as names, Social Security numbers, addresses, phone numbers, email addresses, dates of birth, and account numbers.[11] In 2014, JPMorgan Chase experienced a data breach that compromised millions of customers' credit card numbers, expiration dates, cardholder names, billing addresses, and CVV codes.[12]

And, it is not just financial institutions that are at-risk; many direct-to-consumer businesses are also targets for cyber attacks. For example, in 2021, T-Mobile experienced a data

---

[8] Pub. L. No. 107-56, § 326, 115 Stat. 272 (2001).

[9] *Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks*, 68 Fed. Reg. 25090 (May 9, 2003), https://tinyurl.com/2esfcxfr (explaining that in 2003, Treasury, through the Financial Crimes Enforcement Network (FinCEN), together with the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA), jointly adopted "Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks" (CIP) and that the rule requires financial institutions to "verify the identity of any person seeking to open an account, to the extent reasonable and practicable; 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 provided to the financial institution by any government agency")).

[10] *See* Ani Petrosyan, *Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2024*, Statista (July 14, 2025), https://tinyurl.com/yck3a5km (reporting that in 2024 the United States experienced 3,158 data compromises impacting 1.35 billion individuals; in 2023, 3,205 compromises impacting 353 million individuals; and in 2022, 1,802 compromises impacting 422 million individuals); Ani Petrosyan, *Data Breaches Worldwide*, Statista (Sept. 13, 2025), https://tinyurl.com/yu3tnee3 (reporting "[i]n 2024 about 48 percent of all data breach incidents in global organizations involved customer personal identifiable information (PII), thus making it the most frequently breached type of data.").

[11] *See* Capital One, *Capital One Announces Data Security Incident* (July 29, 2019),https://tinyurl.com/2s3drh8e;

[12] *See* Twingate, *JP Morgan Data Breach: What & How It Happened?* https://tinyurl.com/ymycurue.

breach that compromised the names, dates of birth, Social Security numbers, and driver's license or ID numbers of approximately 7.8 million of their existing customers and 40 million of their former or prospective customers.[13] One of the largest data compromises in U.S. history involved a 2017 cyber attack by foreign adversaries against Equifax, a U.S. credit reporting agency; Equifax experienced a data breach compromising the names, home addresses, phone numbers, dates of birth, Social Security numbers, and driver's license numbers of approximately 150 million Americans.[14] (Subsequently, in 2020, the Department of Justice indicted Chinese military personnel with committing computer fraud, economic espionage, and wire fraud in connection with the Equifax hack.[15])

Federal agencies are also subject to notorious data compromises, including from internal employees or contractors who are trusted with millions of Americans' sensitive personal information. For example, from 2018 through 2020, an independent contractor for the Internal Revenue Service (IRS) stole the tax return information of thousands of high-net-worth individuals and their related entities, and subsequently disclosed it to ProPublica and others. ProPublica used the stolen information to publish a series of news articles about high-profile taxpayers, making many Americans' sensitive financial data public without their permission.[16] There are also incidences of negligence: in 2022, the IRS reported that 120,000 taxpayers' private information was temporarily public.[17] Furthermore, warrantless financial surveillance enables discriminatory or arbitrary enforcement, wherever it occurs.[18]

While these data compromises have negatively impacted American citizens, information collection and retention regimes meant to protect the public and maintain national security have

---

[13] T-Mobile, *Additional Information Regarding 2021 Cyberattack Investigation* (Aug. 20, 2021), https://tinyurl.com/2s3drh8e.

[14] Electronic Privacy Information Center, Equifax Data Breach, https://tinyurl.com/4netc3ku (reporting that in 2017 Equifax experienced a data breach compromising the names, home addresses, phone numbers, dates of birth, Social Security numbers, and driver's license numbers of approximately 150 million Americans).

[15] U.S. Dep't of Justice, *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Equifax* (Feb. 10, 2020), https://tinyurl.com/ykz4xehp.

[16] Greenberg Traurig, *IRS Notifies Thousands of Taxpayers That They Were Victims of a Data Breach* (Apr. 2024), https://tinyurl.com/228j9v9t.

[17] NPR, *IRS Says Private Information for About 120,000 Taxpayers Was Temporarily Public* (Sept. 4, 2022), https://tinyurl.com/2rueepvp.

[18] U.S. House of Representatives, Committee on the Judiciary & Select Subcommittee on the Weaponization of the Federal Government, Financial Surveillance in the United States: How the Federal Government Weaponized the Bank Secrecy Act to Spy on Americans (Interim Staff Report, Dec. 6, 2024) (finding that American financial data has been arbitrarily enforced and weaponized by government agencies; explaining that in recent cases law enforcement eschewed existing laws, regulations, and constitutional protections that bar obtaining customer information from financial institutions without legal process; and stating that "federal law enforcement has regularly abused the information sharing process in order to deploy financial institutions as *de facto* arms of federal law enforcement").

proven ineffective in mitigating illicit activity risks.[19] In fact, contrary to the objectives of the BSA and its subsequent laws, stolen PII is incredibly advantageous for illicit actors. Once in possession of PII, illicit actors are able to immediately control people's accounts, conduct fraudulent transactions, or drain funds, as well as impersonate law-abiding citizens to launder money through traditional channels.[20]

Financial institutions are also able to sell nonpublic personal information, including PII, to unaffiliated third parties, as long as consumers are provided with a notice and given reasonable opportunity to opt out of such disclosures.[21] Unfortunately, these notices provide consumers with limited protection, and make Americans' nonpublic personal information easy to sell, use, or exploit in an open marketplace.[22]

The proliferation of peer-to-peer transactions on a blockchain through DeFi mitigated these risks by removing some of the traditional barriers to accessing traditional financial services (e.g., individuals are not required to submit stored identifying information to be able to functionally transact on the internet—everything is verified through cryptography[23]). However, given that wallet addresses are publicly traceable on the blockchain and pseudonymous identities can sometimes be traced back to a particular person, it is possible to view a vast record of that person's transactional history. For this reason, many developers in the blockchain ecosystem are

---

[19] *See* Gavin Zavatone & Henry Michaelson, *The Bank Secrecy Act Is Broken: Examining the Burdens, Costs, and Failures of the Bank Secrecy Act (BSA), and the Potentially Disastrous Implications of Applying the BSA to Decentralized Finance (DeFi)* (DEF Feb. 2025), (explaining " IRS investigations originating from BSA data constitute approximately 0.00135 percent of the total BSA reports collected by FinCEN. Although the IRS only represents one agency with access to BSA data, the miniscule usage of BSA data to initiate IRS investigations represents a microcosm of a broader trend.").

[20] *See* Alex Petrovski, *10 Biggest Data Breaches in the Financial Sector [2025]* (June 10, 2025), https://tinyurl.com/3k5a2cmt; U.S. Dep't of Justice, *Seven Charged in Sophisticated Stolen Identity Tax Refund Fraud Scheme That Sought Over $100 Million* (Aug. 24, 2023), https://tinyurl.com/yfksmf66 (reporting that a federal grand jury charged "seven individuals with conspiracy to commit mail and wire fraud and other crimes arising out of their scheme to defraud the IRS using stolen identities.").

[21] *See* 15 U.S.C. § 6801 (2018); 12 C.F.R. §§ 1016.10–.12 (2024) (implementing the Gramm-Leach-Bliley Act through Regulation P, requiring financial institutions to provide consumers with notice and a reasonable opportunity to opt out of disclosures of nonpublic personal information to unaffiliated third parties); 12 C.F.R. § 1016.3(m)(1)–(2) (2024) (defining "nonpublic personal information" as personally identifiable financial information and any list, description, or grouping of consumers derived from such information that is not publicly available).

[22] Jay Stanley, *Why Don't We Have More Privacy When We Use Credit Cards?*, ACLU, https://tinyurl.com/cyxccthm (explaining that under the Gramm–Leach–Bliley Act companies face little resistance in selling customers' financial data to third parties, that consumers must repeatedly opt out with every financial institution, and that companies collect and sell personal data such as "how much [consumers] spend on travel, restaurants, political or religious donations, liquor stores, sex shops, [etc.]," information that "is more powerful and revealing when combined with other data," while not disclosing "what specific information will be shared with unaffiliated third parties").

[23] Public-key cryptography is used in authenticating the sender's identity and the transaction's information by producing a digital signature.

focused on developing privacy-enhancing technologies to protect users from emerging threats and malicious actors.

II. Digital Identity Verification

As the government increasingly focuses on addressing illicit finance in crypto, the conversation about whether digital identity verification could be a potential solution has expanded. However, it is important to keep in mind the limitations of digital identity verification and the risks associated with mandating such a solution. Our digital footprints convey intimate details of our lives, and with digital identity, a person's real world identity is more directly tied to their digital footprint, developing a fully intimate profile of a person and exposing them to various risks.

When applied to a blockchain, a digital footprint becomes much clearer. If digital identity exists on a blockchain for smart contract verification without any privacy-enhancing features, a person's financial activities can be easily traced by anyone. This allows bad actors to track a specific person's transactions, allowing them to see who they transact with, which protocols they use, and, most dangerously, the amount of digital assets they own.

In its current form, digital identity verification technology also develops honeypots of sensitive personal information, presenting vulnerabilities to the American people and U.S. national security. Generally, identity management systems have proven problematic due to large scale hacks and the misuse of user data, as they have historically been managed by entities with centralized infrastructure that is prone to hacks and internal malicious actors.[24] While federated models for managing identity have been introduced to increase security by separating tasks to multiple entities, they also maintain centralized control of sensitive data by one of the participating entities and present similar issues. Thus, the safest approach is to decentralize identity management; however, decentralization alone does not mitigate these risks, as digital identity issuance and verification present their own risks.

Section II addresses the infrastructure and risks associated with digital identity management and issuance, as well as risks associated with a digital identity footprint, evolving solutions, and considerations concerning the Fourth Amendment.

A. Digital Identity Management and Issuance

The primary approach for digital identity management systems today relies on centralization, which means that trusted intermediaries oversee the identification process from

[24] Lu Zhou et al., *Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities*, 80 J. Info. Sec. & App. 103678 (2024), at 3.

verification to management of user data. In such systems, users have limited control over their identification data and may not have visibility into the mechanisms governing how the central authority manages, shares, or secures their sensitive information. And, as previously mentioned, centralized infrastructure is a prime target of cyber attacks due to its concentration of sensitive personal data.[25]

A second approach is found in federated identity management systems, which distribute control and responsibilities among identity providers and service providers.[26] However, even within such systems, concentrated data still exists with the identity provider, creating a target for cyber attacks.[27] Privacy concerns remain, as an identity provider could still track and aggregate user activity across different service providers, leading to user privacy and profiling concerns.[28]

In contrast to these two approaches, decentralized identity management is undoubtedly the gold standard because of increased privacy and security for users and their data. In such systems, individuals maintain full control of their data and decide with whom to share it, which minimizes exposure of sensitive information beyond what is needed to complete a certain task and prevents centralized actors from collecting and storing sensitive information in honeypots.[29]

For decentralized identity management, there needs to exist an issuer, a holder, and a verifier. The issuer is a third party that cryptographically signs digital records known as verifiable credentials (e.g., government-issued identification).[30] These credentials are made up of metadata, which includes identifiers, terms of use, and validity and expiration dates; claims, which are verified details about the credential holder; and proofs, which are the cryptographic evidence that the issuer authenticated the credentials.[31] In the context of DeFi, the issuer would likely be a government entity or government-authorized entity; the holder would be the user; and the verifier would be a smart contract. Using public-key cryptography, an issuer is able to authenticate the holder's identity and underlying information (e.g., the credentials) by producing a digital signature.[32] Specifically, the issuer uses a mathematically derived private key to authenticate these credentials, signaling accuracy, so that a verifier can then use the issuer's public key to mathematically verify that the holder's credentials are indeed signed by the issuer.

---

[25] *See Id.*

[26] *Id.* at 4.

[27] Crysta Timmerman, *What Is a Federated Identity? The Pros and Cons*, IPVanish (July 9, 2024), https://tinyurl.com/3kfde53u.

[28] *Id.*

[29] *See* Phillip Shoemaker, *What Is Decentralized Identity? A Comprehensive Guide*, Identity.com (Sept. 2, 2025), https://tinyurl.com/44enas8d.

[30] W3C, *Verifiable Credentials Data Model v2.0* (May 15, 2025), https://tinyurl.com/fdart9dh.

[31] *Id.*

[32] In public-key cryptography, a person can mathematically generate what is known as a private key, and a public key that is then mathematically derived from the private key. While this process is relatively easy computation, reverse engineering the private key from the public key is nearly impossible, making it highly secure.

In other words, an issuer can mathematically sign off on a holder's credentials that a verifier can then mathematically prove, verifying the credentials' authenticity.

B. Risks Posed by Digital Identity Management and Verification

While decentralized identity management is the gold standard of infrastructure, it is merely a building block towards a more private and secure system. Its design *alone* still presents risks for users in the context of digital identity verification. Specifically, a digital identity issuer would need to collect PII—specifically credentials, such as government-issued IDs—to issue verifiable credentials from an operational standpoint. Since it remains the policy of the U.S. that various financial institutions and government entities must retain the PII they collect,[33] the risks previously outlined also remain.

In the context of digital identity implementation within DeFi, this means that users would still have to trust issuers to act in good faith and responsibly handle their personal information. (It's worth noting that this runs counterintuitive to DeFi's inherent design and benefits: DeFi is meant to minimize trust in third-parties, and therefore, minimize risk. Decentralized networks are made more secure by spreading authority so thin that there is no single point of failure nor means for any person or entity to exert control and act maliciously. Introducing off-chain issuers into a decentralized system and requiring their use in order for users to transact removes the benefits of decentralization, and introduces risks inherent to the traditional financial system—risks that have proven detrimental.) Additionally, depending on the design, the issuer could keep track of the use of the proof they developed if their issuance was designed to give users only one proof for their identity,[34] or the verifier—in DeFi, the smart contract—could record and compile information about who is presenting their digital identity for verification.[35]

For digital identity management systems to be used safely, the U.S. must maximize privacy. For example, it is not enough to no longer require PII retention, the issuer must also be prevented from knowing who was issued verifiable credentials, because a time-stamped issuance log combined with metadata (e.g., IP address, device/browser fingerprint, coarse location, etc.) can enable high-confidence linkage between a person and their credential use. In the event there is a data breach or leakage, this correlated dataset would create a dossier of who requested credentials, when, and for what reason, exposing users to the very privacy risks previously discussed.

---

[33] Issuers could be federal agencies or accredited non-government organizations. Depending on the category of the issuer, they likely fall under some sort of PII regulation (e.g., BSA and CIP for financial institutions).

[34] Vitalik Buterin, zkID (June 28, 2025), https://vitalik.eth.limo/general/2025/06/28/zkid.html.

[35] Jay Stanley, *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom*, American Civil Liberties Union (May 2021), https://tinyurl.com/4t3pexd3.

Furthermore, issuers must take certain measures to authenticate the identity of the person applying for verifiable credentials and prevent fraud. For this reason, the National Institute for Standards and Technology (NIST) has written extensive Digital Identity Guidelines ("the Guidelines") specifically for federal agencies who act as issuers—known as "credential service providers" (CSP)—to follow in their issuance of verifiable credentials.[36] The Guidelines define technical requirements for identity assurance and outline procedures for making the process as safe and fraud-resistant as possible. For assuring that the applicant presenting the evidence is the rightful owner, NIST recommends that CSPs may employ, but are not limited to, the following methods: confirmation code verification,[37] visual facial image comparison,[38] and automated biometric comparison.[39] Additionally, in order to conduct fraud checks, NIST also recommends that CSPs may employ, but are not limited to, the following methods: device or account tenure check,[40] device fingerprinting,[41] and transaction analytics.[42]

However, these methods for identity proofing present risks of fraud, honeypots, and discrimination.[43] Confirmation code verification has long been established as insecure, as this

---

[36] David Temoshok et al., *Digital Identity Guidelines: Identity Proofing and Enrollment* (NIST Special Pub. 800-63A-4, July 2025).

[37] *Id.* at 14 (stating "[c]onfirmation code verification: The individual is able to demonstrate control of a piece of identity evidence through the return of a confirmation code.").

[38] *Id.* at 14–15 (stating "[v]isual facial image comparison – remote attended or remote unattended: The proofing agent performs a visual comparison of the facial image presented on identity evidence or stored by the issuing source to the facial image of the applicant engaged in the identity proofing event. The proofing agent may interact directly with the applicant during some or all of the identity proofing process or may conduct the comparison at a later time using a captured video or photograph and the uploaded copy of the evidence.").

[39] *Id.* at 15 (stating "[a]utomated biometric comparison: Automated biometric comparison (e.g., facial recognition or other fully automated algorithm-driven biometric comparison) can be performed for onsite or remote identity proofing events. The facial image or other biometric characteristic (e.g., fingerprints, palm prints, iris and retina patterns, voiceprints, vein patterns) on the identity evidence or stored in authoritative records is compared to the equivalent biometric sample collected from the applicant during the identity proofing event.").

[40] *Id.* at 18–19 (stating "[d]evice or account tenure check: Evaluate the length of time a phone service subscription or other account (e.g., email account) has existed without substantial modifications or changes. Such checks can provide additional confidence in the reliability of a device or piece of evidence used in the identity proofing process.").

[41] *Id.* at 19 (stating "[d]evice fingerprinting: Incorporate device fingerprinting checks to protect against scaled and automated attacks and enrollment duplication. Device fingerprinting is the process of collecting and analyzing the hardware and software characteristics of a device in order to create a unique identifier (i.e., fingerprint) for the device.").

[42] *Id.* (stating "[t]ransaction analytics: Evaluate anticipated transaction characteristics (e.g., IP addresses, geolocations, transaction velocities) to identify anomalous behaviors or activities that can indicate a higher risk or a potentially fraudulent event. Fraud velocity checks monitor the frequency and pattern of transactions over a specific period of time to identify unusual activity associated with transaction data. Such checks can protect against scaled and automated attacks, as well as indicate whether specific attack patterns are being executed on identity systems.").

[43] Identity proofing means "The processes used to collect, validate, and verify information about a *subject* to establish assurance in the subject's *claimed identity*."
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf

method is vulnerable to phishing attacks, stolen devices, and interception attacks.[44] Remote visual facial comparison and automated biometric comparison experience similar flaws and risks. Both approaches are weakening against the backdrop of increasingly sophisticated AI-generated synthetic media, which makes it easier to spoof face and voice biometrics.[45] Like all sensitive personal information, biometric data is an attractive target for cybercriminals.[46]

The process for checking for fraud can carry risks, as well. Device or account tenure could be discriminatory to certain groups (e.g., immigrants or young adults who have recently acquired a device or account) and would prevent them from acquiring a digital identity,[47] in turn, compromising the ethos of DeFi to be permissionless and promote financial inclusion. Device fingerprinting can contribute to identity theft if it is stolen.[48] Transaction analytics involve collecting and analyzing IP addresses and geolocations, and this behavioral analysis creates serious privacy concerns if it's outsourced to third-party contractors, housed in multiple locations, and made available to data brokers.[49]

C. Zero-Knowledge Proofs

The introduction of zero-knowledge proofs (ZKPs) are an important innovation that provides significant privacy protections to the digital asset ecosystem. As NIST explains, zero-knowledge proofs are a form of cryptography that allow for "proving the truthfulness of a mathematical statement, without revealing additional information that may have been useful in finding said truthfulness."[50] In other words, a person can reveal the validity of information without revealing the information itself.

---

[44] *Protect Users With the Confidence of Secure Identity Verification*, CLEAR (May 2, 2024), https://tinyurl.com/22uwmatx.

[45] *EPIC & ACLU Comments on NIST's 2023 Digital Identity Draft Guidelines*, Electronic Privacy Information Center (Nov. 14, 2023), https://tinyurl.com/5he747pm.

[46] *Identity Management Institute, Biometric Threats and Exploitation*, Identity Management Inst. (Jan. 3, 2024), https://tinyurl.com/3tby8ted (stating "[l]ike credit card information and other private data, biometric data, including fingerprints, facial templates, and voiceprints, can also be bought and sold on the dark web. This underground market has become a high priority for cybercriminals who wish to utilize biometric data for identity theft, fraud, and other types of cyber-attacks.").

[47] EPIC & ACLU, *Comments on NIST's 2023 Digital Identity Draft Guidelines* (stating "[f]raud prevention is an important element of any identity proofing scheme, but frequently poses an unnecessary barrier to individuals claiming benefits. The harms of poorly designed fraud prevention technologies fall hardest upon marginalized groups including Black and Brown communities, immigrants, low-income individuals, the elderly, and people living in rural areas. The touchstone for fraud prevention tools should be equity. Tools that exhibit bias or a propensity for error should not be used, even if they claim to be highly effective.").

[48] *What Is Device Fingerprinting?*, Arkose Labs (Apr. 4, 2024), https://tinyurl.com/55zmf3z8 (arguing that "[i]n some cases, device fingerprints may be used to identify and authenticate users. This can be problematic if the fingerprint is used as the sole method of identification or authentication, as it can potentially be stolen or spoofed.").

[49] EPIC & ACLU, *Comments on NIST's 2023 Digital Identity Draft Guidelines*.

[50] NIST, *ZKProof Project*, Cybersecurity and Infrastructure Security Agency, NIST, https://tinyurl.com/r92rwwzw.

While there are various approaches to designing ZKPs' incorporation into a tool, generally the process is as follows:

1. First, a person employs some method for scanning their government-issued identification documents, like a passport or ID card, to serve as their credential.[51]

2. These scanned documents are submitted to an issuer, and after proving the person is who they say they are, the issuer digitally signs the credential with their cryptographic private key.[52]

3. After receiving the issuer's signed credential, a user then generates a ZKP locally on their device using the same application they used to receive the issuer's proof.[53]

4. The user presents the ZKP to any service provider that requires digital identity verification.[54]

Similarly, smart contract digital identity verification allows users to maintain privacy when verifying their identity using a smart contract. However, the use of ZKPs in digital identities is only one step towards safer user privacy. While ZKPs prevent public exposure of a users' sensitive personal information and activities on the blockchain, the real privacy risk still exists with verifiable credential issuance.

To comply with U.S. policy, an issuer would likely still need to retain PII, creating repositories of sensitive personal information ripe for data breaches or leakages that ZKPs cannot prevent or remove. Furthermore, while ZKPs protect the underlying information, they do not obfuscate that they are being used in the first place. Specifically, ZKPs are incredibly effective at offering user privacy from the verifier and other parties, but ZKPs do not themselves prevent the verifier from notifying the issuer of the fact a ZKP is being used with certain verification designs. This design is functionally the same risk as maintaining issuance logs.

While private, decentralized solutions continue to emerge to mitigate the risks of digital identities,[55] this does not suggest the federal government should mandate any particular system

---

[51] Andre Omietanski & Amal Ibraymi, *How to Enable Age Verification on the Internet Today Using Zero-Knowledge Proofs*, Aztec Network (May 14, 2025) at 5, https://tinyurl.com/3hsb7nj3.

[52] *Id*. at 6.

[53] Importantly, when users generate a ZKP, the secret inputs never leave their device.

[54] Omietanski & Ibraymi, Aztec Network (May 14, 2025), at 7.

[55] Peter Van Valkenburgh & Ian Miers, *Tear Down this Walled Garden: American Values and Digital Identity*, Coin Center, Version 4 (Sept. 2025), https://www.coincenter.org/tear-down-this-walled-garden/ (detailing how one emerging approach is to not let ZKPs work on their own and incorporate other mechanisms—specifically, multi-party computation (MPC)—in the verification process to further ensure privacy. Specifically, in the event that

of digital identity verification. Instead, the federal government should consider working with the private sector to ensure development of this technology is done safely and with an eye toward respecting individual's privacy, while developers are free to innovate improved technological solutions. Development in digital identity verification systems must minimize—or altogether eliminate—information retention, especially by centralized actors. And, while blockchain technology offers contemporary solutions to such risks, incorporating new technology will require thoughtfulness, collaboration, and an appetite for innovation.

D. Constitutional Considerations

Digital identity verification systems also pose constitutional concerns. For example, mandating digital identity verification in smart contracts implicates Fourth Amendment issues related to a person's right to be free from unreasonable searches and warrantless surveillance. Software developers make publicly-available software tools, such as smart contracts, that allow others to execute self-directed, peer-to-peer transactions while maintaining custody of their own funds. In DeFi, where there is no intermediary involved in a person's financial transaction, developers have no business or operational purpose to identify users, nor any technical capability to do so, and users have no reason to voluntarily provide their PII to developers with whom they are not in any kind of commercial relationship. Imposing digital identity mandates would inevitably require the collection of PII that would implicate a user's Fourth Amendment rights and fall outside the purview of the third party doctrine, explained below.

For background, the BSA's information collection and reporting regime was predicated on the notion that customers voluntarily provide their personal information in order to use traditional financial services. In the United States Supreme Court case *Katz v. United States* (1967), the Court held that the Fourth Amendment protects people from government searches when they have a "reasonable expectation of privacy" in the instance the search occurred. This holding was extended in *United States v. Miller* (1976), creating what is now known as the "third party doctrine," which states that a person does not have a reasonable expectation of privacy when they voluntarily surrender their information to a third party. This was further discussed in *Smith v. Maryland* (1979), where the Court permitted the government to "constitutionally compel telephone companies to report phone numbers dialed by customers without a warrant because those customers were already 'voluntarily' conveying that information for the telephone company's 'legitimate business interests.'"[56]

---

a user (i.e., holder) requires multiple institutions to provide cross-institution signals (i.e., facts or risk indicators), those parties run an MPC and output a sealed result. The user can then wrap this result with a ZKP and the verifier checks the ZKP against anchors (e.g., issuer keys and revocation/status of credentials) that are published openly on the blockchain. Verifiers would check against these anchors to avoid notifying the issuer.)

[56] Miller Whitehouse-Levine & Amanda Tuminelli, *Comment on the Proposed Rule on Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions (REG-122793-19)*, DEF (Nov. 7, 2023), at 13, https://tinyurl.com/3ywf98zw.

However, the expansion of the third party doctrine was challenged in *Carpenter v. United States* (2018), when the Supreme Court ruled that "the government cannot compel telephone companies to turn over customer location data gleaned from cell phone tower connections, because 'in no meaningful sense does the user voluntarily assume risk of turning over a comprehensive dossier of his physical movements,' and the telephone companies do not need customer location data to connect calls."[57] The same principle holds true in DeFi: users do not voluntarily identify themselves or assume the risk they will be identified in order to use publicly available, decentralized software, because the pseudonymous software does not itself require personal identification in order to function.

As DEF argued in an amicus brief to the Supreme Court in *Harper v. Werfel*, "[the Supreme Court] was careful not to make third-party sharing *sufficient* to defeat a person's right to privacy."[58] Further, *Smith* and *Miller* established three restrictions on the third party doctrine. First, that "the third parties gave the records to the government 'voluntarily,'" meaning that the third parties involved in each case were not coerced by the government to surrender such records.[59] Second, that "the records accessed in *Smith* and *Miller* were limited" and did not involve "encyclopedic or intimate information" but merely "a day's worth of phone numbers, and a handful of business records."[60] Thus, *Smith* and *Miller* restricted the government to obtaining "limited" information under the third party doctrine and did not intend for the government to be "free to use the same method to obtain millions of records or more sensitive information."[61] Third, both *Smith* and *Miller* involved a single person against "whom the government had strong evidence of criminality," meaning "[p]robable cause likely existed against both Smith and Miller" and "[t]he government did not ask for papers of anyone else."[62] *Carpenter* affirmed these limitations on the third party doctrine and acknowledged how information can "revea[l] not only [the person's] particular movements, but through them his 'familial, political, professional, religious, and sexual associations,'" and without protections, the government could access sensitive records "for everyone at 'practically no expense.'"[63]

Requiring DeFi developers to implement digital identity verification into blockchain protocols and mandating a redesign of their software would stretch the third party doctrine, violating users' privacy rights. Such a mandate would be coercive, implicate intimate information, and not be based on strong evidence of criminality on the users. Moreover, once identified, a user's blockchain transactions are easily traceable and would reveal highly intimate information that the Court did not believe the government should so easily access in *Carpenter*.

---

[57] *Id*.

[58] Brief for DeFi Education Fund as *Amicus Curiae* in Support of Petitioner at 7, *Harper v. Werfel*, No. 24-922 (U.S. Mar. 28, 2025) (captioned *Harper v. O'Donnell* at filing), https://tinyurl.com/4ksn3krp.

[59] *Id.* at 9.

[60] *Id.*

[61] *Id.* at 10.

[62] *Id.*

[63] *Id.* at 11.

As DEF wrote, "[t]he Court has repeatedly admonished that when 'advancing technology' makes searches more intrusive, the Fourth Amendment doctrine must recalibrate to 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[64]

III. Response to Illicit Activity Risks Involving Digital Assets

Where in the past, bank robbers were the primary threat to the financial system—attempting to physically infiltrate bank vaults or steal paper records—in the Digital Age, it is the hacker who poses the greatest threat to the traditional financial system and the digital asset ecosystem. Therefore, the U.S. government should focus on cybersecurity solutions for the digital asset eco, and be mindful not to conflate rapidly evolving technology with what is inherently a cybersecurity risk that exists regardless of the technology involved.

For example, while there is no doubt North Korea—and specifically the Lazarus Group—have significant hacking capabilities, North Korea frequently relies on social engineering and supply-chain attacks to compromise their targets.[65] These are common cybersecurity threats that require manipulating people to provide access or sensitive information and compromising trusted third-parties to reach their actual targets.[66]

At its foundation, the digital assets ecosystem has always been focused on developing a secure means for transacting electronically. It is therefore pertinent to focus efforts on strengthening cybersecurity and on building a private-public partnership for addressing hacks, as there are many trusted cryptographers and cybersecurity experts within the industry who can serve as a primary resource.[67]

The DeFi industry has begun these efforts on its own accord, without any rules requiring them to do so, with a variety of coalitions and response groups. For example, the introduction of the Security Alliance (SEAL) was established in 2024 to remedy security risks, provide legal protection for white hat hacking in the digital asset ecosystem, and help with incident response,

---

[64] *Id.* at 16-17.

[65] Samczsun, *Demystifying the North Korean Threat* (Mar. 31, 2025), Paradigm, https://tinyurl.com/cbvudj4u.

[66] Mario Rivas, Ruben Santos & Jorge Sanz, *In-Depth Technical Analysis of the ByBit Hack*, NCC Group (Mar. 10, 2025), https://tinyurl.com/363mv38m (explaining the ByBit hack was a supply-chain attack and not indicative of the underlying digital asset technology. Hackers targeted the Safe{Wallet} application—which requires multiple private-key holders to sign a transaction—by compromising one of their developer's machines and injecting malicious code into their user interface. The ByBit private-key holders, relying on the manipulated interface, were presented with what appeared to be a routine internal transfer of funds, which led them to approve a transaction that subsequently drained their depository).

[67] DEF, *Comment on the Senate Banking Committee's Digital Asset Market Structure Request for Information on Decentralized Finance* (Aug. 1, 2025), at 15, https://tinyurl.com/5auzxzxu.

among other initiatives.[68] And, in August 2025, TRM Labs launched a crypto crime response network known as the Beacon Network in collaboration with law enforcement, exchanges, and stablecoin issuers.[69]

The DeFi industry has also developed competitive marketplaces for security audits of DeFi protocols, as well as industry standards of making such protocols open-source for broad inspection and audit. On platforms like Immunefi, auditors are able to identify vulnerabilities and submit their reports to protocol developers, often receiving compensation for their audits and developing a sustainable market for such work.[70]

These initiatives and others—which are crucial in strengthening cybersecurity and developing a rapid response against illicit actors—are discussed in the additional response DEF sent to Treasury's RFC, alongside Solana Policy Institute and Paradigm.[71] We strongly encourage the federal government to increase engagement with these initiatives. One additional approach to consider is the creation of a joint task force, led by NIST and consisting of industry experts, that develops and solicits public feedback on cybersecurity standards for blockchains and smart contracts. In this way, software developers will be provided with best practices to incorporate into their software and mitigate evolving illicit activity risks through sound cybersecurity.

* * *

DEF sincerely appreciates the opportunity to provide comments on the RFC, and we stand ready and willing to assist Treasury and its government partners in addressing these challenges.

Sincerely,

Lizandro Pieper
Research Director
DeFi Education Fund

---

[68] Security Alliance (SEAL), https://www.securityalliance.org/ (a coalition launched in 2024 focused on security risk mitigation, legal protection for white-hat hackers, and incident response in the digital asset ecosystem).
[69] TRM Labs, *TRM Labs Launches Beacon Network, the First Real-Time Crypto Crime Response Network*, TRM Labs Blog (Aug. 20, 2025), https://tinyurl.com/5xuapvsx (announcing TRM's creation of the Beacon Network, a collaborative crypto crime response system with law enforcement, exchanges, and stablecoin issuers).
[70] Immunefi, *Bug Bounty Program*, https://immunefi.com/bug-bounty-program/ (describing a marketplace that connects protocols with security experts and "white-hat" hackers to run bug-bounty programs and coordinate vulnerability disclosure and payouts).
[71] *Available at* https://www.defieducationfund.org/_files/ugd/84ba66_c10e175b10a7465582a39f806887efab.pdf, and also submitted to the Federal Register on October 17, 2025, Comment Tracking Number: mgv-1ydq-l3wh.