

May 28, 2024

Director Andrea M. Gacki

U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)

Delivered via Federal eRulemaking Portal: <https://www.regulations.gov>

Re: Request for Information and Comment on Customer Identification Program Rule Taxpayer Identification Number Collection Requirement

Dear Director Gacki,

We extend our sincere appreciation to you and the esteemed staff at the Financial Crimes Enforcement Network (FinCEN) for the opportunity to provide input on the RFI related to existing requirements for banks under the Customer Identification Program (CIP) Rule.

FinClusive Capital, Inc. acknowledges the longstanding importance of the requirement for banks to collect identifying information from customers prior to opening an account as a fundamental component of anti-money laundering efforts. We commend FinCEN's proactive stance in recognizing the evolution of technology and financial services since the promulgation of the CIP Rule.

As a forward-thinking entity committed to advancing financial integrity and inclusivity, we embrace the notion of modernizing the U.S. anti-money laundering/countering the financing of terrorism (AML/CFT) regime to adapt to contemporary challenges and opportunities. Our organization fully supports FinCEN's initiative to explore potential enhancements to the CIP Rule, leveraging advancements in customer identifying information collection and verification tools.

We believe that allowing banks to collect partial Social Security number (SSN) information from customers, with subsequent validation from reputable third-party sources prior to account opening, holds promise for streamlining processes without compromising security. Updating the CIP Rule to accommodate new technological capabilities will not only streamline compliance processes but also improve the inclusivity and efficiency of financial services.

Overview of FinClusive

By way of background, FinClusive is a regulatory technology company—specifically, a [global Compliance-as-a-Service \(CaaS\) infrastructure provider](#) that enables increased financial engagement through modernized financial crimes compliance and anti-money laundering (FCC/AML) tools. These tools enhance and strengthen compliance, risk, and governance systems for both traditional and nontraditional financial services companies. They allow our banking and payment partners to confidently demonstrate compliance with global banking standards while expanding their services and engagement to businesses, communities, and alternative technologies that have been traditionally underserved or unwelcomed within the global financial system. These include alternative nonbank and embedded finance applications, as well as decentralized (DeFi) and Web3 financial services products and services.

FinClusive's [Compliance-enabled Credential Environment \(CECE\)](#) connects traditional banking with blockchain-enabled payments, virtual asset networks, and Web3 financial services applications. We do this by providing an embedded FCC/AML application built for both traditional

and alternative financial services companies, including virtual asset service providers. FinClusive's CaaS application is a full-stack AML orchestration layer integrating best-in-class providers to cover global know-your-customer/know-your-business (KYC/KYB), monitoring, watchlist, and sanctions screening, transaction tracking, analytics, and compliance-backed digital identity and verifiable credential capabilities.

These digital identity tools support both centralized and decentralized applications and enable the secure sharing of information across and between financial services providers about their shared customers and counterparties. Furthermore, they are designed to enable essential privacy protections and control by the clients for whom these decentralized identifiers (DIDs) and compliance-backed verifiable credentials (CVCs) are created. With both Web2 and Web3 enablement, CaaS is intended to facilitate 'embedded compliance' by and between traditional as well as decentralized and web-based financial services through a comprehensive toolkit of AML controls in one application.

CaaS provides [compliance-backed, digitally verifiable identity credentials—FinCIDs](#)—and [legal entity identifiers \(LEIs\)](#) to clients, enabling a global standard utility for KYC/KYB verification across various financial and payment networks and service providers. Our team comprises experienced professionals in banking, payments, financial technologies, and regulatory compliance and supervision—including former senior U.S. regulatory officials from the U.S. Treasury and Federal Reserve Bank (FRB), among other federal financial regulatory and supervisory agencies.

Current Challenges and Opportunities for Modernization

Current Landscape

In the existing financial ecosystem, particularly under Web2, consumer data is not self-owned but is held across fragmented, centralized systems. This structure has not only led to significant data breaches—affecting approximately [2.6 billion records over the past two years](#)—but also to a system where consumers have limited control and visibility over their personal information. These vulnerabilities are further exacerbated in cross-border transactions and highlight the urgent need for a regulatory shift towards more secure, transparent, and consumer-centric technologies like those offered by Web3."

Web2 federated identity systems, despite offering the convenience of accessing multiple services with one set of credentials, fall short of achieving the Personal Financial Data Rights policy objectives. These systems lack robust control and security features and are dependent on centralized authorities, introducing vulnerabilities and potential points of failure. This centralized approach restricts consumers' autonomy and limits their visibility into how their data is shared or used, posing ongoing risks of data misuse and unauthorized access.

The situation is compounded in a cross-border context where personal and economic data traverse largely unregulated intermediaries and jurisdictions with minimal controls and supervisory efforts. The increasing involvement of payments services, banking as a service (BaaS), and client-facing fintech heightens these risks as these entities may not prioritize data privacy in the same way. Despite these challenges, consumers deserve comprehensive protection for their personal and financial data, a right that should be universally upheld.

Policy framework and the “same activity, same risk, same regulation” principle

In 2019, FinClusive initiated a grassroots, open-source effort to integrate traditional finance with the burgeoning virtual asset market by creating the "[Rulebook](#)." This dynamic framework, published under a Creative Commons license, sets compliance standards for nonbank financial services, decentralized finance (DeFi), and blockchain activities. The full framework, named the [Compliance & Inclusive Finance Rulebook](#), is publicly available.

FinClusive has also partnered with the [Sovrin Foundation](#) and other global entities to form the [Compliance and Inclusive Finance Working Group \(CIFWG\)](#). This group aims to establish essential controls and promote self-governance within the rapidly growing virtual asset sector, ensuring that these services comply with regulatory safeguards while supporting a secure, accessible financial system.

The "Rulebook" developed by the CIFWG addresses both traditional and emerging financial services, including token-based transactions and other virtual asset network activities. This best-practices governance framework is informed by global regulators and designed to be flexible, reflecting the operational realities of advanced payment technologies and building upon existing governance and data privacy rules.

The approach shifts from entity-based regulation to focusing on "activities and practices," advocating for financial regulatory frameworks that adapt to ongoing innovations. Importantly, it enables new and innovative financial services providers that emerge outside traditionally regulated spaces to ensure appropriate and similar FCC controls inherent in such activities. This principle aligns with the FSB Recommendations, which suggest "same activity, same risk, same regulation." It applies to network participants involved in creating, storing, transacting, or providing liquidity for digital units of value, enabling them to navigate AML and financial compliance responsibilities effectively.

This modernized regulatory approach aims to protect the global financial system from illicit activities, support financial inclusion, and ensure that emerging financial technologies can serve underserved and unbanked communities without being hindered by outdated regulations. The Rulebook exemplifies a shift towards a regulatory framework that is nimble yet effective in managing the complexities of a cross-border, peer-to-peer financial ecosystem.

Identity is central to FCC and Privacy

The central role of identity is underscored by the need for covered institutions to understand for whom they are providing services. Access and AML/FCC requirements revolve around the central question of KYC (and KYB), which are essential for effective onboarding, client risk evaluation, and ongoing monitoring. This includes core elements related to CDD and CIP as part of the five core pillars. Identity verification involves establishing, authenticating, and authorizing identity, enabling institutions to link properties and assets to a person with a verified identity.

Identification is based on resolving an identity, ensuring the bona fides of a person using trusted, reliable sources to achieve confidence that the person not only exists but is actually the one engaging with the institution. The strength of the identification process contributes directly to the

integrity of information used to discern connections to potential proceeds of crime and separate illegitimate from legitimate assets.

Global guidance for KYC includes both traditional and modernized digital identity systems, emphasizing the importance of identity management and verification for financial institutions to prevent access by illicit actors while being inclusive to legitimate participants. The Financial Action Task Force (FATF) provides extensive guidance on KYC to address AML/CFT and broader FCC issues, specifically recommending digital identities that use reliable sources to ensure trustworthiness. During the global COVID pandemic, FATF emphasized the need to explore digital identity solutions to modernize financial services and manage security risks.

Many developed economies have enhanced the security features of paper-based identities, making them more resistant to forgery and exploitation in synthetic identity fraud schemes. However, simply providing paper-based identities to the underbanked does little to address the issues faced by the unbanked. Overreliance on static personal identifying information (PII) exacerbates identity management challenges in many financial institutions, leading to problems such as difficulty in opening new accounts and high losses from new account fraud. The [U.S. Federal Reserve reported](#) in 2019 that synthetic identity fraud is costing U.S. lenders \$6 billion annually and is the fastest-growing type of financial crime in the country. Additionally, the volume of PII data exposed in data breaches has increased by 126% over the past decade, with more than 446 million records exposed.

In the U.S., we often take for granted that we are provided a birth certificate and social security card at birth without cost. However, for individuals in rural and remote regions of the world, obtaining a physical identification from a central authority can be time-consuming and costly, potentially resulting in lost income, especially for those living on the poverty line. Furthermore, over-reliance on centralized government-issued documentation does little to address the plight of [approximately 850 million people around the world do not have an official ID and over 1 billion people who do not have a digital record of their identity](#).

Jurisdictional regulations often limit the effectiveness of certain government-issued identities across borders, exacerbating exclusion due to interoperability issues or failing to meet cross-border data and authentication standards. Given the global nature of finance and the digitization of our economies, there is a critical need for alternative and digital identity representations. This will allow individuals and organizations to function more effectively in an increasingly web-native and cross-border world. Consequently, identity should be recognized as a fundamental human right, essential for accessing key services.

Digital access and inclusion are crucial across industries, particularly in sensitive or 'highly regulated' sectors like finance, healthcare, and education, which increasingly operate online. As global interconnectedness expands, the mechanisms to ensure safe and secure operations must also evolve.

The digital shift requires new trust models for information sharing, which is challenging in a vulnerable cyber world and raises concerns for regulators and policymakers focused on consumer protection and financial system integrity. Digitization amplifies the flow of sensitive data, heightening risks of misuse and unauthorized access. This prevalence in federated and centralized

systems weakens protections against data exploitation by companies and restricts consumers' control and transparency over their data usage across platforms.

Digital information handling must empower both institutions that rely on identity verification for security and access, and individuals whose personal data is essential for services like banking. Thus, identity and KYC/KYB standards should include strong security features to protect both consumer and business privacy. Moreover, individuals and organizations should control how their information is disclosed and used by third parties, ensuring it remains secure from exploitation. This makes self-sovereign identity (SSI) and Web3 ID solutions both promising and necessary.

As finance and banking grow increasingly seamless across jurisdictions, financial compliance regulation and oversight lag behind. Identity is central to these efforts, and cross-jurisdictional identity verification methods significantly enhance KYC and broader FCC obligations. Such solutions bolster financial system integrity, mitigate fraud and illicit activities, and strengthen privacy controls simultaneously.

Proposed Solutions

Web3 and New Technologies

Web3 signifies a revolutionary paradigm shift in the digital landscape. Unlike its predecessors, Web3 leverages blockchain technology to empower individuals with complete control over their identities and personal data on decentralized platforms across an open-architected web. More financial services companies are issuing (creating), transacting, and redeeming value across Web3 applications, which also offer efficiencies that come with an 'always on' financial services environment. Transactions can be settled between counterparties directly (with no bank/financial intermediary involved), instantaneously, 24/7, 365 days a year.

Web3 guarantees that data is no longer restricted to centralized repositories but distributed across users' devices, creating a secure and transparent environment. Its architecture—emphasizing decentralization, permissionless and trustless transactions, and cryptographic security—seamlessly aligns with the principles of self-sovereign identity. This empowers users to assert authority over their digital personas and data, liberating them from the constraints of traditional, centralized systems.

Web3 standards and technological implementations shouldn't be overlooked in discussions about the proposed rule, whether in current or future implementations. Doing so would severely limit consumers' ability to update their personal "tech stack" as businesses and financial institutions (FIs) innovate new solutions granting access to covered data. Moreover, Web3-enabled tools are proving effective in supporting key aspects of financial system integrity controls. These include enhancing payment transparency through verifiable credentials attached to transactions across various payment rails and types.

Importance of Decentralized Identity and Verifiable Credentials

Enabling digital information management can strengthen covered financial institutions (FIs) in their mandated handling and verification of clients' identities. This enhancement brings both security and efficiency to KYC, CDD, and CIP processes. Web3 ID solutions provide a promising and

necessary path forward, contrasting with Web2 federated identity systems, which are vulnerable to risks associated with centralization and often reliant on outdated, paper-based systems that are prevalent worldwide.

Modernizing identity management and verification will enable financial market infrastructure to better align with the Personal Financial Data Rights policy objectives required in an increasingly digitized financial services economy. This priority has recently been addressed by the [Consumer Financial Protection Bureau \(CFPB\)](#) and the [White House](#). Relying on centralized authorities creates potential single points of failure among other challenges.

Harnessing Web3 for personal and financial data control hinges on integrating decentralized identifiers (DIDs) and compliance-backed verifiable credentials (CVCs). DIDs give individuals ownership of their compliance information, allowing them to securely share it with their chosen financial institutions and service providers. CVCs streamline identity verification processes by embedding essential controls driven by Know Your Customer/Know Your Business (KYC/KYB) requirements, associated due diligence, and monitoring. CVCs also reduce costs for financial institutions while maintaining individuals' control over their financial identities, providing a value-added 'asset' to both service providers (increased secure engagement with their consumers and partners) and consumers (essential consumer protections related to their personal and proprietary identifying and economic data).

Web3ID and the use of DIDs/VCs ensure that sensitive personal and economic data are distributed across users' respective devices and financial intermediary services, fostering a secure and transparent environment. The architecture reinforces essential attributes: decentralization, permissionless and trustless transactions, and cryptographic security. This enables users to assert authority over their digital personas and sensitive personal and economic data. With identity verification and management at the core of cross-jurisdictional approaches to KYC/KYB, CIP, and broader FCC obligations, DIDs/VCs reinforce essential financial system integrity controls that serve to mitigate fraud and illicit activities while strengthening essential privacy controls in tandem. In an increasingly web-native financial (and other commercial and social applications) global environment that is increasingly using tokenized value in payments and other services, Web3 and related technology stacks advance our broader economic security, consumer protection, and frictionless finance goals.

FinClusive believes that the use of DIDs and CVCs could play a significant role in ensuring that essential information about transaction senders and receivers is provided. These identifiers carry attestable attributes that substantiate this information without needing to disclose it within the payment chain, regardless of the intermediaries and payment rails involved.

Issuer-Holder-Verifier Model: A Consumer-Centric Approach for Web3 Digital Identity

One DID and CVC implementation model worth considering is the Issuer-Holder-Verifier model, which underscores a transition towards a consumer-centric approach to data control. In this model, consumers become the rightful holders of their personal data, establishing direct relationships with verifiers. This ensures a secure and transparent process for data verification without compromising privacy, a stark departure from the traditional centralized and intermediary-dependent model. This new model attaches attestable attributes to an individual or entity for verification and authentication alongside financial data, account credentials, and other identifiers,

enhancing privacy. It allows regulated institutions, like banks, to validate individuals' verified statuses without exposing sensitive information.

Legal Entity Identifier for Emerging Markets and Driving Greater Inclusion

FinClusive advocates for the widespread use of Legal Entity Identifiers (LEIs) across all financial services activities involving legal entities. LEIs enable entities of all types to engage in payments activities compliantly and securely, ensuring their verifiability and validity throughout transactions. These identifiers validate the identity of business entities and are increasingly integrated with SWIFT and Business Identifier Codes (BICs), simplifying their assignment across various financial services sectors, including money service businesses, card issuers, banks, mobile wallets, and others. While BICs may not always accurately link to specific legal entities involved in a payment, their combination with LEIs enhances the verification of business units within these entities.

GLEIF is the sole global online source for open, standardized, and high-quality legal entity reference data, adhering to ISO standards. Supported by the G20 and the Financial Stability Board, the LEI system is becoming the global standard for identifying business entities. Notably, FinClusive is one of the few US-based issuers and verifiers of LEIs, operating within the global business registry managed by the GLEIF Foundation.

This system offers trading partners and financial institutions a new level of efficiency, promising significant benefits for global trade and business-to-business transactions. From small businesses and nonprofits to global corporations and alternative financial service providers, entities can obtain a credible LEI through FinClusive, enhancing their participation in the global economy with legitimacy and transparency.

FinClusive advocates for the adoption of LEIs for all merchants and offramps in payment protocols, not just for cross-border wires. In its absence, full KYC measures are necessary to mitigate risks.

Conclusion

FinClusive wholeheartedly supports FinCEN's initiative to modernize the Customer Identification Program (CIP) Rule in alignment with today's technological advancements that enable greater efficiencies in client engagement, verification, and ongoing monitoring. We believe that enhancing the rule to include the collection and verification of partial Social Security numbers, verified through trusted third-party sources, will not only improve the efficiency and inclusivity of the financial services industry but also maintain the robust security standards necessary for effective anti-money laundering efforts. Additionally, allowing the use of modern digital identity tools, including those that embed compliance/KYC/KYB processes into shareable forms of identity verification, will enhance privacy protections while advancing the efficient and secure verification/validation of unique identifiers associated with financial services clients.

Our commitment to advancing financial integrity and inclusivity through innovative, compliance-backed solutions such as our Compliance-as-a-Service (CaaS) infrastructure and the Compliance-enabled Credential Environment (CECE) is a testament to our dedication to these principles. By bridging traditional banking with blockchain-enabled payments and virtual asset networks, we aim to facilitate seamless and secure financial transactions that uphold the highest standards of compliance and consumer protection.

We appreciate the opportunity to contribute to this critical discussion and look forward to any further dialogue with FinCEN as you consider updates to the CIP Rule. We remain at your disposal to discuss the capabilities described herein and the ongoing work we are undertaking to embed essential AML/FCC controls rooted in privacy enhancements and security for sensitive personal data, which continue to be the cornerstone of financial system integrity initiatives. Thank you for considering our perspective and for your continued commitment to enhancing the security and efficiency of the financial services landscape.

With our best regards,

FinClusive