SpruceID

Spruce Systems, Inc.
228 Park Ave S, PMB 28788
New York, New York 10003-1502

VIA REGULATIONS.GOV

October 17, 2025

U.S. Department of the Treasury
Scott Bessent
Secretary of the Treasury
1500 Pennsylvania Ave., NW
Washington, DC 20220

Re: Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets, Docket Number–2025-0070.

Dear Secretary Bessent:

We appreciate the opportunity to respond to the Department of the Treasury's ("Treasury") request for comment on the use of innovative or novel methods, techniques, or strategies to detect and mitigate illicit finance risks involving digital assets.

Spruce Systems Inc. (dba SpruceID) is a U.S.-headquartered company with a stated mission of letting users control their data across all digital interactions. SpruceID provides end-to-end solutions for digital licensing, permitting, and identity. We specialize in delivering lifecycle management systems for government-issued credentials that are secure, privacy-preserving, and interoperable across ecosystems. Our approach is built on verifiable digital credential (VDC) technology, which reduces the cost and complexity of in-person verification while protecting individual privacy in online interactions.

Our response addresses all of Treasury's questions in a comprehensive and integrated manner, offering a cohesive solution that reflects both technical feasibility and policy alignment. The structure below outlines the key components of our submission and how they correspond to Treasury's areas of inquiry:

Executive Summary

The Bank Secrecy Act (BSA), enacted in 1970 to detect and deter financial crime in a paper-based era, now underpins a vast anti–money laundering and countering the financing of terrorism (AML/CFT) regime that has become increasingly costly and inefficient in the digital age. Despite continuous expansion, the current system delivers limited impact: U.S. financial institutions spend roughly $59 billion annually on financial crime compliance, yet only an estimated 0.2% of illicit proceeds are ultimately seized. Rising costs fall disproportionately on smaller institutions—community banks devote up to 9% of non-interest expenses to compliance—driven by manual processes, false positives, and fragmented data systems. The result is a regime that encourages "de-risking" and the exclusion of vulnerable customers: as of 2023, 4.2% of U.S. households remained unbanked and 14.2% underbanked, with the highest rates among low-income, minority, and single-parent households. Modernization of the BSA/AML framework is therefore imperative to enhance effectiveness, reduce burdens, and promote equitable financial inclusion in the digital economy.

The technology to strengthen and improve this out-dated system exists today. Verifiable digital credentials (VDCs) such as mobile driver's licenses (mDLs) and cryptographic trust identity frameworks have proven scalable and secure in other domains. Seventeen U.S. states now issue mDLs, with more than a dozen others developing programs,[1] and the TSA already accepts them at over 250 airports.[2] These digital credentials are bound to a user's device, resistant to tampering, and capable of selective disclosure—enabling, for instance, proof of age without revealing full identity details. Combined with modern cryptography and open APIs, these technologies are ready to integrate directly into financial institutions' compliance systems today, provided there is a regulatory environment that recognizes and approves their use for AML/CFT compliance. These technologies can be leveraged as powerful AML/CFT tools that make compliance more effective without the financial and social costs of third party surveillance.

The **Identity Trust** model enables regulated entities, such as banks or state- or nationally-chartered trusts, to verify individuals, issue pseudonymous cryptographic credentials, and manage lawful access through auditable key systems. It operates within existing regulatory frameworks, limited to contexts that explicitly require identification under laws like the BSA. The model unfolds in four stages:

1. **Identifying:** A regulated Identity Trust verifies individual identities and issues encrypted, pseudonymous credentials protected by multi-party keys.
2. **Transacting:** Transactions use one-time-use identifiers to preserve unlinkability while maintaining auditability.
3. **Investigating:** Lawful access is granted through threshold key recovery, balancing enforcement needs with individual privacy.
4. **Monitoring:** Enables real-time screening for suspicious activity and sanctions list updates with continuous attestations, such as credit or sanctions status, conducted in a privacy-preserving, policy-driven and auditable manner.

These mechanisms create a foundation for a more adaptive and privacy-preserving compliance regime—one that aligns regulatory oversight with modern technology. To enable their adoption at scale, we propose several policy updates and regulatory clarifications for Treasury's consideration. Our top requests and their reasoning are summarized in the following table:

Summary of Suggested Recommendations: *Modernizing AML/CFT Rules for the Digital Asset Economy*

Request for Consideration	Reasoning and Impact
1. Recognize verifiable digital credentials (VDCs) issued by many acceptable sources as valid evidence under Customer Identification Program (CIP) and Customer Due Diligence (CDD) obligations, including as "documentary" verification methods when appropriate. Treasury and FinCEN should interpret 31 CFR § 1020.220 (and corresponding CIP rules and guidance) to include verifiable digital credentials if they can meet industry standards, such as a baseline of National Institute of Standards and Technology (NIST) SP 800-63-4 Identity Assurance Level 2 (IAL2) identity verification or higher, issued directly from government authorities, or through reliance upon approved institutions or identity trusts. These verifiable digital credentials (VDCs), such as those issued pursuant to the State-Endorsed Digital Identity (SEDI) approaches, should be treated as "documentary" evidence where appropriate. The principle of data minimization should become a pillar of financial compliance, enabling VDC-enabled attribute verification encouraged over requiring the sharing of unnecessary personally identifiable information (PII), such as static identity documents, where possible.	Current CIP programs largely presume physical IDs, limiting innovation and remote onboarding, even as the statute is not prescriptive in medium or security mechanisms. Verifiable digital credentials issued by trusted authorities provide cryptographically proven authenticity and higher assurance against forgery or impersonation, to better fulfill the aims of risk-based compliance management programs. Recognizing VDCs as documentary evidence would enhance verification accuracy, reduce compliance costs, and align U.S. practice with FATF Digital ID Guidance (2023) and EU eIDAS 2.0, promoting global interoperability. Attribute-based approaches to AML, such as "not-on-sanctions-list" or "US-person," should be preferred whenever possible as they can effectively manage risks without the overcollection of PII data, avoiding a "checkpoint society" riddled with unnecessary ID requirements.
2. Permit financial institutions to rely on VDCs issued by other regulated entities, identity trusts, or accredited sources via verified real-time APIs for AML/CFT compliance. Treasury and FinCEN should authorize institutions to accept credentials and attestations from peer financial institutions or identity trust networks when those issuers meet assurance and audit standards. Congress should further consider the addition of a new § 201(d) to the *Digital Asset Market Structure Discussion Draft (Sept. 2025)* clarifying Treasury's authority to	While current CIP programs still assume physical ID presentation, the underlying statute is technology neutral and does not mandate any specific medium or security mechanism. Recognizing VDCs can modernize onboarding by reducing costs and friction, improving AML data quality and transparency, and enabling faster, more collaborative investigations across institutions and borders—all while minimizing data-collection risk. Statutory clarity ensures that Treasury's modernization efforts rest on a durable, technology-neutral foundation. This amendment would future-proof the U.S. AML/CFT regime, align it with G7 digital-identity roadmaps, and strengthen U.S. leadership in global digital-asset regulation.

recognize and accredit digital-identity and privacy-enhancing compliance frameworks.	
3. Permit privacy-enhancing technologies (PETs) to meet verification and monitoring obligations. Treasury should issue interpretive guidance or rulemaking confirming that zero-knowledge proofs, pseudonymous identifiers, and multi-party computation may be used for CIP, CDD and Travel-Rule compliance if equivalent assurance and auditability are maintained.	PETs enable institutions to prove AML/CFT compliance without exposing underlying PII, minimizing data-breach and insider-risk exposure while maintaining verifiable oversight. Recognizing PETs would modernize compliance architecture, lower data-handling costs, and encourage innovation consistent with global privacy and financial-integrity standards.
4. Modernize the Travel Rule to enable verifiable digital credential-based information transfer. Treasury should amend 31 CFR § 1010.410(f) or issue guidance allowing originator/beneficiary data to be transmitted via cryptographically verifiable credentials or proofs instead of plaintext PII.	The current Travel Rule framework was built for wire transfers, not blockchain systems. Verifiable digital credentials can carry or attest to required information with integrity, selective disclosure, and traceability. This approach preserves law-enforcement visibility while protecting privacy, ensuring interoperability with FATF Recommendation 16 and global Virtual Asset Service Providers (VASPs).
5. Establish exceptive relief for good-faith reliance on accredited identity trust, VDC and Privacy-Enhancing Technology (PET) systems. Treasury should use its § 1020.220(b) rulemaking authority to provide exceptive relief deeming institutions compliant when they rely on Treasury-accredited credential or PET frameworks meeting defined assurance standards.	Institutions adopting accredited compliance tools should not face enforcement liability for third-party system errors beyond their control. Exceptive relief would provide regulatory certainty and clear boundaries of accountability. Exceptive relief incentivizes adoption of privacy-preserving identity systems such as identity trusts, reducing costs while strengthening overall compliance integrity.
6. Leverage NIST NCCoE collaboration for technical pilots and standards. Treasury and FinCEN should partner with NIST's National Cybersecurity Center of Excellence (NCCoE) Digital Identities project to pilot mDLs, VDCs, and interoperable trust registries for CIP and CDD testing.	The NCCoE provides standards-based prototypes (e.g., NIST SP 800-63-4 and ISO/IEC 18013-5/-7 mDL) that validate real-world feasibility and assurance equivalence. Collaboration ensures technical soundness, interagency alignment, and rapid deployment of privacy-preserving digital-identity frameworks.

7. Direct FinCEN to engage proactively with industry on adoption of advanced technologies that enhance AML compliance, investigations, and privacy protection. Treasury should issue formal direction or guidance requiring FinCEN to establish an ongoing public-private technical working group with industry, academia, states, and standards bodies to pilot and evaluate advanced compliance technologies.	Continuous engagement with the private sector ensures that FinCEN's rules keep pace with innovation and that compliance tools remain effective, privacy-preserving, and economically efficient. This collaboration would strengthen AML/CFT investigations, reduce false positives, and alleviate the compliance burden on financial institutions while upholding privacy and data-protection standards.

Introduction

The Bank Secrecy Act of 1970 (BSA) established the foundation of the United States' anti–money laundering and countering the financing of terrorism (AML/CFT) framework. Originally intended to detect and deter criminal activity in a paper-based financial system, the BSA has evolved into a vast compliance regime that has struggled to adapt to the realities of the digital economy.

Despite decades of refinement, the system remains inefficient, costly, and only marginally effective. A 2023 LexisNexis study found that U.S. financial institutions spent $59 billion on financial crime compliance—averaging $9 million per bank, with the largest institutions spending over $1 billion annually.[3] Yet these expenditures yield limited results: the United Nations estimated that in 2009, approximately $1.6 trillion (about 2.7% of global GDP) was laundered, while just 0.2% of criminal proceeds were ultimately seized or frozen.[4]

Compliance costs continue to rise, disproportionately affecting smaller institutions. According to the Federal Reserve Bank of St. Louis, large banks (with $1-10 billion in assets) spend between 2.7 and 3.0% of their non-interest expenses on compliance, midsized banks spend between 4.0 and 5.9%, and small community banks spend between 6.8 and 9.1%.[5] Key cost drivers include operational inefficiencies such as manual reviews and non-interoperable systems, high false-positive rates that divert resources from genuine threats, and growing regulatory and reputational pressures that encourage risk aversion.

As compliance burdens mount, many institutions engage in "de-risking"—terminating or denying accounts for customer categories perceived as high risk. This practice disproportionately affects low-income, unbanked, and marginalized populations, pushing them toward unregulated financial channels. The FDIC's 2023 National Survey of Unbanked and Underbanked Households found that 4.2% of U.S. households (5.6 million) were unbanked and 14.2% (19 million) were underbanked.[6] Unbanked rates were significantly higher among lower-income, less-educated, and minority households, as well as single-parent households and adults with disabilities.

Efforts to modernize compliance infrastructure have been uneven. Large institutions such as JPMorgan Chase, which employs over 63,000 technologists and invests $18 billion annually in technology, can internalize compliance costs and innovate.[7] By contrast, the more than 4,000 community banks in the U.S. rely on a small number of legacy core processors. These vendors dominate the market through long-term contracts that include high termination fees, exclusivity clauses, and costly integrations,[8] leaving smaller banks dependent on outdated systems and unable to access or leverage their own data efficiently.

The BSA, once pioneering, was drafted for a pre-digital world in which transactions were primarily cash-based and bank-intermediated. The financial landscape today encompasses fintech platforms, mobile applications, and decentralized finance, yet the statutory framework has not evolved accordingly. The Supreme Court's early review of the BSA upheld its constitutionality but acknowledged potential First, Fourth, and Fifth Amendment privacy concerns.[9] Justices Powell and Blackmun justified the Act's $10,000 reporting threshold as "reasonably high" and not unduly invasive—yet that figure has never been adjusted for inflation. In today's terms, $10,000 in 1970 equals roughly $83,000.

Because the threshold remains static, U.S. financial institutions filed 20.8 million Currency Transaction Reports (CTRs) in FY 2023, a 62% increase since 2002.[10] A 2024 GAO report concluded that had the threshold been inflation-adjusted, CTR filings would have dropped by at least 90% annually since 2014, and that law enforcement accessed fewer than 3% of those reports.[11]

Similarly, Suspicious Activity Reports (SARs)—triggered by subjective suspicion rather than confirmed wrongdoing—have increased by more than 50% between 2020 and 2024.[12] Institutions, wary of regulatory penalties, frequently engage in "defensive filing." In 2024, 27.1% of SARs related to identity theft, while reports

linked to synthetic identity fraud have been increasing 37% year over year, driven in part by advances in generative AI.[13]

In the U.S. financial sector, digital identity remains in an early stage of adoption. Most institutions still rely on uploading scans of physical documents—passports, driver's licenses, and utility bills—that were never designed for online verification. Security features such as holograms or UV-activated inks are rendered ineffective when converted to images, and this already-weakened process is now further undermined by the proliferation of AI-generated deepfakes of documents and biometrics.[14]

By contrast, emerging verifiable digital credential (VDC) implementations such as mobile driver's licenses (mDLs) and state-endorsed digital identity (SEDI) offer a more secure, interoperable, and privacy-preserving foundation for identity verification. These technologies encode verified facts in a machine-verifiable, tamper-resistant format, enabling reliable authentication without exposing unnecessary personal data.[15] Unlike scanned documents, VDCs are designed for digital exchange and are resistant to forgery.

Adoption is expanding rapidly: seventeen U.S. states currently issue mDLs, with more than a dozen others developing programs.[16] Over 75 million Americans are eligible to enroll, and the TSA now accepts mDLs at more than 250 airports.[17] Bound to a user's device and protected by native authentication mechanisms, mDLs are harder to counterfeit and enable selective disclosure—for instance, confirming legal age without revealing full identity details. These developments demonstrate a growing technical foundation for secure digital identity that can improve both financial inclusion and compliance integrity within existing regulatory frameworks.

Enabling a New Compliance Architecture

We have the opportunity today to restructure the entire Know Your Customer (KYC)/AML process to be less burdensome, more privacy-preserving, and more effective for enforcement operations. By combining digital credentials with modern cryptography, the U.S. can reimagine how financial compliance is performed. SpruceID refers to this forward-looking concept as the Identity Trust framework, a model for how identity verification and cryptographic safeguards could be structured in future compliance frameworks.

This Identity Trust architecture is meant to be applied only to activities subject to these obligations, as defined under the GENIUS Act (i.e., payment stablecoins) and under the forthcoming Market Structure Bill (i.e., digital securities and digital commodities) where identification is explicitly necessary. The principle of data minimization should be used in all other cases to prevent unintended consequences such as compliance overreach, privacy risks, and chilling effects to financial innovation.

The Identity Trust model works in four stages:

1. **Identifying.** A regulated entity (the Identity Trust, of which there can be many) is responsible for verifying an individual's identity using digital and physical methods, based on modern best practices such as NIST SP 800-63-4A for identity proofing. Once verified, the trust issues a pseudonymous credential to the individual and encrypts their personal information. Conceptually, the unlocking key is split into three parts: one held by the individual, one by the Trust, and one by the courts, with any two sufficient to unlock the record (roughly, a "two-of-three key threshold").

2. **Transacting.** When the individual conducts financial activity, the individual presents their pseudonymous credential. Transactions are then tagged with unique one-time-use identifiers that prevent linking activity across contexts, even if collusion were attempted. Each identifier carries a cryptographically-protected payload that can only be "unlocked" with the conceptual two-of-three key threshold. Entities and decentralized finance protocols processing the identifiers are able to cryptographicly verify that the identifier is correctly issued by an Identity Trust and remains valid.

3. **Investigating.** If law enforcement or regulators demonstrate lawful cause, conceptually both the court and the Identity Trust decide to operate their keys to reach the two-of-three threshold to designate authorized access to specific limited data justified by the circumstances. The Identity Trust must have a robust governance framework for granting access to law enforcement that respects privacy and due process rights with law enforcement needs through judicial orders. Once the keys from the two entities are combined, the vault containing the relevant information about the identity can then be decrypted if it exists, revealing the individual's information in a controlled and auditable manner, including correlating other transactions depending on the level of access granted by the lawful request. Alternatively, the individual is able to combine their key with the Identity Trust's key to gain the ability to see their entire audit log, and also create cryptographic proofs of their actions across their transactions.

4. **Monitoring**. The Identity Trust performs these continuous checks against suspicious actors and sanctions lists in a privacy-preserving manner with approved policies for manner and intervals, with the auditable logs protected and encrypted such that only the individual or duly authorized investigators can work with the Identity Trust to access the plaintext. Individuals may also request attribute attestations from the Identity Trust, for example, that they are not on suspicious actors or sanctions lists or attestations for credit checks.

The Identity Trust framework can be implemented through existing BSA-regulated entities—such as banks, trust companies, or supervised private vendors—without requiring new rulemaking. It is explicitly designed to fit within current regulatory structures, allowing for issuance of credentials from state-chartered or nationally-chartered trusts, as well as other non-depository institutions already under federal and state supervision. In other words, Identity Trusts can operate today under existing authority and oversight, provided they meet the applicable requirements for Treasury registration, recordkeeping, fiduciary duty, and criminal liability. These institutions would issue and verify digital credentials under current AML and fiduciary standards, aligning with established supervisory models. This structure extends the Credential Service Provider (CSP) approach from NIST[18] and GSA to the financial sector, allowing private CSPs to operate as or alongside regulated entities for compliant credential issuance, verification, and lifecycle management. The result is a clear, auditable, and privacy-preserving identity infrastructure built on existing regulatory foundations.

Benefits

Reduced compliance costs. KYC obligations cost the financial sector an estimated $2.9 billion annually by 2025. Consolidating identity verification within regulated Identity Trusts removes duplicative effort and allows costs to be offset by digital efficiencies.

Improved quality of KYC processes. Identity Trusts specialize in identity management, allowing them to excel at data quality, customer service, use of advanced technologies, and security measures. This is in contrast to smaller financial institutions already facing resourcing constraints for their core banking functions, resulting in varying levels of implementation success for identity onboarding, monitoring, reporting, and security management.

More effective reporting, monitoring and investigations. With transactions tied to pseudonymous credentials, SARs and CTRs could be augmented so that they can resolve individual identities after legal due process in a standard manner. With the same technical standards used across transaction types, this would create interoperability across blockchain transactions, ACH transfers, and even SWIFT transactions. The level of metadata connectivity allows for transaction-level reporting, and standardized, machine-readable formats to enable regulators and financial institutions to apply advanced analytics and AI-driven tools for more efficient monitoring and investigation of illicit activity.

Stronger privacy protections. Individuals transact pseudonymously, protecting them from data brokers, blockchain observers, and excessive government collection under the third-party doctrine. This can eliminate the

need for BSA entities to collect and retain digital copies of sensitive documents such as passports, driver's licenses, and et cetera.

Improved investigative access. Law enforcement retains lawful access to identities when authorized by a court, creating a transparent and verifiable balance between privacy and enforcement. This approach allows for an auditable legal process to prevent abuse and also expedient access to data without delay when rightfully attained.

How This Frames Our Response

The Identity Trust model offers a path for APIs, AI, digital identity verification, blockchain monitoring, privacy-enhancing technologies (PETs), and Trusted Execution Environments (TEEs) to be deployed in ways that are privacy-preserving, auditable, and regulatorily sound. Each section of this response applies the GENIUS Act factors to the Identity Trust model to show how Treasury can guide adoption of these technologies, maximizing effectiveness against illicit finance while reducing systemic risk and compliance burdens.

Q1 - Greatest Trends and Risks

In your experience, what illicit finance risks and vulnerabilities pose the greatest risk in the digital asset ecosystem? What key trends in illicit finance risks have financial institutions observed in the digital asset ecosystem?

The digital asset ecosystem exposes financial institutions to both well-known illicit finance risks and new challenges that are unique to decentralized technologies. One of the most significant is synthetic identity fraud. Because onboarding processes often vary in rigor across institutions, criminals can combine real and fabricated information to create new identities that pass initial checks. The Government Accountability Office reported that banks flagged more than $182 million in suspicious activity linked to synthetic identity fraud in 2021,[19] and the Federal Reserve estimates that related losses grew to over $35 billion in 2023, with generative AI accelerating the scale and sophistication of these schemes.[20]

The rise of deepfakes and other AI-enabled fraud is also reshaping the risk landscape. Generative AI now produces convincing synthetic images, voice samples, and video streams that can defeat remote onboarding and undermine biometric verification. Academic studies warn that identity verification systems face growing difficulty detecting adversarial deepfake inputs.[21] At the same time, the use of “agentic” AI tools that transact on behalf of individuals raises new questions about liability and accountability when such tools are misused.

A growing illicit finance risk in the digital asset ecosystem is the migration toward privacy-focused blockchains[22] and mixers[23], which obscure transaction flows and make it difficult for institutions and law enforcement to distinguish legitimate privacy from concealment of illicit activity.[24] As adoption of these “privacy chains” expands, traditional blockchain analytics tools will lose visibility, complicating monitoring, investigations, and regulatory oversight. One potential safeguard is to embed privacy tags—cryptographic markers linked to a user’s verifiable digital identity—within transactions. These tags would preserve anonymity for ordinary use but allow identity to be lawfully referenced only under warrant and due process, creating a system that upholds both financial privacy and accountable enforcement.

Another growing concern is cross-chain obfuscation. Criminal actors increasingly use bridges, token swaps, and mixer services to move assets across multiple blockchains and disrupt traceability. Cross-chain crime, or ‘chain-hopping,’ has fast become a mainstream money-laundering technique.[25] Researchers have noted persistent limits in attributing complex, multi-network laundering paths with confidence.[26] Similar to above, there are technology advances through a digital identity and verifiable digital credentials that can mitigate this risk.

These risks are already being exploited by state-sponsored groups, ransomware operators, and sanctions evaders. Chainalysis reported in July that illicit digital asset volumes in 2025 are on track to meet or surpass last year’s estimated $51 billion.[27] Against this backdrop, financial institutions are beginning to explore portable, verifiable digital credentials as a way to improve the quality of identity data while reducing unnecessary exposure of personal information. These tools can help close gaps in KYC and transaction monitoring, offering a path toward compliance methods that are both more effective and more privacy-preserving.

Q2 - Application Programming Interfaces (APIs)

What innovative or novel methods, techniques, or strategies related to APIs are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to APIs?

APIs are critical tools already in broad use for enabling financial institutions to manage compliance obligations, and their evolution to use the latest technologies and software industry approaches will be critical to enable the digital asset ecosystem's continued growth. When designed with appropriate safeguards, incorporation of new technologies such as digital signatures, high throughput real-time messaging, and advanced access control for granular data sharing can allow compliance frameworks to meet the rapid pace of financial innovation in the digital asset ecosystem while also reducing fraud.

Importantly, the use of APIs for compliance and supervision is already authorized and in practice under existing rulemaking—financial institutions routinely integrate with regulatory systems, payment networks, and reporting portals via APIs. Expanding these capabilities to verifiable and real-time architectures can occur within current legal and supervisory frameworks, leveraging existing regulatory permissions for data transmission, recordkeeping, and reporting. We believe that financial APIs can be modernized to great effect by (1) becoming *verifiable* by incorporating VDCs or other cryptographic elements for verified identity and attributes, and (2) becoming *real-time* by leveraging technical standards for common messaging protocols and data formats.

Examples of APIs which are "*verifiable*" include the UK's Open Banking[28] and EU PSD2[29], which use digital signatures to verify counterparties and important authorizations. Many of these systems are built on technologies such as the OpenID Financial API (FAPI) profile and/or mutual TLS, which require that the counterparty and payload are cryptographically verifiable. They can also include new systems that include identifiers (such as W3C Decentralized Identifiers or blockchain smart accounts) with guaranteed properties, such as being able to be resolved to an individual's and organization's identity after legal due process.

"*Real-time*" means event-driven machine-to-machine (M2M) exchange, which can work across different counterparties. Examples of these systems include the private sector settlement network CHIPS® Network, which migrated to ISO 20022 for messaging in April 2024 and processes $1.8 trillion in payments daily.[30] Similarly, Fedwire Funds completed its ISO 20022 migration in 2025.[31] Finally, advanced protocols such as x402 combine blockchain transactions with the HTTP internet protocol to produce a seamless payments interface for developers, and are extensible to be verifiable as well.[32]

For the remainder of our response, we will designate APIs with these improvements as "verifiable real-time APIs".

Today, FinCEN already supports electronic submissions for filings such as SARs, CTRs, and other forms via batch upload in their online portal.[33] Financial institutions must hold required BSA/CIP records for 5 years,[34] which can contain troves of PII such as passport scans, driver's license scans, and other sensitive documents from individuals that are not relevant to those particular financial services other than for identity onboarding and customer due diligence. The quality of these collection processes for KYC and CDD and data security practices may vary depending on the abilities of the financial institution, as we elaborate on in Q4 - Digital Identity Verification.

Electronic filing processes can be enhanced with the use of verifiable real-time APIs. These APIs incorporate verifiable digital credentials and identifiers, which can rely upon parties such as the Identity Trust described above (an example of a verifiable real-time API) and/or participating BSA-regulated entities. This modernization builds directly upon existing electronic filing and reporting authorities, enabling a range of regulated institutions—such as banks, trust companies—to participate in the Identity Trust framework as credential issuers. It enables interoperable, secure, and compliant data exchange with government systems without requiring new rulemaking.

This approach allows investigators to gain secure, auditable, and efficient lawful access to compliance data in real time, while minimizing the amount of PII shared across organizations. The result is a system that improves investigative efficiency, enhances individual privacy, and reduces opportunities for data misuse or unauthorized access.

The cycle of reporting relevant data, analyzing patterns, detecting suspicious activity, gathering further information, and starting an investigation can currently take between days and weeks to coordinate all the different parties, and to coordinate and normalize data within the same system. The addition of implicit transaction-based monitoring for blockchain transactions adds complexity to this process, requiring new techniques and approaches for assets such as stablecoins and digital securities, which then must be integrated into an organization's risk-based compliance management strategy, increasing the burden.

By upgrading financial service APIs to also support real-time messaging protocols and data formats that can cover the entirety of these functions, machine-to-machine approaches for compliance become possible, and in many cases they can reduce the process from days and weeks to minutes. With these improvements, institutions can transmit standardized data directly to regulators in near real time, improving both the speed and quality of suspicious activity reporting.

These protocols can be implemented with improved security, counterparty authentication, and reliability using cryptography, extensible data schemas, and modern messaging architectures. For example, these features could support encrypted subgroup exchanges for use under Section 314(b) Voluntary Sharing Among Institutions[35], allowing institutions to share information securely within defined peer groups. In this model, only authorized U.S. participants can view shared data, while FinCEN retains visibility into privileged fields where necessary. This creates a more targeted and auditable reporting ecosystem.

Specifically, this is a non-exhaustive list of open technical standards which can be considered for adding verifiable digital credentials to financial APIs:

- NIST SP 800-63-4
- eIDAS 2.0 / EUDI wallet
- ETSI EN 319 411 EU Qualified Trust Service Providers
- vLEI (GLEIF)
- W3C Digital Credentials API
- ISO/IEC 18013-5 Mobile Driver’s License (mDL)
- ISO/IEC 18013-7 Online mDL
- W3C Verifiable Credentials
- W3C Decentralized Identifiers
- FIDO2 / WebAuthn (passkeys)
- IETF Selective Disclosure JWTs (SD-JWTs)
- IETF SD-JWT-VC
- IETF OAuth 2.0
- IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- OpenID Connect
- OpenID FAPI 2.0
- OpenID Identity Assurance (eKYC/IDA)
- OpenID Federation 1.0
- OpenID Shared Signals (SSE) with CAEP/RISC for zero-trust eventing/webhooks
- OpenID for Verifiable Credentials, including:
    - OpenID for Verifiable Presentations (OID4VP)
    - OpenID for Verifiable Credential Issuance (OID4VCI)
    - Self-Issued OpenID Provider (SIOP)
- Google Longfellow ZK

- Key Event Receipt Infrastructure (KERI)

Additionally, this is a non-exhaustive list of open technical standards which can be considered for creating interoperable messaging layers with strong security features:

- ISO 20022
- IETF RFC 8705 OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens (mTLS)
- IETF RFC 9180 Hybrid Public Key Encryption (HPKE)
- IETF JOSE and COSE (including Post-Quantum Cryptography)
- IETF RFC 6455 The WebSocket Protocol
- IETF RFC 6120 Extensible Messaging and Presence Protocol (XMPP)
- IETF RFC 9420 The Messaging Layer Security (MLS) Protocol
- The Matrix Protocol
- W3C ActivityPub
- The AT Protocol

Benefits. Properly deployed, the use of verifiable real-time APIs improves compliance outcomes by enabling faster detection of suspicious activity, reducing duplicative KYC processes, and lowering integration costs across institutions. It creates a consistent foundation for interoperability that can extend to decentralized finance (DeFi) protocols and other existing or novel environments: blockchains, privacy blockchains, FedNow, ACH, SWIFT, EU TIPS, and more.

Risks and Challenges. Without adequate safeguards, automated reporting could expose sensitive data or create uncertainty about regulatory acceptance. Key risks include unauthorized access to API endpoints, misuse of credentials, and inconsistent implementation across the sector. Smaller institutions may face barriers to adoption due to cost or lack of technical capacity, although this transition cost will likely be quickly recouped by decreased reporting costs.

Safeguards. These risks can be mitigated with strong authentication and authorization requirements, end-to-end encryption, digital signatures, rate-limiting, and independent certification of implementations. The principle of least privilege should guide design, ensuring that the API exposes only the minimum data necessary to meet compliance requirements. A robust ecosystem of vendors and experts built from open standards, many already existing, would increase the implementation quality, cost basis, and speed for these improvements.

a) What factors do financial institutions consider when deciding whether to employ APIs for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use APIs for these purposes, what specific compliance functions do/will APIs support? For financial institutions that decided not to use APIs, please provide additional details on the rationale for that decision.

When evaluating whether to adopt verifiable real-time APIs, financial institutions focus primarily on whether FinCEN and other regulators will accept these functions (e.g., CDD processes, automated filings, data sharing under Section 314(b)) as compliant under the Bank Secrecy Act[36] and considerations during examinations and best practices that can create mitigations during penalties. Regulatory clarity is often more determinative than technical capability.[37] Institutions also weigh the sensitivity of the data being transmitted, the availability of common standards, vendor ecosystem maturity, and integration costs with existing case management systems.[38]

b) How are financial institutions using API tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of API tools with other existing or previous tools used for similar purposes.

Today, most institutions are deploying APIs as a way to augment existing compliance systems with more layers rather redesigning them[39] to use a digital-native approach that incorporates real-time fraud signals that can be automated, extended with modules, and utilized with AI anti-fraud agents. Over time, some institutions have begun to use APIs to replace legacy batch uploads and manual entry,[40] which improves timeliness and reduces clerical errors. When combined with verifiable digital credentials and messaging protocols, these new APIs can become more efficient and consistent, but full effectiveness depends on regulatory acceptance of automated, credential-enabled reporting to allow FinCEN and investigators to utilize these new tools as well.

c) Are there regulatory, legislative, supervisory, or operational obstacles to using APIs to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

The largest obstacles are regulatory and supervisory ambiguity. Institutions need confirmation that automated submissions via verifiable real-time APIs will satisfy BSA obligations, what evidentiary artifacts (e.g., digital signatures, audit logs) must be retained, and how liability is assigned across participants and vendors. Models for addressing such constraints already exist in adjacent sectors—most notably in the standardized agreements and liability frameworks that govern relationships between payment networks, issuing banks, and merchants[41]—demonstrating that clear, interoperable trust arrangements can balance compliance assurance with operational scalability. Without this clarity, institutions risk building duplicative systems. Operationally, legacy systems may lack compatibility with credential-addressed APIs,[42] and smaller institutions face the fixed costs of secure endpoint development and monitoring.[43]

Legislative gaps also exist: Section 314(b) safe harbors were not designed for encrypted subgroup APIs, and the BSA does not give examiners guidance on recognizing privacy-preserving, attribute-level attestations as compliant for different required processes.

Our recommendations are detailed in the next section, part (d).

d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of APIs for detecting illicit finance involving digital assets?

Treasury and FinCEN should take concrete steps to enable compliant, privacy-preserving digital credentials adoption across the financial system. This includes formally recognizing use of pseudonymous identifiers in SAR/CTR submissions, recognizing standardized technical specifications for their operation across investigations, and establishing a certification framework for vendors and institutions. Treasury should also clarify that privacy-preserving, attribute-level data exchanges through verifiable real-time APIs meet compliance obligations when policy objectives are achieved.

1. **Formally recognize API-based usage of verifiable digital credentials for identity verification for filings as compliant**, publish technical approaches which satisfy the needs of the legal process and investigators (e.g., OpenAPI/JSON schemas, standardized error codes, uptime, and retry SLAs), and provide a certification path for filers and vendors. Existing FinCEN e-filing standards[44] should inform and be developed in alignment with, the use of verifiable digital credentials ;

2. **Issue joint guidance with OFAC on API evidence** necessary for sanctions screening, including required audit trails, retention periods, and human-in-the-loop controls;

3. **Endorse least-privilege, attribute-level exchanges**—including selective-disclosure proofs—as satisfying Customer/Enhanced Due Diligence (CDD/EDD) where policy objectives are met;

4. **Encourage modernization of Section 314(b) implementations** to explicitly cover encrypted, subgroup information-sharing via APIs along with strong incentives for firms to participate fully to enhance detection of illicit activity;

5. **Align with standards bodies such as NIST, ISO, W3C, and IETF for identity and cryptographic guidance** and reference interoperable standards (e.g., NIST SP 800-63-4A IAL2 for remote identity verification baselines or OpenID4VC for credential exchange) for identity-related or message-streaming API flows; and

6. **Provide space for responsible innovation and collaboration,** such as exceptive relief and implementation grants or shared services for non-bank entities under GENIUS Act, community banks, and credit unions to lower initial compliance and security costs.

Together, these measures would modernize regulatory reporting, strengthen collaboration between institutions, and make compliance both more efficient and more privacy-protective. By clearly signaling that APIs are a compliant, trusted channel for regulated information exchange, Treasury and FinCEN can accelerate innovation while enhancing oversight, auditability, and financial integrity across the digital asset ecosystem.

These same principles can also be applied to cross-institution and cross-border information exchange under the "Travel Rule." As detailed later in this response Question 4 (d), verifiable digital credentials and standardized API protocols can enable financial institutions and virtual asset service providers to meet Travel Rule transmission obligations through privacy-preserving, machine-readable attestations, rather than transmitting raw personal data.

e) Treasury will evaluate APIs and consider their impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.

1. **Improvements in the ability of financial institutions to detect illicit activity involving digital assets.** Verifiable real-time APIs with these improvements allow financial institutions to validate and exchange verifiable identity credentials at the time of transaction, binding attributes such as age, citizenship, or sanctions status directly to payment events. By automating the collection of high-assurance, cryptographically signed attributes, the improved APIs raise data quality and reduce synthetic identity fraud—a major entry point for money laundering. Because verifiable real-time APIs support automated, encrypted reporting to FinCEN and 314(b) subgroups, they shorten the time from suspicious activity detection to regulator notification, improving system-wide responsiveness.

2. **Costs to financial institutions.** The main cost of these improvements is initial integration—building secure endpoints, aligning with wallet/verifier standards (e.g., W3C Digital Credentials API, OIDF's OpenID4VP), and upgrading compliance workflows. However, these investments replace fragmented, manual identity checks with reusable credential validation across institutions. Over time, this lowers operational costs by reducing false positives, duplicate KYC efforts, and inefficient manual reporting. Smaller institutions could benefit from a shared API service layer which supports verifiable digital credentials and advanced messaging protocols, or Treasury-supported reference implementation.

3. **The amount and sensitivity of information that is collected or reviewed.** Unlike current processes, an API with these improvements enables least-privilege exchanges: only the attributes required by policy are revealed (e.g., “is over 18” or “not on OFAC list”), not full documents or extraneous PII. This reduces the amount of sensitive data institutions must collect and store, shrinking the attack surface and the compliance burden associated with long-term data retention.

4. **Privacy risks associated with the information that is collected or reviewed.** The verifiable real-time API’s design mitigates privacy risks by using selective disclosure proofs and encrypting all data in transit and at rest. Access can be restricted to authorized subgroup participants (e.g., U.S.-only 314(b) members), and cryptographic receipts provide auditability without exposing raw personal data. Compared to legacy systems that routinely transmit entire identity documents, verifiable real-time APIs substantially reduces privacy exposure.

5. **Operational challenges and efficiency considerations.** Institutions will need to update compliance systems to interoperate with wallets and credential issuers, which may pose challenges for legacy infrastructure. However, once deployed, an improved API consolidates multiple compliance functions—KYC, sanctions screening, SAR preparation, and 314(b) sharing—into a standardized, automated workflow. This reduces duplication, improves data consistency, and allows compliance teams to focus on higher-value investigations rather than clerical review.

6. **Cybersecurity risks.** Like any API, even improved APIs can introduce risks such as credential theft or endpoint compromise. These can be addressed through mutual TLS, OAuth 2.0 with dynamic client registration or OIDF Financial API (FAPI) 2.0 Security Profile, FIPS-validated cryptography, rate limiting, and continuous monitoring. While APIs are not inherently more secure than databases, they can enable more privacy-preserving architectures. Moreover, by minimizing the amount of sensitive raw PII stored in institutional databases, a ‘honey pot’, the API significantly reduces both the likelihood and the potential impact of a data breach.

7. **Effectiveness of methods, techniques, or strategies at mitigating illicit finance**. Verifiable real-time APIs strengthen AML/CFT efforts by combining stronger identity assurance with more targeted data exchange. They enable faster detection of synthetic identities, improves sanctions screening, and reduces opportunities for regulatory arbitrage across institutions. Its effectiveness depends on clear rulemaking from FinCEN confirming that automated, API-based filings and attribute-level credential exchanges meet Bank Secrecy Act obligations. With that clarity, verifiable real-time APIs can scale across the ecosystem as a common compliance backbone.

Q3 - Artificial Intelligence

What innovative or novel methods, techniques, or strategies related to AI are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to AI? Please describe the use of AI to conduct analysis of transactional data, including transactions that occur on blockchains, and to identify complex illicit financial networks, as well as key lessons learned from use of AI in this context.

Artificial intelligence is increasingly viewed as a force multiplier for AML/CFT compliance,[45] particularly when combined with structured data flows from verifiable real-time APIs. By automating analysis of large datasets—including blockchain transactions, sanctions lists, and credential-based identity attributes—AI can help financial institutions detect illicit activity earlier and with greater precision than manual or rules-based methods alone.[46]

Innovative Applications. Financial institutions are piloting AI systems that analyze blockchain transaction data to identify patterns of layering, obfuscation, and cross-chain movement associated with illicit finance.[47] Machine learning models can detect typologies that span multiple ledgers, such as rapid movement of funds through mixers and bridges. AI is also being applied to compliance reporting, where natural language systems assist in drafting Suspicious Activity Reports (SARs) based on transaction patterns flagged by monitoring tools. These SARs are then reviewed and verified by human analysts before submission, improving efficiency without removing accountability.[48]

Another novel strategy is the use of AI agents that operate within credential-based frameworks. With delegated authority, an AI agent can transact on behalf of a customer using derived, pseudonymous identifiers. These derived credentials can be tied back to the principal through cryptographic proofs, preserving accountability if the agent is misused. This approach anticipates a future where agentic AI plays a direct role in financial transactions and ensures that compliance systems can attribute actions accurately.

Benefits. AI improves the ability of institutions to detect complex, cross-network illicit finance networks that are difficult to identify using rule-based systems. It reduces manual workload by triaging alerts, lowering false positives, and highlighting higher-risk patterns for human review. AI can also bring consistency across institutions by applying shared models to standardized data streams, such as those provided through verifiable real-time APIs.[49]

Risks and Challenges. The most significant risks include false confidence in model outputs, potential bias or blind spots in training data, and the ability of adversaries to use AI themselves—for example, through deepfakes or synthetic identities designed to evade detection. Recent research[50] (shared with Treasury under this RFC) underscores these concerns as synthetic and AI-generated data can undermine financial integrity if provenance and identity linkages are not preserved. There is also a risk of over-reliance: an AI-generated SAR that is too persuasive could be accepted without sufficient human review. Additionally, resource-constrained institutions may struggle to deploy and maintain explainable, well-governed AI systems that meet supervisory expectations.[51] AI agents that operate on behalf of a financial institution should be identified and linked back to an organizational identity or specific individual; otherwise, regulatory accountability and auditability would be compromised, eroding the traceability required for risk management and supervisory oversight.

Safeguards. Effective safeguards include maintaining human-in-the-loop oversight for enforcement-related actions, establishing model risk management frameworks that address explainability, accuracy, and concept drift, and retaining auditable records of inputs and outputs for examination. AI systems should be tested regularly against adversarial scenarios, such as deepfake-based onboarding attempts or novel cross-chain laundering typologies. Integration with verifiable real-time APIs also provides a safeguard, as AI can operate on verified, minimal identity attributes rather than unstructured documents, reducing data quality issues and privacy risk.

a) *What factors do financial institutions consider when deciding whether to employ AI for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use AI for these purposes, what specific compliance functions does/will AI support? For financial institutions that decided not to use AI, please provide additional details on the rationale for that decision.*

When evaluating whether to employ AI for AML/CFT and sanctions compliance, financial institutions primarily consider regulatory acceptance,[52] data quality, and operational readiness.[53] Institutions are more willing to deploy AI when there is clear guidance that its outputs—such as alert triage or SAR drafting—will be recognized as compliant so long as human oversight is maintained. They also weigh whether they can access structured, trustworthy data feeds (for example, from verifiable real-time APIs) that allow AI models to operate effectively without amplifying errors or privacy risks.[54] Finally, institutions assess the costs of developing explainable models, training compliance staff, and maintaining audit trails that examiners can review.[55]

Where adopted, AI can support several compliance functions. It can be used to analyze blockchain transaction patterns for obfuscation and layering, triage alerts to reduce false positives, screen transactions in real time against sanctions and watchlists, and assist in drafting SARs by generating narratives from flagged patterns. AI can also play a role in detecting synthetic identities and deepfakes by analyzing biometric and document data for anomalies that human reviewers might miss.

However, institutions cite concerns about model explainability, supervisory uncertainty, and the risk of regulatory pushback if AI-generated outputs are seen as replacing rather than supporting human judgment.[56] Smaller institutions, in particular, worry about the cost of acquiring or developing models, the need for continuous tuning, and the burden of meeting examiner expectations for model governance. As a result, many have taken a “wait and see” approach.

b) *How are financial institutions using AI tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of AI tools with other previous or existing tools used for similar purposes.*

Financial institutions are largely using AI to augment existing compliance tools rather than to replace them.[57] In practice, AI models run alongside rule-based transaction monitoring systems and manual case review, providing triage and pattern-detection capabilities. Some institutions operate AI in testing or shadow mode, validating outputs against traditional methods before expanding adoption. Compared to legacy tools, AI is more effective at surfacing complex cross-chain or synthetic identity risks, but its outputs still require human review to meet regulatory expectations and address the ethical and operational risks inherent in autonomous decision-making.

c) *Are there regulatory, legislative, supervisory, or operational obstacles to using AI to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.*

The biggest obstacle to using AI in AML/CFT is regulatory and supervisory uncertainty.[58] Financial institutions are reluctant to rely on AI-generated outputs without clear guidance from FinCEN and prudential regulations on how these tools will be evaluated during examinations. In particular, institutions need to know whether AI-assisted suspicious activity detection and AI-drafted SARs are acceptable so long as human review remains in place.

Without this clarity, many firms continue to run AI in pilot or shadow mode rather than integrate it into production workflows, and not capture most of the efficiency and accuracy gains it offers.

Model governance expectations are another barrier. Current frameworks under the Bank Secrecy Act do not explicitly address explainability, adversarial testing, or concept drift for AI models. Examiners often apply standards developed for credit risk models, which may not map neatly to transaction monitoring or identity verification use cases. This lack of fit discourages adoption and creates inconsistent supervisory outcomes.

Operational challenges also remain. Smaller institutions face high costs to acquire models, train staff, and maintain the infrastructure needed for continuous monitoring and retraining. Data quality is a further obstacle: legacy systems often provide fragmented or unstructured data, making AI outputs unreliable unless paired with structured, verifiable data feeds such as those enabled by verifiable real-time APIs.[59]

Our recommendations are detailed in the next section, part (d).

d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of AI for detecting illicit finance involving digital assets?

Treasury and FinCEN should:

1. issue guidance clarifying that AI may be used in AML/CFT programs when supported by human oversight, with specific expectations for SAR drafting and alert triage;
2. publish supervisory standards for AI model risk management tailored to financial crime compliance (covering explainability, adversarial testing, and recordkeeping);
3. support pilot programs where institutions can test AI models with regulator participation; and
4. encourage adoption of structured, privacy-preserving data sources—such as portable digital identity credentials—so that AI operates on high-quality inputs.

These steps would reduce uncertainty, promote consistent supervision, and allow institutions to deploy AI in ways that enhance both effectiveness and accountability.

e) Treasury will evaluate AI and consider its impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.

1. **Improvements in the ability of financial institutions to detect illicit activity involving digital assets.** AI significantly enhances detection capabilities by identifying complex, cross-chain laundering typologies, obfuscation techniques, and synthetic identities that are difficult to capture with rules-based systems. When paired with structured, high-assurance inputs from verifiable real-time APIs, AI models can operate on verified attributes rather than noisy or incomplete data, which improves both precision and recall in compliance monitoring.[60]

2. **Costs to financial institutions.** AI adoption entails material upfront and ongoing costs: acquiring or developing models, curating training datasets, hiring skilled staff, and maintaining infrastructure for continuous retraining. Large institutions are better able to absorb these costs; smaller firms may find them prohibitive unless shared services, reference models, or government-supported pilots are available. Over time, efficiency gains—such as reducing false positives and accelerating SAR preparation—can lower compliance costs relative to manual-only systems.

3. **The amount and sensitivity of information that is collected or reviewed.** AI itself does not require more information than existing systems, but the quality and format of the information matter. Operating on portable, attribute-level credentials exchanged via verifiable real-time APIs allows AI to function effectively with less raw personal data, mitigating the need to ingest and store full identity documents or sensitive biometrics.

4. **Privacy risks associated with the information that is collected or reviewed.** Without safeguards, AI could encourage over-collection or retention of sensitive data. These risks are reduced when AI operates on selective-disclosure proofs or other least-privilege data provided through trusted APIs. Privacy protections are further strengthened by retaining auditable logs of AI decision-making rather than retaining unnecessary personal data.

5. **Operational challenges and efficiency considerations.** AI models require continuous tuning to remain effective against evolving illicit finance typologies. Institutions must also establish governance processes for explainability, error handling, and examiner review. When integrated with APIs that deliver standardized, machine-readable inputs, AI can streamline workflows, improve efficiency, and reduce duplicative manual review.

6. **Cybersecurity risks.** AI systems are vulnerable to adversarial manipulation, including synthetic inputs (deepfakes, fabricated credentials) designed to evade detection. Attackers may also attempt to probe or corrupt training data. Mitigation requires adversarial testing, red-teaming, and integration with verified data sources such as verifiable real-time APIs. Using cryptographically signed credentials and enforcing provenance for training data reduces exposure to manipulated inputs.

7. **Effectiveness of methods, techniques, or strategies at mitigating illicit finance**. When deployed with strong governance, human oversight, and high-quality data inputs, AI improves the ability of financial institutions to detect and report illicit finance in digital assets. Its effectiveness depends on regulatory clarity that AI-assisted outputs—such as alert triage or SAR drafting—are acceptable with documented oversight, and that privacy-preserving data exchange mechanisms are recognized as valid sources for model inputs. With this clarity, AI can deliver measurable improvements in both compliance outcomes and systemic resilience.

Q4 - Digital Identity Verification

What innovative or novel methods, techniques, or strategies related to digital identity verification are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to digital identity verification? Please describe the portable digital identity credentialing tools in use and how such tools are being used.

Digital identity verification is shifting from repeated document-based KYC checks toward portable, cryptographically-verifiable credentials issued by authoritative entities.[61] These credentials can be presented through user-controlled wallets and validated by financial institutions at the point of onboarding or transaction. This model strengthens AML/CFT programs by providing high-assurance attributes—such as proof of legal name, age, citizenship, or sanctions-screening status—without exposing full documents or unnecessary personal data.

This traditional identity verification model also underpins how transaction-level compliance is implemented, including the Travel Rule which requires the transmittor's bank to send the transmittor's PII to the recipient bank for each transaction. By using verifiable digital credentials to transmit authenticated, privacy-preserving proofs of originator and beneficiary information, financial institutions can satisfy Travel Rule requirements while reducing exposure of sensitive personal data. This approach links digital identity modernization directly to secure, interoperable data exchange across the financial system.

In practice, this shift feels similar to the evolution of consumer trust systems like Disney's MagicBand—a wristband that lets park visitors seamlessly enter attractions, unlock hotel rooms, and make purchases without repeatedly showing tickets or ID. It's voluntary, privacy-preserving, and feels effortless to the user, yet it's powered by deep technical assurance behind the scenes. In the same way, digital identity wallets could let customers verify who they are across banks, apps, or exchanges through a single, secure interaction.

Adoption and Technology. Portable digital identity verification is no longer theoretical—governments are already issuing credentials. mDLs are live in over seventeen states[62] and accepted at over 250 airports by the Transportation Security Administration (TSA).[63] In California, over two and a half million mobile driver's licenses have been issued through the mobile driver's license program.[64] Across the United States, an estimated 71.5 million people are eligible to enroll in their state's mobile driver's license program.[65]

Importantly, the NIST National Cybersecurity Center of Excellence (NCCoE) is leading a mobile driver's license project that brings together banks, technology providers, and state agencies to define how ISO 18013-5/7 compliant mDLs can be used for KYC in financial services.[66] This initiative demonstrates the feasibility of portable, standards-based credentials for regulated onboarding and offers a blueprint for integrating mDLs into AML/CFT compliance workflows. Specifically, these VDCs can be used as evidence for achieving NIST SP 800-63A-4 IAL2, and digital identity evidence strength is determined by the same strength qualities as physical evidence. These can be combined with industry certification frameworks such as FIDO certification for Identity Verification which includes Document Authenticity (DocAuth) and also Face Verification.

Additionally, the European Union is rolling out its Digital Identity Wallet[67], and cross-industry groups like NIST, AAMVA, FIDO, and the W3C are driving interoperability standards.[68] Credential formats such as ISO mDLs, W3C Verifiable Credentials, and SD-JWTs (IETF) are being demonstrated in production pilots, supporting selective disclosure of attributes and minimizing over-collection of user data.[69] These tools are increasingly integrated into compliance workflows through APIs that request only the attributes required for a given regulatory obligation.

Voluntary identity frameworks like TSA PreCheck and CLEAR demonstrate the success of public and private models that provide secure identity verification that meets legal requirements. Similar to how travelers opt in to share verified data once and gain expedited passage everywhere the program is recognized, digital identity credentials could create a trusted traveler experience for finance: a "pre-vetted lane" for compliance that still upholds rigorous AML/CFT controls.

Financial institutions are beginning to see digital credentials the way the payments industry once saw EMV chips in payment cards—an upgrade in trust infrastructure.[70] Just as EMV introduced shared accountability among merchant acquirers, issuing banks, and the card network, credential-based identity verification can distribute liability and assurance among issuers, verifiers, and wallet providers. A regulated set of verifiable real-time APIs could act like the payment rails, allowing multiple participants to transact securely under common governance.

Policy Foundations. The TSA's acceptance requirements for mDLs at airports provide a strong technical baseline. Those standards—covering issuance, authentication, and cryptographic binding—can be adapted to financial services, as demonstrated in the NIST National Cybersecurity Center of Excellence mobile driver's license initiative, to ensure credentials meet AML/CFT and sanctions compliance needs.[71] Similarly, NIST SP 800-63 provides the federal benchmark for digital identity assurance; expanding its normative profile to include modern cryptographic methods (PKI, zero-knowledge proofs) would better align with portable credential use in finance.[72]

The U.S. AML/CFT framework could be improved to explicitly recognize verifiable digital credentials—including government-issued digital IDs, such as mDLs and/or state-endorsed digital identity (SEDI) credentials, regulated financial institution-issued credentials, and interoperable verifiable credentials that meet defined assurance standards—as valid forms of documentary evidence under the CIP rule. See ***Part (d)*** below for further explanation of how this could be implemented.

At the state level, Utah's State-endorsed Digital Identity (SEDI) program, codified at Utah Code § 63A-16-1201, establishes a legal framework for issuing and recognizing verifiable digital credentials. California has also advanced digital identity legislation through SB 786, and other states continue to pass mDL bills. This bipartisan momentum demonstrates a growing consensus that digital credentials can enhance both trust and privacy in identity verification. The American Civil Liberties Union, along with a coalition of civil society groups, has published guidelines for digital identity programs that are aligned with the principles encoded in the Utah SEDI program, showing that strong identity assurance can be advanced without compromising user rights.[73]

Concrete operational shapes for an Identity Trust could include entities already permitted under existing BSA requirements. For example, a Federally Regulated Bank—whether state- or nationally-chartered—could serve as such an organization, issuing and verifying digital credentials as part of its existing customer identification and record-retention duties. A State-Chartered or Nationally Chartered Trust Company could act as a specialized identity fiduciary, maintaining verified customer data under current fiduciary and AML obligations. A non-bank private vendor could also fulfill this role under a supervised model, functioning as an outsourced service provider or technology intermediary to a regulated institution—similar to how payment processors or credit bureaus operate today—subject to the same BSA, data-retention, and audit standards. Each of these entities functions without requiring rule changes, aligning this hypothetical ecosystem role with current supervisory frameworks while expanding verifiable access across the financial ecosystem.

Importantly, an Identity Trust can be viewed as an evolution of the Credential Service Provider (CSP) model recognized by the General Services Administration (GSA) for federal digital identity assurance. Private-sector CSPs already perform credential issuance, validation, and lifecycle management for government and enterprise systems under NIST SP 800-63 accreditation. Extending this model to the financial sector—where a CSP partners with or operates as a BSA-regulated entity—would provide a clear, auditable path for compliant credential issuance and verification. In practice, a private CSP could serve as the operational arm of an Identity Trust, handling credential provisioning and revocation while the regulated institution maintains ultimate responsibility for AML/CFT compliance and supervisory reporting. This approach leverages existing policy precedent and procurement pathways, reducing regulatory friction while ensuring that private credential providers meet the same assurance, retention, and audit standards as financial institutions.

In this way, emerging identity frameworks could mirror existing co-regulatory ecosystems—like how CLEAR operates under TSA rules but with private execution, or how credit card networks enforce rules across member

banks. Public-private credentialing partnerships could achieve both scale and oversight, creating a shared backbone for trustworthy digital identity, much like the card networks created standardized payments.

Benefits. The move to portable credentials reduces duplication of KYC processes, improves data quality, and lowers the operational costs of onboarding. It also enhances privacy by enabling selective disclosure—for example, proving a user is "over 18" or "not on the OFAC list" without sharing their full date of birth or government ID number. Regulators also benefit from verifiable audit trails tied to cryptographic proofs rather than unverifiable scans or PDFs.

For users, this could feel like an everyday upgrade—akin to moving from a paper ticket to a digital wallet pass, or from swiping a magnetic card to "Tap to Pay." For institutions, it parallels the evolution from manual paper processing to EMV and tokenized transactions: fewer points of failure, better traceability, and higher assurance built into the system design.

Benefits for Investigations. Other important benefits include more accurate reporting, monitoring and investigations as described below:

1. **Cryptographic provenance & chain of custody:** Each credential is signed by a trusted issuer and time-stamped; validation and revocation checks create a tamper-evident audit trail that strengthens evidentiary reliability.

2. **Higher data quality = fewer false positives:** Attributes can be proofed to NIST SP 800-63A-4 IAL2 or above, and lifecycle-managed (updates/revocations), improving sanctions/KYC screening quality and reducing noise in alerts and case queues.

3. **Rapid entity resolution:** Reliable and stable digital identifiers and standardized schemas (W3C VC, DID, mDL) enable fast de-duplication across institutions, linking related accounts/wallets and accelerating network-analysis.

4. **Selective disclosure with lawful expandability:** Day-to-day use can minimize PII exposure (ZK/SD-VCs), while lawful process can retrieve full underlying data—improving privacy *and* investigative depth as required by regulations.

5. **Interoperable cross-border cooperation:** Trust registries and common schemas make cross-jurisdiction verification faster, improving responsiveness to 314(a) requests and mutual legal assistance.

6. **Revocation intelligence:** Real-time revocation/status checks provide fresh signals (e.g., issuer revoked after fraud report), useful for triage and dynamic risk scoring.

7. **Attribution and accountability of issuers:** Each claim is traceable to an accredited issuer, clarifying who is responsible for accuracy and enabling targeted follow-up or subpoenas.

8. **Travel Rule correlation:** VDC references can bind originator/beneficiary assertions to transfers, simplifying counterparty identification and funds-flow reconstruction.

9. **Device/app binding (where used):** Possession proofs and authenticator binding (Authenticator Assurance Level 2: AAL2 or above) help attribute actions to a user/device pair, tightening circumstantial links in case building.

Risks and Challenges. Challenges include varying assurance levels across issuers, a lack of uniform wallet certification, and the risk of normalization of over-collection if financial institutions request full credentials when only partial attributes are needed. Another is clarifying who bears responsibility when a credential is misissued or misused. Established models in payments—such as the liability frameworks among networks, issuers, and merchants—show how standardized agreements can balance compliance assurance with scalability.[74] Legacy banking systems may also lack the ability to integrate verifiable credential flows without significant upgrades.

Safeguards. Adherence to recognized standards (NIST SP 800-63, ISO 18013-5/-7, W3C VC, SD-JWT, FIDO) and independent certification of wallets and verifiers are key to ensuring consistent quality. Privacy safeguards should include least-privilege design and regulatory endorsement of selective disclosure as a best practice. Treasury should also encourage alignment with state-level initiatives such as Utah's SEDI framework and with civil-liberties recommendations to avoid overreach in implementation. Establishing uniform assurance levels and certification processes across diverse participants would promote trust and interoperability without imposing unnecessary concentration of responsibility or restricting innovation.

Takeaway. Governments are already issuing digital identity documents in portable, cryptographically verifiable formats, and financial institutions are beginning to incorporate them into AML/CFT compliance. Through an Identity Trust, these credentials can be integrated into reporting and monitoring systems, offering higher assurance against synthetic identities, reducing privacy risks, and creating a more efficient compliance foundation for both centralized and decentralized financial services.

a) What factors do financial institutions consider when deciding whether to employ digital identity verification for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use digital identity verification for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use digital identity verification, please provide additional details on the rationale for that decision.

When considering whether to implement digital identity verification for AML/CFT and sanctions compliance, financial institutions weigh several factors: regulatory acceptance, assurance of credential quality, integration costs,[75] and the likely adoption of credentials by customers. Institutions are most likely to invest when they have confidence that portable, standards-based credentials will be recognized as meeting Bank Secrecy Act and sanctions obligations.[76] They also assess whether credentials originate from trusted issuers such as Department of Motor Vehicles (DMVs) or passport authorities and whether they can be validated through cryptographic proofs. Just as importantly, institutions consider whether customers will actually adopt and use these credentials. Adoption tends to be driven by utility in everyday transactions—for example, when an mDL can be used both at airport security and to open a financial account, the convenience creates a stronger incentive for customer uptake.[77]

For those moving forward, digital identity verification supports critical compliance functions. Portable credentials can be used to strengthen KYC at onboarding, prevent synthetic identity fraud, and support ongoing customer due diligence.[78] Attribute-level credentials (e.g., "over 18," "U.S. person," "not on the OFAC list") can also be bound to transactions in real time through an Identity Trust, improving the accuracy of sanctions screening and reducing the risk of illicit actors accessing services. These tools also create cryptographically verifiable audit trails that simplify examinations and investigations.

Institutions that have not yet adopted digital identity verification typically point to regulatory uncertainty,[79] lack of infrastructure readiness, and uncertainty around consumer uptake. Without explicit guidance from FinCEN and prudential regulators, some firms are hesitant to invest in credential-based workflows for fear they may need to maintain duplicative document-based processes. Others—particularly smaller institutions—cite the challenge of upgrading legacy systems to interoperate with wallets and APIs.[80] If customers do not see clear benefits to

adopting and presenting digital credentials, institutions face the risk of building compliance processes that are underused in practice. Broader adoption will depend not only on clear supervisory expectations and uniform assurance standards, but also on ensuring that digital credentials are useful across multiple high-value contexts, so customers have a reason to carry and present them.

b) How are financial institutions using digital identity verification tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of digital identity tools with other existing or previous tools used for similar purposes.

Financial institutions are primarily using digital identity verification tools to augment existing KYC/AML controls, often in pilot or parallel-run modes. Institutions keep legacy workflows for audit continuity while measuring error rates, reviewer effort, and examiner feedback on the credential-based flow. Where pilots mature—such as in NCCoE-style mDL-for-KYC configurations—firms can begin progressive replacement of manual document reviews for well-scoped use cases (e.g., domestic retail onboarding), while retaining traditional methods for edge cases or low-assurance issuers. Based on our experience, major financial institutions are mainly piloting workflows utilizing digital identity credentials for risk-focused use cases such as account recovery and pre-transfer confirmations, as they lack sufficient guidance from regulators on their applicability within risk-based compliance management programs, despite their potential benefits.

Compared with prior tools, digital identity credentials generally show higher data quality and lower friction. Cryptographic binding to authoritative issuers reduces synthetic and tampered-document risk; selective disclosure lowers over-collection of user data and downstream PII handling; and machine-readable proofs cut re-keying and clerical errors. In parallel runs, institutions report faster analyst cycle times and fewer false positives stemming from inconsistent identity data. Credentials also improve auditability: verifiers retain signed receipts of what was asserted and when, rather than screenshots or PDFs of uncertain provenance.

In effect, this shift resembles the transition from handwritten checks to modern payment networks, where verification is built into the process rather than mainly conducted after acceptance. Cryptography and liability-sharing agreements, identity credentials embed compliance logic directly into onboarding and transaction flows.

Effectiveness gains are most pronounced where (1) the credential's assurance level is clear (e.g., ISO 18013-5/-7 mDL, NIST SP 800-63-aligned issuance), (2) the verifier flow is least-privilege (attribute-only rather than full document), and (3) customer adoption/utility is high (e.g., the same mDL works at TSA and at account opening). By contrast, traditional tools (document scans, knowledge-based checks, fragmented database lookups) are more error-prone, slower, and create larger privacy and breach surfaces due to broad data capture and storage.

Credential effectiveness depends on issuer coverage and wallet assurance, consistent regulatory acceptance, and legacy integration readiness. As those conditions are met, institutions can shift from "augment" to "replace" for defined segments, using the Identity Trust as the backbone for standardized ingestion, logging, and evidence retention.

Over time, digital identity credentials could serve financial compliance much like EMV chips did for payments—quietly upgrading trust and reducing fraud behind the scenes, while making the user experience simpler and more secure.

c) Are there regulatory, legislative, supervisory, or operational obstacles to using digital identity verification to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

The most significant barriers to using digital identity verification for AML/CFT and sanctions compliance stem from outdated laws and regulatory uncertainty.[81] Current Bank Secrecy Act provisions and Section 314(b) frameworks were designed for paper-based processes and have not yet adapted to cryptographically verifiable or privacy-preserving credentials.

1. **Outdated statutory and regulatory definitions.** The BSA and its implementing rules under 31 CFR § 1020.220 were drafted around paper-based and manual "documentary" identity verification. These provisions do not explicitly recognize digitally signed, cryptographically verifiable credentials or zero-knowledge proofs as valid methods of identity verification or ongoing customer due diligence.

2. **Absence of recognition for privacy-preserving methods.** Existing AML frameworks implicitly assume that compliance requires full disclosure of personal data. PETs such as selective disclosure and zero-knowledge proofs can allow verification of identity attributes (e.g., sanctions-screened, age-verified, U.S.-resident) without exposing underlying personal data, but there is no regulatory pathway for their use.

3. **Supervisory uncertainty and lack of examiner guidance.** Financial institutions face inconsistent supervisory treatment when adopting new identity solutions. Examiners lack clear criteria for acceptable assurance levels, credential issuers, revocation processes, or evidence retention for verifiable credentials.

4. **Operational barriers for smaller institutions and VASPs.** Community banks and VASPs face high vendor costs, limited access to interoperable APIs from core processors, and the absence of pre-approved standards or vendor lists for digital identity verification.[82]

5. **Fragmented federal and state initiatives.** State-level initiatives are moving forward quickly, highlighting the need for federal alignment. Utah's State-endorsed Digital Identity (SEDI) program, codified at Utah Code § 63A-16-1201, provides a legal framework for issuing and recognizing verifiable digital credentials. California's SB 786 has created a pathway for digital identity pilots in that state, and several other legislatures have advanced mDL bills. While this activity demonstrates bipartisan momentum, the lack of consistent federal guidance risks producing a fragmented system where compliance obligations vary by jurisdiction.

In short, the landscape today resembles the early days of card payments—when each region, network, and merchant had slightly different rules. Just as the EMV standard eventually unified the ecosystem through shared liability and technical conformity, digital identity will need harmonized regulatory acceptance and wallet certification to scale securely.

Our recommendations are detailed in the next section, part (d).

d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets?

To modernize the U.S. AML/CFT framework for a digital economy, Treasury should focus on the following foundational actions:

1. **Regulatory clarity.** Treasury and FinCEN should issue guidance clarifying that portable digital identity credentials meeting NIST SP 800-63 assurance levels satisfy BSA customer identification, CDD, and sanctions obligations.

2. **Supervisory consistency.** Treasury and federal banking agencies should publish examination handbooks and related guidance that address digital identity verification explicitly, ensuring consistent supervisory treatment and examiner expectations across agencies.

3. **Interoperability and standards**. Treasury should coordinate with state and federal issuers to support interoperability profiles (built on standards like ISO 18013-5/-7, W3C Verifiable Credentials, IETF SD-JWT) and promote a wallet/verifier certification program, similar to how FIDO Alliance certifies authenticators.

4. **Implementation support.** To ease operational burdens, Treasury could sponsor an Identity Trust reference implementation and work with the NIST NCCoE mDL project to extend KYC pilots, providing smaller institutions with tested patterns for adoption.

5. **Legal modernization.** Congress could update statutory language to explicitly recognize attribute-level, privacy-preserving credential exchanges as compliant evidence, reducing reliance on over-collection.

These measures establish the operational and regulatory foundations for verifiable digital credentials—ensuring that identity assurance, privacy protection, and supervisory oversight advance together. The following deep-dive sections outline how these principles can be implemented in practice through updated regulatory guidance, public-private credentialing models, and legislative reform.

Customer Identification Program (CIP)

As noted above, the U.S. AML/CFT framework could be improved to explicitly recognize verifiable digital credentials issued by trusted authorities—including government-issued digital IDs, such as mDLs and/or state-endorsed digital identity (SEDI) credentials, regulated financial institution-issued credentials, and interoperable verifiable credentials that meet defined assurance standards, particularly NIST SP 800-63A-4 (IAL2 or higher)—as valid forms of documentary evidence under the CIP rule.

Leveraging "documentary methods" under the CIP Rule

Under the current framework (31 CFR § 1020.220 et seq.), "documentary methods" have been historically thought about in terms of physical documents, such as government-issued photo IDs on printed plastic cards, passport parchment, or utility bills received in the mail. The rules are technology-neutral, and the Financial Action Task Force 2020 Digital Identity Guidance already affirms that digital identity solutions can satisfy CDD requirements where they provide equivalent reliability.[83]

However, the statute itself does not prescribe specific media (e.g., paper, plastic, or digital), security features (e.g., holograms, security ink, cryptographic signatures), or method of delivery (e.g., fully in person, mail-in, online through a web portal, live video call, or email), or procedures for inspection (e.g., inspecting security seals, processing machine-readable barcodes, validating digital signatures against trust frameworks, use of AI-generated content detection tools). Thus, firms have taken it upon themselves to interpret this statute and implement internal policies as part of their risk-based compliance management programs.

This has resulted in varying degrees of quality across processes to accept CIP requirements or meet CDD obligations, especially for internet-based use cases such as online retail banking. For example, smaller community banks or credit unions may not have IT security experts working alongside their compliance teams, and sometimes may accept easy-to-counterfeit PDF or image uploads over email as evidence, without checking for document authenticity using a verification service or digital signatures. To the hardworking compliance professionals used to scanning a torrent of physical documents with the customer present at their physical location, it may look very similar to what they are used to checking, and therefore reasonable. To the document security expert who also has experience with digital documents, this is a disaster waiting to happen, as most

security features of a physical document do not translate (holograms, UV security ink, etc.) when naively captured as a photo from the user's device. New emerging threats enabled by AI-generated deepfakes, increased availability of AI computation, are turning these gaps into fissures and creating existential risk for the financial sector. [84]

FinCEN could interpret the definition of "documentary methods" to include digital identity credentials that are cryptographically verifiable, issued by trusted authorities and financial institutions that meet a minimum assurance level consistent with NIST SP 800-63-4 (IAL2 or higher).

Leveraging "non-documentary methods" under the CIP Rule

At the same time, FinCEN should clarify when non-documentary methods are applicable to digital credentials. These non-documentary methods could include independent information sources, such as corroboration via third party credential registries, blockchain-anchored attestations, or aggregated KYC utilities. To maintain integrity, such non-documentary verification via independent information sources should be permissible only when the financial institution documents its risk-based rationale for relying on that method and demonstrates independent corroboration of identity attributes.

Leveraging exemptive relief under CIP Rule

If the other pathways for improving the CIP Rule described above are not sufficient, §1020.220(b)(2) authorizes the Secretary of the Treasury, acting through FinCEN, to exempt any bank or type of account from the requirements of this section "by order or regulation" if such exemption is consistent with the purposes of the Bank Secrecy Act. This statutory flexibility provides an existing legal pathway to recognize modern digital identity technologies without requiring a wholesale rewrite of the CIP rule.

In addition to the CIP rule improvements described above, FinCEN can also exercise its authority to issue a conditional exemption or interpretive order clarifying that institutions may satisfy their "documentary verification" obligations under §1020.220(a)(2)(ii)(A) by using verifiable digital credentials that meet defined assurance and authenticity standards. Such credentials could include government-issued digital IDs, regulated financial institution–issued KYC credentials, or interoperable verifiable credentials that are cryptographically bound to the customer and attest to identity attributes verified at NIST IAL2 assurance level or higher.

This exemption would not weaken AML/CFT controls — rather, it would strengthen the "reasonable belief" standard by leveraging cryptographic assurance, tamper-evidence, and ongoing verification. It would also reduce identity theft and false positives by ensuring identity data is verified once by a trusted source and then reused securely across institutions.

Specifically, FinCEN could:

- Issue a pilot or class exemption allowing participating institutions to treat digital identity credentials meeting defined criteria as "documentary evidence" under CIP;
- Require that such credentials be issued by entities subject to AML/CFT supervision (e.g., banks, money service businesses, government agencies, or approved trust frameworks);
- Permit institutions to rely on shared credential registries or trust frameworks that ensure interoperability and auditability across institutions; and
- Maintain examiner access by requiring retention of the credential metadata, issuer information, and validation logs for a defined period (e.g., 5 years).

This exemption would be fully consistent with the purposes of the BSA — namely, to ensure that financial institutions "know their customers," prevent misuse of the financial system, and safeguard national security — while enabling the use of 21st-century identity verification methods that are both more accurate and privacy-protective than legacy document scans.

FinCEN has previously used this authority to accommodate innovation while maintaining AML/CFT safeguards (e.g., prepaid access rules, CVC guidance, and pilot exemptions for low-risk accounts). A similar approach here would provide a risk-based, technology-neutral framework that advances the Administration's digital identity objectives and aligns the United States with FATF's Digital ID Guidance and other international standards.

FinCEN could also structure this exemption as an exemptive relief for equivalent assurance — allowing institutions to adopt digital identity methods that demonstrably achieve a "reasonable belief" of customer identity equal to or greater than that provided by traditional documentary methods. This would create a dynamic compliance framework that promotes innovation without undermining risk integrity.

This modernization would align the U.S. AML/CFT practice with the FATF Digital ID Guidance (2023) and the EU eIDAS 2.0 framework, enabling interoperable, privacy-preserving verification that enhances compliance effectiveness while reducing friction and fraud. Recognizing verifiable digital IDs as valid documentary evidence—and defining clear guardrails for non-documentary digital verification—would provide regulatory certainty for both traditional financial institutions and emerging VASPs, strengthening the integrity and inclusivity of the U.S. financial system.

Leveraging NIST's NCCoE Digital Identity Work to Strengthen CIP Implementation

FinCEN should collaborate with the NIST and NCCoE to accelerate the safe adoption of digital identity technologies in compliance with the CIP requirements under 31 CFR §1020.220. The NCCoE's ongoing work on mobile driver's licenses, verifiable credentials, and digital identity assurance provides a ready technical foundation for this modernization.[85]

The NCCoE's pilot projects have already demonstrated that cryptographically verifiable, privacy-preserving credentials can achieve assurance levels equivalent to or higher than traditional documentary methods, consistent with NIST SP 800-63-4 IAL2. These implementations also provide auditable, privacy-by-design mechanisms for identity proofing and attribute sharing—precisely the controls envisioned by the CIP "reasonable belief" standard.

We recommend that FinCEN leverage the NCCoE's findings and technical playbooks to:

- Establish a joint FinCEN–NIST pilot program to evaluate how mDLs and other NIST-validated digital identity credentials can satisfy "documentary verification" under CIP;
- Develop technical implementation guidance for banks and money services businesses on how to integrate digital credentials that meet NIST IAL2 or higher into their CIP procedures, including use of particular evidence evaluation techniques recommended such as document authentication or biometric matching;
- Create or approve a trust registry usable for the financial sector recognizing approved digital credential issuers (e.g., state DMVs, regulated financial institutions, and certified identity providers) consistent with NCCoE interoperability standards; and
- Use the exemptions authority under §1020.220(b)(2) to permit early adopters to treat NCCoE-validated credentials as acceptable documentary evidence for CIP compliance.

By drawing on the NCCoE's applied research and testbeds, FinCEN can ensure that digital identity verification under the BSA is both technically robust and operationally interoperable, providing financial institutions with clear standards while maintaining strong AML/CFT safeguards.

Travel Rule: Modernizing the Travel Rule Through VDCs

Just as modernizing the CIP rule would improve how institutions verify identities at onboarding, reforming the "Travel Rule" would modernize how verified identity information moves between institutions. The Travel Rule governs the transmission of originator and beneficiary information during funds transfers, but its current design—built for paper-based and intermediary systems—forces institutions to share raw personal data across multiple networks, increasing privacy and cybersecurity risks. By leveraging verifiable digital credentials and standardized API frameworks, the same trust architecture that strengthens KYC can also enable privacy-preserving, machine-readable identity exchange at the transaction layer. This approach would transform Travel Rule compliance from a manual data-sharing exercise into a cryptographically verifiable proof of compliance.

The existing "Travel Rule" under 31 CFR § 1010.410 was designed for an intermediary-based banking system and does not reflect the technological capabilities or privacy expectations of modern digital-asset and cross-border payments. Currently, the rule requires financial institutions and VASPs to transmit originator and beneficiary information—including PII—with every transaction above the $3,000 or $10,000 threshold, depending on the type of originator. While effective in the traditional wire-transfer context, this approach can introduce unnecessary privacy, data security, and interoperability risks in digital environments.

To strengthen compliance integrity while protecting consumer privacy, the Treasury Department and FinCEN should modernize the Travel Rule to allow financial institutions and VASPs to meet their information-transmission obligations through verifiable digital credentials. These credentials, built on cryptographically secure, privacy-preserving, and interoperable standards, would enable institutions to exchange verifiable proofs of identity and compliance, rather than transmitting sensitive personal data in plaintext.

Specifically, we recommend that FinCEN recognize that originator and beneficiary information may be transmitted via a VDC or equivalent digital identity proof if the following conditions are met:

- The credential is issued or attested to by a trusted authority, such as a regulated financial institution, government agency, or certified digital-identity provider;
- The credential meets a minimum assurance level consistent with NIST SP 800-63-4 IAL2 or higher;
- The credential includes, or cryptographically binds to, all information required under § 1010.410(f) and allows the receiving institution to verify authenticity, validity, and non-revocation in real time; and
- The necessary information for lawful investigations is available upon approved legal request by FinCEN or law enforcement.

The use of verifiable credentials would not weaken AML/CFT safeguards; rather, it would strengthen them by ensuring that transmitted identity information is cryptographically authenticated, tamper-evident, and auditable. This approach also aligns with FATF Recommendation 16[86] and the FATF Digital Identity Guidance (2023),[87] both of which emphasize the importance of leveraging trusted digital-ID systems to improve compliance efficiency and reduce illicit-finance risks.

Treasury could implement this modernization incrementally by:

- Launching a FinCEN–NIST pilot program to evaluate how verifiable digital identity credentials can satisfy Travel Rule obligations;

- Developing technical guidance (in partnership with NIST's National Cybersecurity Center of Excellence) outlining credential schemas, signing standards, and interoperability APIs;

- Establishing an Identity Credential Trust Framework that recognizes approved credential issuers and trust registries; and

- Providing a safe harbor or conditional exemption deeming institutions compliant if they use FinCEN-approved credential frameworks, such as an Identity Trust, that offer equivalent or greater assurance than traditional methods.

Modernizing the Travel Rule in this manner would preserve FinCEN's and law enforcement's ability to trace illicit funds, while reducing systemic privacy and cybersecurity risks associated with transmitting PII across intermediaries. It would shift the focus of compliance from data transfer to trust transfer—ensuring that each transaction carries cryptographic proof that both counterparties have been verified under the Bank Secrecy Act, without exposing sensitive identity data unnecessarily.

Building on the suggestions above, the pending Financial Innovation and Technology for the 21st Century Act (the "Market Structure bill") provides an important legislative opportunity to update AML provisions for the digital era. Congress can use this bill to harmonize digital-asset regulation with 21st-century identity standards and privacy technologies by explicitly recognizing verifiable digital credentials and PETs as acceptable identity-verification methods**.** Our recommendation is to amend the BSA/AML section of the bill to authorize Treasury and FinCEN to establish standards under which verifiable digital credentials, decentralized identifiers, and zero-knowledge proofs may satisfy customer identification, due diligence, and Travel Rule requirements when: the credential is issued by a trusted authority (e.g., a financial institution, state DMV, or qualified trust service provider), its integrity and revocation status can be cryptographically verified, and it supports selective disclosure or privacy-preserving proofs of compliance attributes.

Taken together, these recommendations on regulatory clarity, customer identification, and the Travel Rule establish the operational and policy foundations for a privacy-preserving, interoperable digital identity ecosystem within the AML/CFT framework—one that the Market Structure bill could advance as the next legislative step toward codifying these standards and harmonizing financial regulation for the digital era.

e) Treasury will evaluate digital identity verification and consider its impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.

1. **Improvements in the ability of financial institutions to detect illicit activity involving digital assets.** Portable, verifiable digital identity credentials strengthen AML/CFT controls by ensuring that onboarding and ongoing due diligence are tied to cryptographically bound, authoritative attributes rather than unverifiable document scans. This reduces the risk of synthetic identity fraud—a major entry point for money laundering—and enables consistent sanctions screening. When integrated through an Identity Trust, these credentials can also be bound to transactions in real time, allowing illicit actors to be flagged before completing a transfer.

2. **Costs to financial institutions.** Upfront costs include system integration, wallet/verifier deployment, and training compliance staff. However, portable credentials reduce duplication across institutions by enabling "verify once, reuse many times." Over time, institutions benefit from lower false positives, faster onboarding, and reduced manual review, which collectively reduce compliance costs. Smaller institutions may still face barriers without reference implementations or shared service models.

3. **The amount and sensitivity of information that is collected or reviewed.** Digital identity verification reduces the amount of sensitive personal information collected. Instead of transmitting full identity documents, institutions can request only the attributes required for compliance (e.g., “over 18” or “not on OFAC list”). This least-privilege exchange minimizes exposure of personally identifiable information and lowers long-term retention obligations.

4. **Privacy risks associated with the information that is collected or reviewed.** The principal privacy risk is over-collection—if institutions demand full credentials when only an attribute-level proof is necessary. This risk is mitigated by selective-disclosure technologies (e.g., W3C Verifiable Credentials, IETF SD-JWT) and by wallet certification standards that ensure user consent and prevent tracking across verifiers. Utah’s SEDI law (Utah Code § 63A-16-1201) and ACLU-published principles demonstrate that credential frameworks can be designed to advance compliance while protecting privacy.

5. **Operational challenges and efficiency considerations.** Adoption challenges include uneven state issuance of mDLs and other digital credentials, inconsistent assurance levels, and legacy system integration. Pilots like the NCCoE mDL project—which brings together banks, technology vendors, and state issuers to test ISO-compliant mDLs for KYC—demonstrate that these obstacles can be overcome with standard profiles. Once implemented, portable credentials improve efficiency by reducing redundant checks and providing standardized, machine-readable proofs.

6. **Cybersecurity risks.** Like any digital infrastructure, wallets and APIs must be secured against credential theft, spoofing, or replay attacks. These risks can be mitigated through FIPS-validated cryptography, mutual TLS, signed audit receipts, and independent certification of wallets/verifiers. By reducing the need for institutions to store large volumes of raw PII, digital credentials also lower breach impact compared to current document-based methods.

7. **Effectiveness of methods, techniques, or strategies at mitigating illicit finance**. Digital identity verification raises the assurance level of customer onboarding, strengthens sanctions screening, and prevents illicit actors from exploiting weak KYC to access digital asset markets. State-level initiatives such as Utah SEDI (Utah Code § 63A-16-1201) and California SB 786, along with federal pilots at the NCCoE, show that portable credentials are already viable in practice. With clear federal guidance that these tools satisfy BSA/AML obligations, they can be scaled nationwide, yielding a system that is both more effective at detecting illicit finance and more respectful of user privacy.

Q5 - Blockchain

What innovative or novel methods, techniques, or strategies related to blockchain technology and monitoring are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to blockchain technology and monitoring? Please describe how financial institutions are integrating information from blockchain analytics with off-chain data and mention any key challenges associated with using blockchain analytics (e.g., obfuscation tools and methods that can complicate tracing and assessing confidence in attribution or complexities inherent in cluster analysis).

Financial institutions increasingly view blockchains not only as transaction rails but also as a reporting mechanism. Every transaction recorded on-chain functions as a form of public reporting, but on its own this data is incomplete for compliance purposes. The most effective future models would connect blockchain's reporting function to APIs, allowing on-chain activity to be enriched with sanctions lists, case-management data, and verifiable identity credentials. Through an Identity Trust, banks could create compliance records that combine blockchain provenance with off-chain identity attestations, resulting in higher confidence and more auditable outcomes.

Innovative or Novel Methods. Institutions today use blockchain analytics to detect cross-chain laundering typologies, while monitoring tools parse smart-contract interactions to separate legitimate DeFi activity from obfuscation tactics.[88] In the future, banks could embed compliance directly into blockchain transactions—for example, by enabling a smart contract to query an verifiable real-time API for a sanctions or CDD check before execution. This would generate a cryptographic receipt of compliance, creating a new form of embedded reporting that goes beyond today's reliance on after-the-fact monitoring.

Integration with Off-Chain Data. On-chain analytics alone face attribution challenges. Cluster analysis can suggest which addresses are linked, but cannot reliably distinguish custodial accounts or shared wallets.[89] By linking blockchain activity to portable digital identity credentials through APIs, institutions could ground attribution in verifiable attributes. This hybrid model would connect blockchain's inherent reporting function with trusted off-chain data, improving detection while lowering false positives.

Benefits. Blockchain monitoring enables rapid detection of illicit activity across networks and creates immutable records that enhance auditability. If combined with credential proofs exchanged through an API, banks could conduct more accurate and privacy-preserving monitoring, sharing only the attributes required for compliance. Regulators would then be able to review cryptographic logs instead of unverifiable screenshots or PDFs.

Risks and Challenges. A strategic risk is the emergence of fully privacy-preserving blockchains. The explosion of stablecoins—from just a few billion dollars to more than $250 billion in circulation—shows strong consumer demand for digital money, and a portion of that demand is for privacy.[90] This latent demand will drive the development of private technologies, which will only become more efficient and cheaper over time. Compliance programs must be designed with this trajectory in mind or risk being outpaced by market adoption.

Safeguards. Institutions can mitigate current risks by supplementing blockchain analytics with API-based identity exchange, requiring confidence scoring and data lineage in vendor outputs, and adopting a least-privilege design for any identity integration. To prepare for privacy-preserving chains, compliance frameworks will need to evolve toward policy proofs—cryptographic attestations that confirm sanctions or CDD checks without exposing underlying data. Over time, regulators could establish standards for compliance logs, certification of analytics vendors, and wallet assurance programs to ensure trust in these systems.

a) What factors do financial institutions consider when deciding whether to employ blockchain technology and monitoring for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use blockchain technology and monitoring for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use blockchain technology and monitoring, please provide additional details on the rationale for that decision.

When considering whether to adopt blockchain technology and monitoring for AML/CFT and sanctions compliance, financial institutions weigh several factors. The most important is whether regulators recognize blockchain analytics as a valid compliance tool[91] and how examiners evaluate the confidence levels of attribution based on clustering and heuristics. Institutions also assess the quality and availability of vendor solutions, their ability to integrate monitoring outputs into existing case-management systems, and the cost of scaling infrastructure to handle high-volume chains. Another factor is whether blockchain's inherent reporting function can be enriched through APIs with identity attributes, since the ability to link on-chain flows to verifiable off-chain data significantly affects usefulness.

Where institutions employ blockchain monitoring today, it primarily supports suspicious activity detection, sanctions screening, and transaction tracing. Monitoring systems can flag exposure to mixers, darknet markets, or sanctioned entities; trace funds through cross-chain bridges or decentralized exchanges; and provide evidentiary packages for SARs.[92] In the future, blockchain monitoring could also support embedded compliance—for example, enabling smart contracts to check policy proofs via verifiable real-time APIs before executing a transaction. This would allow institutions to demonstrate sanctions screening or CDD verification at the point of execution, not just after the fact.

Institutions that have not yet adopted blockchain monitoring often cite uncertainty about attribution confidence, cost of integration, and regulatory ambiguity.[93] Many are concerned that without clear supervisory expectations, they may invest heavily in monitoring systems only to have examiners question the reliability of outputs. Smaller institutions may also lack the resources to evaluate multiple vendor platforms, keep up with constant changes in obfuscation typologies, or maintain the infrastructure needed for real-time monitoring of high-throughput blockchains.

b) How are financial institutions using blockchain technology and monitoring tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of blockchain technology and monitoring tools with other existing or previous tools used for similar purposes.

Financial institutions today use blockchain technology and monitoring tools mainly to augment existing AML/CFT and sanctions systems rather than replace them. Most deployments run in parallel with legacy sanctions screening and transaction monitoring, allowing blockchain analytics to flag wallet exposure to mixers, darknet markets, or sanctioned services.[94] In some cases, blockchain monitoring has begun to replace manual tracing of wallet flows, but broad substitution of traditional tools has not yet occurred.

Finally, there are recent innovations in the ability for blockchain protocols or smart control layers atop to be able to help meet compliance requirements through embedded regulation. For example, it is possible to keep several accounts to be mapped to the same pseudonymous individual, which would create event triggers such as automatic CTR filings upon reaching a $10,000 threshold of collective transfers, even if used across multiple addresses within that system. However, for these approaches to succeed, a balance must be struck across market adoption, implementability, and compliance risks.

Compared with legacy systems, blockchain monitoring offers greater transparency and speed, since public ledgers inherently disclose transaction flows and allow detection of typologies like cross-chain layering and peel chains. These tools also generate cryptographically verifiable records that strengthen audit trails. At the same time, attribution carries confidence limits that supervisors may not always accept. Traditional systems, by contrast, rely on direct identity data and watchlist matching, which are more definitive but vulnerable to synthetic identities and over-collection. The most effective model blends the two—using blockchain analytics to harness the reporting function of public ledgers while enriching those signals with off-chain data through APIs to produce compliance records that are both verifiable and tied to high-assurance identity attributes.

c) Are there regulatory, legislative, supervisory, or operational obstacles to using blockchain technology and monitoring to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

The most significant obstacles to broader use of blockchain monitoring for AML/CFT and sanctions compliance are regulatory and supervisory uncertainty.[95] While blockchain analytics can surface exposure to mixers, darknet markets, and sanctioned wallets, attribution can rely on probabilistic methods, which examiners may not always accept as equivalent to direct identity evidence, creating hesitancy among financial institutions. Without clear supervisory guidance on how attribution confidence should be assessed, banks risk investing in systems that may not be recognized as meeting BSA obligations.

Legislative and policy gaps also exist. Current frameworks under the Bank Secrecy Act and Section 314(b) do not explicitly contemplate the use of blockchain as a reporting mechanism or the integration of policy proofs into compliance workflows. This is especially relevant given the anticipated growth of privacy-preserving blockchains, driven by latent consumer demand. The explosion of stablecoins demonstrates that digital assets can scale rapidly when they meet user needs, and a meaningful percentage of that demand is for privacy. As privacy chains grow in adoption, institutions will need clear rules for how compliance can be demonstrated when transaction contents are not directly observable.

Our recommendations are detailed in the next section, part (d).

d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of blockchain technology and monitoring for detecting illicit finance involving digital assets.

Treasury and FinCEN should:

1. Issue guidance clarifying how blockchain analytics can be used to satisfy AML/CFT obligations, including expectations for confidence scoring and evidentiary standards.
2. Update statutory and regulatory frameworks to recognize policy-proof mechanisms—cryptographic attestations that confirm sanctions or CDD checks without exposing raw transaction data—as acceptable evidence of compliance, particularly in the context of privacy-preserving blockchains.
3. Map federal expectations to state initiatives (e.g., Utah SEDI; California SB 786) so identity credentials and blockchain monitoring can interoperate across jurisdictions without duplicative document collection.
4. Provide supervisors with examination job aids that explain how to evaluate blockchain monitoring outputs consistently across institutions.

5. Encourage standards-setting around evidence packages and compliance logs to ensure interoperability and auditability.

6. Support smaller institutions through reference implementations, shared services, or NCCoE-style pilots that demonstrate integration of blockchain monitoring with APIs and identity credentials.

With these steps, blockchain monitoring can become a trusted complement to existing compliance tools while preparing the financial system for a future where privacy-preserving blockchains are widely adopted.

e) Treasury will evaluate blockchain technology and monitoring and consider their impact based on the research factors identified in the GENIUS Act.22 Provide any information pertinent to those factors.

1. **Improvements in the ability of financial institutions to detect illicit activity involving digital assets.** Blockchains inherently provide a reporting function by recording all transactions on a public ledger. Monitoring tools allow financial institutions to trace flows, identify exposure to mixers or sanctioned entities, and detect layering through cross-chain bridges or decentralized exchanges. Effectiveness improves when blockchain signals are enriched with off-chain identity attributes via APIs, as this shifts attribution from probabilistic clustering to verifiable credentials. Looking ahead, policy-proof mechanisms will be necessary to sustain effectiveness as activity migrates to privacy-preserving blockchains.

2. **Costs to financial institutions.** Upfront costs include infrastructure for high-volume data ingestion, analytics vendor subscriptions, and integration with case-management systems. Larger institutions are better positioned to absorb these costs, while smaller firms may struggle without shared services or government-supported pilots. Over time, costs may decline as monitoring tools mature and as APIs streamline the process of linking blockchain data to compliance records, reducing manual tracing and improving analyst efficiency.

3. **The amount and sensitivity of information that is collected or reviewed.** Blockchain monitoring generates detailed transaction histories but does not inherently contain personally identifiable information. When paired with credential-based attestations exchanged via an Identity Trust, institutions can collect only the attributes necessary to meet compliance requirements (e.g., sanctions-screening status) rather than storing extensive PII. This reduces the sensitivity of information held by financial institutions compared to legacy document-heavy methods.

4. **Privacy risks associated with the information that is collected or reviewed.** The main risk is over-collection—if institutions pair blockchain analytics with full identity documents instead of attribute-level proofs. Selective-disclosure credentials and policy proofs mitigate this risk, ensuring that compliance objectives are met without exposing unnecessary personal data. As privacy-preserving blockchains proliferate, there is a risk of regulatory overreach through pressure to demand more invasive identity verification; safeguards are needed to keep the balance between effectiveness and user privacy.

5. **Operational challenges and efficiency considerations.** Monitoring high-throughput chains produces large data volumes, requiring constant updates to typologies and analytics models. Attribution confidence is variable, as clustering techniques are inherently heuristic. Efficiency improves when monitoring is integrated with APIs that deliver structured, verifiable data into compliance workflows, reducing manual review. NCCoE-style programs demonstrate that standardized data exchange can lower integration costs and improve operational consistency.

6. **Cybersecurity risks.** Analytics platforms and APIs increase the attack surface, creating risks of credential compromise, endpoint misuse, or data manipulation. These risks can be mitigated with strong authentication, FIPS-validated cryptography, continuous monitoring, and independent certification of

vendor solutions. Importantly, portable credentials reduce systemic risk by minimizing the volume of raw PII stored in institutional databases.

7. **Effectiveness of methods, techniques, or strategies at mitigating illicit finance**. Blockchain technology and monitoring strengthen AML/CFT efforts by leveraging the transparency of public ledgers, detecting cross-chain obfuscation strategies, and creating immutable audit trails. Their long-term effectiveness depends on regulatory clarity around attribution standards and on preparing for a shift toward privacy-preserving blockchains. The Identity Trust offers a conceptual path forward, allowing institutions to integrate blockchain's reporting function with portable, privacy-preserving credentials. By doing so, compliance programs can remain effective even as consumer demand and stablecoin adoption drive greater use of privacy technologies that will only improve and become cheaper over time.

Q6 - Other Innovative Technologies

What innovative or novel methods, techniques, or strategies related to any other innovative technologies such as cryptographic protocols and other privacy-enhancing tools, cloud-based solutions, on-chain compliance tools, oracles, or new verification tools for smart contracts are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to these other innovative technologies?

Innovative or novel methods. Financial institutions are beginning to apply privacy-enhancing technologies (PETs) and trusted execution environments (TEEs) to strengthen AML/CFT while increasing privacy by minimizing exposure of personal data. PETs—such as selective-disclosure credentials (e.g., SD-JWT/VC) and zero-knowledge (ZK) proofs—allow a customer to prove compliance-relevant facts (e.g., "not on the OFAC list," "over 18," "U.S. person") without revealing full identity documents. TEEs (confidential computing) enable screening and analytics on encrypted or shielded data, producing signed attestation reports that the right code ran on the right hardware against the right inputs. Together, these tools let banks check policy conditions and generate verifiable evidence of those checks while limiting raw PII handling.

Benefits. PETs reduce over-collection and lower breach impact by exchanging only the attributes required for a control objective. ZK proofs and SD-JWT/VCs are machine-verifiable, cutting manual review and clerical error. TEEs add a run-time trust layer for sanctions screening, list matching, and alert triage on sensitive datasets, yielding cryptographically signed receipts suitable for examinations. In combination, PETs and TEEs improve precision (fewer false positives from poor data), strengthen auditability, and create a path that remains effective as transaction privacy grows.

Risks and challenges. Key risks include implementation flaws (incorrect proof circuits; misconfigured verifier policy), attestation gaps or rollback/side-channel risks in TEEs, key-management weaknesses, and issuer/wallet assurance variance that can undermine trust in presented credentials. Operationally, smaller institutions may lack in-house expertise; inconsistent supervisory expectations can force duplicative, document-heavy fallbacks that dilute PET/TEE benefits.

Safeguards. Adopt least-privilege design (attribute-only exchanges by default), back proofs with issuer authenticity and revocation checks, and require independent certification of wallets/verifiers and TEE stacks. Enforce strong key lifecycle, replay protection, and evidence logs that chain inputs to code identity to outputs. Establish proof/model governance and maintain clear examiner artifacts: what was proven, by whom, when, with what assurance.

Within an Identity Trust model, PETs supply selective-disclosure proofs from user-controlled credentials, while TEEs provide confidential screening and signed compliance receipts. Banks can bind those receipts to transactions and, where permitted, automate portions of reporting. This keeps identity verification portable and privacy-preserving, yet auditable, and positions programs to remain effective as privacy-preserving blockchains and user demand for confidentiality increase.

a) What factors do financial institutions consider when deciding whether to employ other innovative technologies for AML/CFT and sanctions compliance purposes? For financial institutions that decided to use or plan to use other innovative technologies for these purposes, what specific compliance functions does it/ will it support? For financial institutions that decided not to use other innovative technologies for these purposes, please provide additional details on the rationale for that decision.

When considering PETs and TEEs for AML/CFT and sanctions compliance, financial institutions focus on regulatory acceptance, assurance, and operational feasibility.[96] They want confidence that regulators will accept cryptographic proofs or TEE attestations as valid evidence, that the technologies are independently certified, and that integration will not require duplicative document-based processes.

Where adopted, PETs enable selective disclosure of identity attributes, sanctions screening based on proofs rather than full documents, and verifiable audit logs. TEEs allow institutions to run checks on encrypted data and generate signed attestation receipts, improving both privacy and auditability. These tools reduce PII over-collection and improve precision by tying compliance outcomes to cryptographic evidence.

Institutions holding back cite regulatory uncertainty about examiner acceptance, resource constraints (particularly for smaller firms), and a preference to wait for standardized certification schemes to avoid dependence on proprietary solutions.

b) ***How are financial institutions using other innovative technologies in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of other innovative technologies with other existing or previous tools used for similar purposes.***

Financial institutions are currently using PETs and TEEs to augment, rather than replace, traditional AML/CFT and sanctions compliance tools.[97] Selective-disclosure credentials and zero-knowledge proofs are being layered alongside conventional document checks to validate their effectiveness, while TEEs are tested in parallel with existing screening engines to confirm that attestation receipts meet supervisory expectations.

Compared to legacy methods, these tools show clear advantages: PETs reduce over-collection of personal data, TEEs enable confidential processing of sensitive information, and both provide cryptographically verifiable audit trails. However, their ultimate effectiveness depends on regulatory recognition. For now, most institutions continue to operate PETs and TEEs in parallel with legacy processes, using them to supplement but not yet fully replace established compliance systems.

c) ***Are there regulatory, legislative, supervisory, or operational obstacles to using other innovative technologies to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.***

The principal obstacles are regulatory and supervisory.[98] Current BSA/AML rules and exam procedures were designed around document-centric evidence, not cryptographic proofs or TEE attestation reports. Institutions lack clear confirmation that such artifacts will be accepted as satisfying KYC/CDD/EDD and sanctions obligations without duplicative document collection. Examiner expectations for what constitutes sufficient proof (inputs, algorithms, assurance levels, and audit artifacts) are not standardized, leading firms to run PET/TEE flows in parallel with legacy processes, diluting benefits.

Operational and assurance hurdles also limit adoption.[99] PETs and TEEs require mature key management, issuer/wallet/verifier assurance, and verified attestation chains from hardware to workload. Side-channel and rollback protections, proof/attestation versioning, and revocation handling must be demonstrably in place. Smaller institutions face resource constraints to integrate PET/TEE controls into case management and evidence retention, and fear vendor lock-in absent interoperable profiles and certifications.

Legislative gaps further slow deployment. Neither the BSA nor 314(b) explicitly contemplates attribute-level exchanges or privacy-preserving policy proofs as primary evidence. Without statutory or regulatory recognition, institutions worry that PET/TEE outputs will be treated as supplemental rather than definitive.

Our recommendations are detailed in the next section, part (d).

d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of other innovative technologies for detecting illicit finance involving digital assets?

Treasury and FinCEN should publish supervisory guidance that:

1. recognizes PET-based proofs and TEE attestation receipts as acceptable evidence when mapped to control objectives;
2. defines minimum evidence requirements—what must be logged, signed, time-stamped, and retained—for examinations; and
3. aligns with NIST identity and cryptographic guidance to specify interoperable profiles for SD-JWT/VCs, revocation, and verifier/wallet assurance.

They should also create a conformance and certification path for wallets, verifiers, and TEE stacks (e.g., FIPS-validated crypto, attestation verification, change control) and provide examiner job aids to drive consistency. Modernize 314(b) safe harbors and BSA implementing rules to explicitly permit attribute-only, encrypted exchanges and policy proofs.

Finally, Treasury and FinCEN should sponsor a reference implementation (optionally via an NCCoE-style effort) and shared services to lower integration costs for community banks and credit unions.

These steps would unlock risk-based, privacy-preserving adoption of PETs and TEEs while improving auditability and detection performance.

e) Treasury will evaluate other innovative technologies and consider their impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.

1. **Improvements in the ability of financial institutions to detect illicit activity involving digital assets.** PETs, such as selective-disclosure credentials and zero-knowledge proofs, allow institutions to verify sanctions status, age, or residency without exposing full identity documents, reducing the risk of synthetic identities while preserving privacy. TEEs enable confidential processing of sensitive datasets (e.g., sanctions screening or watchlist checks) and generate cryptographically signed receipts showing that checks were performed. Together, these technologies improve precision and create auditable evidence of compliance actions.

2. **Costs to financial institutions.** Initial implementation requires investment in cryptographic infrastructure, wallet/verifier integration, and TEE-enabled cloud or hardware platforms. Institutions must also train compliance staff to interpret proofs and attestation receipts. Over time, PETs and TEEs can reduce compliance costs by minimizing redundant document collection, lowering false positives, and streamlining examiner reviews with machine-verifiable evidence. Shared services or reference implementations could help smaller institutions manage upfront costs.

3. **The amount and sensitivity of information that is collected or reviewed.** PETs support least-privilege data exchange, transmitting only the attributes required for compliance (e.g., “not on OFAC list”) rather

than full PII. TEEs allow the processing of sensitive data without exposing it to operators or external parties. Compared with legacy systems, PETs and TEEs significantly reduce the volume and sensitivity of data collected and retained.

4. **Privacy risks associated with the information that is collected or reviewed.** Poorly implemented PETs could still allow over-collection if institutions request entire credentials instead of attribute proofs. TEEs may be subject to side-channel attacks or weak attestation verification. These risks are mitigated through standards-based implementation, independent certification, and governance frameworks that enforce attribute-only queries, strong attestation validation, and auditable logging.

5. **Operational challenges and efficiency considerations.** Institutions must integrate proofs and attestation outputs into case-management systems, ensure key-management robustness, and maintain revocation and version control. Smaller institutions may lack in-house cryptographic or attestation expertise. Efficiency gains arise once integrated: PETs reduce manual review, TEEs provide verifiable runtime evidence, and both shorten examiner validation cycles.

6. **Cybersecurity risks.** PETs depend on secure key storage and revocation mechanisms; compromise could allow forged proofs. TEEs require protection against rollback and side-channel exploits. Mitigations include FIPS-validated cryptography, HSM-backed key management, attestation verification, and adversarial testing. Compared to legacy processes that store broad PII, PETs and TEEs reduce systemic breach risk by minimizing sensitive data exposure.

7. **Effectiveness of methods, techniques, or strategies at mitigating illicit finance**. By enabling attribute-level verification and verifiable runtime compliance, PETs and TEEs improve detection of illicit actors while reducing privacy risks. Their effectiveness depends on regulatory recognition that cryptographic proofs and attestation receipts are acceptable compliance evidence. With clear standards and supervisory guidance, these technologies offer a scalable, risk-based path to AML/CFT compliance that remains viable even as digital assets move toward more privacy-preserving architectures.

Conclusion

In summary, the convergence of APIs, AI, digital identity verification, blockchain monitoring, and privacy-enhancing technologies offers the United States an opportunity to modernize financial compliance in ways that are more effective, more efficient, and more respectful of individual privacy. Each of these technologies, when aligned with common standards and supported by clear supervisory guidance, can strengthen the fight against illicit finance while reducing the compliance burdens that weigh heavily on financial institutions. The Identity Trust model illustrates how these components can be integrated into a coherent framework: regulated entities verify and credential individuals, transactions are conducted under pseudonymous identifiers, and regulators gain lawful, auditable access when necessary.

Treasury and its partner agencies have a unique chance to guide this transition. By clarifying evidentiary standards, endorsing privacy-preserving approaches such as selective disclosure and policy proofs, and harmonizing federal rules with state-led initiatives like Utah's SEDI and California's SB 786, the Department can foster a compliance ecosystem that is simultaneously more secure, more private, and more cost-effective. With thoughtful leadership, the United States can set a global standard for financial integrity and digital trust that safeguards both markets and civil liberties.

Endnotes

1. American Association of Motor Vehicle Administrators, 'mDL Implementation and Digital Trust Service Participation", accessed October 13, 2025, https://www.aamva.org/jurisdiction-data-maps#anchorformdlmap

2. Transportation Security Administration, "Digital ID: How It Works," *TSA.gov*, accessed October 13, 2025, https://www.tsa.gov/digital-id#:~:text=How%20it%20Works,to%20present%20at%20TSA%20checkpoints

3. LexisNexis Risk Solutions, *True Cost of Financial Crime Compliance Study — U.S. Report* (2023), https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-for-the-united-states-and-canada.

4. United Nations Office on Drugs and Crime (UNODC), *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes* (2011), https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

5. Drew Dahl, Andrew P Meyer, Michelle Clark Neely, "Scale Matters: Community Banks and Compliance Costs", *Regional Economis*t (July 14, 2016), https://www.stlouisfed.org/publications/regional-economist/july-2016/scale-matters-community-banks-and-compliance-costs

6. Federal Deposit Insurance Corporation (FDIC), *2023 National Survey of Unbanked and Underbanked Households,* https://www.fdic.gov/household-survey.

7. JPMorgan Chase Annual Report (2023), https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/annualreport-2023.pdf

8. Federal Reserve Bank of Kansas City, "The Market Structure of Core Banking Services Providers," *KansasCityFed.org*, (September 2022), https://www.kansascityfed.org/research/payments-system-research-briefings/market-structure-of-core-banking-services-providers.

9. *California Bankers Association v. Shultz*, 416 U.S. 21 (1974).

10. Financial Crimes Enforcement Network (FinCEN), *Annual Report FY 2023,* https://www.fincen.gov/system/files/shared/FinCEN_Infographic_Public_508FINAL_2024_June_7.pdf.

11. U.S. Government Accountability Office (GAO), *Bank Secrecy Act: Agency Efforts to Modernize Currency Transaction Reporting* (GAO-24-XXXX, 2024).

12. Financial Crimes Enforcement Network (FinCEN), *SAR Data Statistics Portal* (2024). https://www.niceactimize.com/blog/fraud-prevention-insights-from-unpacking-the-2024-fincen-sar-stats/

13. Aite-Novarica Group, *Synthetic Identity Fraud: 2024 Trends and Projections*. https://www.niceactimize.com/blog/fraud-prevention-insights-from-unpacking-the-2024-fincen-sar-stats/

14. Shubham Bansal and Aditi Sharma, "Generative AI and Deepfake Detection in Biometric Systems," Cognitive Computation (Springer), 2025, https://link.springer.com/article/10.1007/s12559-025-10469-3

15. World Economic Forum, Reimagining Digital ID (Geneva: World Economic Forum, 2023), https://www.weforum.org/publications/reimagining-digital-id/

16. American Association of Motor Vehicle Administrators, 'mDL Implementation and Digital Trust Service Participation", accessed October 13, 2025, https://www.aamva.org/jurisdiction-data-maps#anchorformdlmap

17. Transportation Security Administration, "Digital ID: How It Works," *TSA.gov*, accessed October 13, 2025, https://www.tsa.gov/digital-id#:~:text=How%20it%20Works,to%20present%20at%20TSA%20checkpoints

18. U.S. General Services Administration, Special Item Number SIN 541519CSP Credential Service Providers,, accessed October 13, 2025, https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it/credential-service-providers

19. U.S. Government Accountability Office, *Social Security Administration:Actions Needed to Help Ensure Success of Electronic Verification Service*, GAO-24-106770, Published: Sep 10, 2024. Publicly Released: Oct 10, 2024, https://www.gao.gov/products/gao-24-106770 .

20. Mike Timoney, *Gen AI is ramping up the threat of synthetic identity fraud,* Federal Reserve Bank of Boston, April 2025, https://www.bostonfed.org/news-and-events/news/2025/04/synthetic-identity-fraud-financial-fraud-expanding-because-of-generative-artificial-intelligence.aspx .

21. Chuo Jun Zhang, Asif Q. Gill, Bo Liu, Memoona J. Anwar,, *AI-based Identity Fraud Detection: A Systematic Review*, arXIV Cornell University, January 16, 2025, https://arxiv.org/abs/2501.09239 .

22. Steven Burnett, Kathleen Kinder, "Privacy Coins vs. Regulatory Compliance Statistics 2025:Adoption Rates and Compliance Issues", (June 16, 2025), https://coinlaw.io/privacy-coins-vs-regulatory-compliance-statistics.

23. *2024 National Money Laundering Risk Assessment* (U.S. Treasury), https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf

24. U.S. Department of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* (2023)

25. Elliptic, The State of Cross-Chain Crime 2025 (London: Elliptic, 2025), https://www.elliptic.co/blog/new-elliptic-report-cross-chain-money-laundering-reaches-22-billion

26. Emma Oye, Sarah Williams, Grace Anderson, "The Effectiveness of Blockchain Analytics in Detecting Illicit Financial Flows", *Research Gate*, (August 2025), https://www.researchgate.net/publication/394929590_The_Effectiveness_of_Blockchain_Analytics_in_Detecting_Illicit_Financial_Flows?__cf_chl_tk=1MY_KlGakuMDeAKvDGK344VP40HhnnqW_x6epXnkK3w-1760373166-1.0.1.1-D48AKth7o67ad1iCW4P9rQjlkr1pFc66hEeAD6_IMMI

27. "2025 Crypto Crime Mid-year Update: Stolen Funds Surge as DPRK Sets New Record", Chainanalysis, (July 17, 2025), https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/

28. Open Banking Implementation Entity (OBIE), *"About Open Banking: Standards and Security," OpenBanking.org.uk*, accessed October 13, 2025, https://www.openbanking.org.uk/about-us/.

29. Open Banking Europe, *"OASIS–OBE: API Identification and Security Standards for APIs and Communications," OpenBankingEurope.eu*, (2020), https://www.openbankingeurope.eu/media/1943/oasis-obe-api-identification-and-security-standards-for-apis-and-communications.pdf.

30. "CHIPS Network Successfully Migrates to ISO 20022 Message Format", *The Clearing House*, (April 10, 2024), https://www.theclearinghouse.org/payment-systems/Articles/2024/04/CHIPS_Network_Migrates_ISO_20022_04-10-2024

31. The Federal Reserve, *August 2025: On the Wire - ISO® 20022 Newsletter*, https://www.frbservices.org/resources/financial-services/wires/iso-20022-implementation-center/on-the-wire-iso-20022-newsletter/august-2025-iso-20022-newsletter#:~:text=Thank%20you%20for%20your%20support,for%20your%20dedication%20and%20preparation.

32. Coinbase, *"x402: The Internet-Native Payment Protocol," Coinbase Developer Platform*, accessed October 13, 2025, https://www.coinbase.com/developer-platform/products/x402.

33. Financial Crimes Enforcement Network (FinCEN), *"BSA E-Filing System Overview," FinCEN.gov*, accessed October 13, 2025, https://bsaefiling.fincen.gov

34. 31 C.F.R. § 1010.430 — *Records to be retained by financial institutions*.

35. USA PATRIOT Act § 314(b); implemented at 31 CFR § 1010.540

36. "Technology Adoption in Financial Services: A sector view of KPMG's 2024 Global Technology Survey", KPMG (2024), https://assets.kpmg.com/content/dam/kpmg/ca/pdf/2024/11/ca-financial-services-global-technology-report-2024-en.pdf "Complex regulatory developments is the top factor denting the investment confidence of financial services executives, 7 percentage points higher than the cross-sector average." slide 7

37. Paul Grewal, "The Bank Secrecy Act Is Broken. Technology Can Fix It.," Coinbase Blog, August 4, 2025, accessed October 13, 2025, https://www.coinbase.com/blog/the-bank-secrecy-act-is-broken-technology-can-fix-it

38. Michael Meyer, “Five Common Data-Sharing Challenges and How to Overcome Them,” Alation, (January 4, 2024), https://www.alation.com/blog/data-sharing-challenges/

39. Fenergo. *KYC & Onboarding Trends in 2024 for Banking: Global KYC Trends in 2024*. Survey of over 450 C-suite executives. Accessed October 2025. https://resources.fenergo.com/reports/kyc-trends-2024-banking. (See discussion of banks adopting multiple point solutions and still relying on them instead of moving to end-to-end enterprise solutions)

40. Elaine Duffus, “The Spreadsheet Era of Tracking Compliance is Ending,” *Scotsman Guide* (May 2025), https://www.wolterskluwer.com/en/expert-insights/the-spreadsheet-era-of-tracking-compliance-is-ending

41. Bank for International Settlements, Committee on Payments and Market Infrastructures, *Service Level Agreements for Cross-Border Payment Arrangements* (2024), 4. https://www.bis.org/cpmi/publ/d222.pdf

42. Deloitte, *Modernizing Legacy Systems in Banking*. (2020), accessed October 2025. https://www.deloitte.com/us/en/Industries/financial-services/articles/modernizing-legacy-systems-in-banking.html

43. Thomas F. Siems, *Do Banking Regulations Disproportionately Impact Smaller Community Banks? Conference of State Bank Supervisors Working Pape*r (25-01, July 29, 2025). https://www.csbs.org/csbs-working-paper-2501-compliance-costs

44. https://bsaefiling.fincen.gov/supported-forms

45. U.S. Treasury, “Under Secretary John Hurley Emphasizes AI as a ‘Force Multiplier’ in AML/CFT Compliance,” *FinTech Global*, October 1, 2025, https://fintech.global/2025/10/01/u-s-treasury-pushes-aml-compliance-into-the-ai-era/

46. Khandakar Md Shafin, Saha Reno, “Integrating Blockchain and Machine Learning for Enhanced Anti-Money Laundering System,” International Journal of Information Technology, vol 17, pp. 2439 - 2447 (2025), https://doi.org/10.1007/s41870-024-02318-7

47. CoinJournal, “*Santander assesses crypto exposure with blockchain analytics*” (2021), https://coinjournal.net/news/santander-assesses-crypto-exposure-with-blockchain-analytics/

48. WorkFusion, “Valley Bank automates sanctions alert adjudication for faster payments, better employee experience,” WorkFusion, 2025, accessed October 14, 2025, https://www.workfusion.com/wp-content/uploads/2025/02/WorkFusion-Valley-Bank-Case-Study.pdf; NICE Actimize, “Automating SARs with ActOne’s X-Sight AI Narrate,” NICEActimize.com, accessed October 14, 2025, https://www.niceactimize.com/Lists/Brochures/GENAI-SAR-narrative-Brochure.pdf

49. Art Mueller, “The Effective Use of AI for SARs,” *ACAMS Today*, August 19, 2024, accessed October 14, 2025, https://www.acamstoday.org/the-effective-use-of-ai-for-sars/; Richard D. May, “Fighting Money Launderers with Artificial Intelligence at HSBC,” *Google Cloud Blog*, November 29, 2023, accessed October 14, 2025, https://cloud.google.com/blog/topics/financial-services/how-hsbc-fights-money-launderers-with-artificial-intelligence; Google Cloud, “AML AI Overview,” *Google Cloud Documentation*, last updated October 2025, accessed October 14, 2025, https://cloud.google.com/financial-services/anti-money-laundering/docs/concepts/overview; NICE Actimize, “Silencing the Noise: Effective Strategies for Reducing False Positives in Transaction Monitoring,” *NICEActimize.com* (brochure), 2024, accessed October 14, 2025, https://www.niceactimize.com/Lists/Brochures/aml-reducing-false-positives-in-transaction-monitoring-brochure.pdf; World Wide Web Consortium (W3C), “First Public Working Draft: Digital Credentials,” *W3C News*, July 1, 2025, accessed October 14, 2025, https://www.w3.org/news/2025/first-public-working-draft-digital-credentials/

50. Linda Jeng, Wayne Chang, Kim Duffy, Kristy Lam, and Elissa Maercklein, “Chains of Trust: Combatting Synthetic Data Risks of AI,” *Oxford Academic* (March 20 2025), https://doi.org/10.1093/9780198945215.003.0096

51. National Institute of Standards and Technology (NIST), “Artificial Intelligence Risk Management Framework: Generative AI Profile (NIST.AI.600-1),” NIST.gov, July 26, 2024, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf;

52. ACAMS−SAS (with KPMG), Global AML Tech Survey (2025). Accessed Oct. 13, 2025. https://www.sas.com/en_sg/news/press-releases/2025/february/anti-money-laundering-survey-ai-machine-learning.html; “Fifty-one percent said their regulator promotes or encourages AI/ML innovation − a 15-point drop from 2021. Those who said regulators are apprehensive or cautious about AI/ML adoption rose from 28% to 36%, and those describing regulators as ‘resistant to change’ more than doubled from 6% to 13%.”

53. Bank of England, “The AI Public-Private Forum: Final report,” bankofengland.co.uk, February 17, 2022, https://www.bankofengland.co.uk/research/fintech/ai-public-private-forum

54. Standard Chartered, “Balancing risk and reward: Deploying AI in the fight against financial crime,” *StandardChartered.com*, October 15, 2024, https://www.sc.com/en/news/corporate-investment-banking/balancing-risk-and-reward-deploying-ai-in-the-fight-against-financial-crime/

55. Bank of England, “The AI Public-Private Forum: Final report,” bankofengland.co.uk, February 17, 2022, https://www.bankofengland.co.uk/research/fintech/ai-public-private-forum

56. Bank of England & Financial Conduct Authority, “Artificial intelligence in UK financial services – 2024,” BankofEngland.co.uk, November 21, 2024, https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024

57. U.S. Government Accountability Office, “Artificial Intelligence: Use and Oversight in Financial Services”, GAO-25-107197 (May 19, 2025), https://www.gao.gov/assets/gao-25-107197.pdf.

58. ACAMS−SAS (with KPMG), Global AML Tech Survey (2025). Accessed Oct. 13, 2025. https://www.sas.com/en_sg/news/press-releases/2025/february/anti-money-laundering-survey-ai-machine-learning.html; “Fifty-one percent said their regulator promotes or encourages AI/ML innovation − a 15-point drop from 2021. Those who said regulators are apprehensive or cautious about AI/ML adoption rose from 28% to 36%, and those describing regulators as ‘resistant to change’ more than doubled from 6% to 13%.”

59. Conference of State Bank Supervisors, “2024 CSBS Annual Survey of Community Banks,” October 2, 2024, https://www.csbs.org/sites/default/files/other-files/FINAL2024CSBSSurvey.pdf.; U.S. Government Accountability Office, *Artificial Intelligence: Use and Oversight in Financial Services (GAO-25-107197)*, May 19, 2025, https://www.gao.gov/assets/gao-25-107197.pdf.

60. WorkFusion, “Valley Bank automates sanctions alert adjudication for faster payments, better employee experience,” February 2025, https://www.workfusion.com/wp-content/uploads/2025/02/WorkFusion-Valley-Bank-Case-Study.pdf

61. Raluca Ochiana, “Emerging Technologies and Trends in Identity Verification, KYC, and KYB Report 2024”, The Payers, (2024), https://thepaypers.com/fintech/reports/emerging-technologies-and-trends-in-identity-verification-kyc-and-kyb-report-2024

62. American Association of Motor Vehicle Administrators, ‘mDL Implementation and Digital Trust Service Participation”, accessed October 13, 2025, https://www.aamva.org/jurisdiction-data-maps#anchorformdlmap

63. Transportation Security Administration, “Digital ID: How It Works,” *TSA.gov*, accessed October 13, 2025, https://www.tsa.gov/digital-id#:~:text=How%20it%20Works,to%20present%20at%20TSA%20checkpoints

64. California Department of Motor Vehicles, “mDL adoption statistics”, https://www.dmv.ca.gov/portal/mdl-adoption-statistics/, accessed October 14, 2025.

65. U.S. Department of Transportation, Federal Highway Administration, Highway Statistics, DL-1C, available at www.fhwa.dot.gov/policyinformation/statistics.cfm as of June 2015, as presented at https://www.bts.gov/content/licensed-drivers accessed October 13, 2025.

66. NCCoE Project Use Cases, accessed October 13, 2025, https://www.nccoe.nist.gov/projects/digital-identities-mdl

67. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

68. American Association of Motor Vehicle Administrators (AAMVA). *Identity Management.* Accessed October 2025. https://www.aamva.org/identity; American Association of Motor Vehicle Administrators (AAMVA). *Driver License and Identification Standards.* Accessed October 2025. https://www.aamva.org/topics/driver-license-and-identification-standards; World Wide Web Consortium (W3C). *Credentials Community Group.* Accessed October 2025. https://w3c-ccg.org/., World Wide Web Consortium (W3C). *W3C Publishes the Digital Credentials API: The Next Step to Privacy-Preserving Identities on the Web.* August 2025. https://www.w3.org/blog/2025/w3c-digital-credentials-api-publication-the-next-step-to-privacy-preserving-identities-on-the-web.

69. Biometric Update. “What Does Selective Disclosure Really Mean? A Deep Dive into the Latest ETSI Technical Report.” September 2023 https://www.biometricupdate.com/202309/what-does-selective-disclosure-really-mean-a-deep-dive-into-the-latest-etsi-technical-report; World Wide Web Consortium (W3C). *Verifiable Credentials Data Model 2.0: Overview.* 2023. https://www.w3.org/TR/vc-overview/; Internet Engineering Task Force (IETF). *Selective Disclosure for JWTs (SD-JWT),* IETF Draft 20, April 2024. https://www.ietf.org/archive/id/draft-ietf-oauth-selective-disclosure-jwt-20.html; European Blockchain

Services Infrastructure (EBSI). *Selective Disclosure – SD-JWT Framework Overview.* 2024. https://hub.ebsi.eu/vc-framework/did/selective-disclosure-sd-jwt.

70. Mobey Forum. *The Rise of Digital Identity Wallets: Will Banks Be Left Behind?* 2023. https://mobeyforum.org/wp-content/uploads/2023/01/The-Rise-of-Digital-Identity-Wallets-report-by-Mobey-Forum.pdf; Taylor Wessing. "Digital Identities in Financial Services: Navigating Risks and Seizing Opportunities." *Global Data Hub,* September 2023.https://www.taylorwessing.com/en/global-data-hub/2023/september---financial-data/digital-identities-in-financial-services-navigating-risks-and-seizing-opportunities

71. National Institute of Standards and Technology (NIST), National Cybersecurity Center of Excellence (NCCoE). "Mobile Driver's License (mDL) Project, Real world use case #2 U.S. Federal Government Credential Service Provider (CSP) and Federation"*,* Accessed October 2025. https://pages.nist.gov/nccoe-mdl-project-static-website/

72. Andrea Flamini, Giada Sciarretta, Mario Scuro, Amir Sharif, Alessandro Tomasi, Silvio Ranise, "On Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials", arXiv:2401.08196

73. American Civil Liberties Union (ACLU). *Digital Identity Guidelines: Second Public Draft.* 2023. https://www.aclu.org/documents/digital-identity-guidelines-second-public-draft

74. Bank for International Settlements, Committee on Payments and Market Infrastructures, *Service Level Agreements for Cross-Border Payment Arrangements* (2024), 4. https://www.bis.org/cpmi/publ/d222.pdf

75. Michael Meyer, "Five Common Data-Sharing Challenges and How to Overcome Them," Alation (January 4, 2024), https://www.alation.com/blog/data-sharing-challenges/

76. "Technology Adoption in Financial Services: A sector view of KPMG's 2024 Global Technology Survey", KPMG (2024), https://assets.kpmg.com/content/dam/kpmg/ca/pdf/2024/11/ca-financial-services-global-technology-report-2024-en.pdf "Complex regulatory developments is the top factor denting the investment confidence of financial services executives, 7 percentage points higher than the cross-sector average." slide 7

77. Nikki Davidson, "Where Are Mobile Driver's Licenses Taking Off? A Data Dive"*, Government Technology* (August 12, 2024), https://www.govtech.com/biz/data/where-are-mobile-drivers-licenses-taking-off-a-data-dive

78. Oliver Wyman, "The Growing Significance of Trusted Digital Identities in U.S. Financial Services," American Bankers Association, (2022), https://www.aba.com/news-research/analysis-guides/the-growing-significance-of-trusted-digital-identities-in-us-financial-services

79. Paul Grewal, "The Bank Secrecy Act Is Broken. Technology Can Fix It.," Coinbase Blog (August 4, 2025), accessed October 13, 2025, https://www.coinbase.com/blog/the-bank-secrecy-act-is-broken-technology-can-fix-it

80. Jeffery Kendall, "Community Banks Can't Delay Core Modernization," Bank Directors Magazine (fourth quarter 2025), https://www.bankdirector.com/article/community-banks-cant-delay-core-modernization

81. "Technology Adoption in Financial Services: A sector view of KPMG's 2024 Global Technology Survey", KPMG (2024), https://assets.kpmg.com/content/dam/kpmg/ca/pdf/2024/11/ca-financial-services-global-technology-report-2024-en.pdf "Complex regulatory developments is the top factor denting the investment confidence of financial services executives, 7 percentage points higher than the cross-sector average." slide 7

82. Thomas F. Siems, *Do Banking Regulations Disproportionately Impact Smaller Community Banks? Conference of State Bank Supervisors Working Pape*r (25-01, July 29, 2025). https://www.csbs.org/csbs-working-paper-2501-compliance-costs

83. Financial Action Task Force (FATF), "Guidance on Digital Identity" (March 2020), pp. 3, 17–18, https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html

84. FinCEN, "FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial," news release (Oct. 7, 2025), https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial

85. NIST, Digital Identities - Mobile Driver's License (mDL), *nist.gov*, accessed October 14, 2025, https://pages.nist.gov/nccoe-mdl-project-static-website/index.html

86. Financial Action Task Force (FATF), “Update — Recommendation 16: Payment Transparency” (June 2025), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html.

87. Financial Action Task Force (FATF), “Guidance on Digital Identity”, (Mar. 2020), https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html.

88. Carter Pape, “NY Regulator Tells Banks to Monitor Customers’ Crypto Risk,” *American Banker*, September 17, 2025, https://www.americanbanker.com/news/ny-regulator-tells-banks-to-monitor-customers-crypto-risk; Elliptic Enterprises Ltd., “The State of Cross-Chain Crime 2025: The Growing Threat of Cross-Chain Laundering and Obfuscation Techniques”, April 2025, https://www.elliptic.co/hubfs/The%20state%20of%20cross-chain%20crime%202025/The%20state%20of%20cross-chain%20crime%202025%20-%20FINAL.pdf.

89. Chainanalysis, “The Data Accuracy Flywheel: How Chainanalysis consistently identifies and verifies blockchain entities, Chainanalysis Company News (January 16, 2024), https://www.chainalysis.com/blog/chainalysis-data-accuracy

90. Steven Burnett, Kathleen Kinder, “Privacy Coins vs. Regulatory Compliance Statistics 2025:Adoption Rates and Compliance Issues”, (June 16, 2025), https://coinlaw.io/privacy-coins-vs-regulatory-compliance-statistics; Gbenga Ibikunle, Vito Mollica, Qiao San, “Why so many coins? Examining the demand for privacy-preserving cryptocurrencies”, The British Accounting Review (2025), pp. 1-19. https://doi.org/10.1016/j.bar.2025.101637; Jack Caporal, “Stablecoin Usage & Trends Survey,” *The Motley Fool* (August 4, 2025), https://www.fool.com/research/stablecoin-usage-trends-survey/; Fumiko Hayashi, Aditi Routh, “U.S. Consumers’ Use of Cryptocurrency for Payments”, Federal Reserve Bank of Kansas City (September 24, 2025), https://www.kansascityfed.org/research/payments-system-research-briefings/us-consumers-use-of-cryptocurrency-for-payments/

91. Ruchi Mishra, Rajesk Kumar Singh, Satish Kumar, Sachin Kumar Mangla, Vikas Kumar, “Critical success factors of Blockchain technology adoption for sustainable and resilient operations in the banking industry during an uncertain business environment,” *Electronic Commerce Research* 25, 595–629 (2025). https://doi.org/10.1007/s10660-023-09707-3

92. Chainanalysis Company News, “Cross River Expands Cryptocurrency Services; Selects Chainalysis as Partner,” March 23, 2022, https://www.chainalysis.com/blog/chainalysis-cross-river/; Circle Internet Financial, LLC, “TRM Labs & Circle Conquer Crypto Compliance,” *Circle Pressroom*, October 25, 2021, https://www.circle.com/en/pressroom/trm-labs-circle-conquer-crypto-compliance; Coinbase, “Our Approach to Preventing Illicit Activity in Crypto,” *Coinbase Blog*, October 17, 2023, https://www.coinbase.com/blog/our-approach-to-preventing-illicit-activity-in-crypto.

93. Nansen, “Overcoming Institutional Blockchain Analytics Hurdles: Key Challenges & Solutions,” *Nansen Blog*, 2024, https://www.nansen.ai/post/overcoming-institutional-blockchain-analytics-hurdles-key-challenges-solutions; Vrun Jain, “What’s Stopping Banks from Fully Embracing Blockchain? A Thorough Exploration of Regulatory, Technological and Operational Challenges,” *ESSEC Metalab Report*, 2024, https://metalab.essec.edu/whats-stopping-banks-from-fully-embracing-blockchain-a-thorough-exploration-of-regulatory-technological-and-operational-challenges; Ron FInklestein, “Regulatory Uncertainty Remains Obstacle for Blockchain Innovation,” *Wall Street Waves*, 2024, https://wallstreetwaves.com/expert-highlights-ongoing-regulatory-challenges-impeding-blockchain-innovation.

94. Chainanalysis Company News, “Cross River Expands Cryptocurrency Services; Selects Chainalysis as Partner,” March 23, 2022, https://www.chainalysis.com/blog/chainalysis-cross-river/ “... employed in tandem and integrated into Cross River’s existing technology stack…”

95. Ruchi Mishra, Rajesk Kumar Singh, Satish Kumar, Sachin Kumar Mangla, Vikas Kumar, “Critical success factors of Blockchain technology adoption for sustainable and resilient operations in the banking industry during an uncertain business environment,” *Electronic Commerce Research* 25, 595–629 (2025). https://doi.org/10.1007/s10660-023-09707-3; Hartman, “AI and Community Banks - Understanding the risks and Opportunities,” September 16, 2024, https://hartmanadvisors.com/ai-and-community-banks-understanding-the-risks-and-opportunities

96. Natalie Hurler, “Privacy Enhancing Technologies (PETs) in the Fight Against Financial Crime,” MSG Compliance Blog (July 21, 2021), https://www.msg-compliance.de/en/blog/privacy-enhancing-technologies-in-the-fight-against-financial-crime

97. Mastercard, “Privacy Enhancing Technologies White Paper,” (February 2024), https://b2b.mastercard.com/media/z0pnu32l/privacy-enhancing-technologies-white-paper-final.pdf

98. Center for Information Policy Leadership, Privacy Enhancing and Privacy Preserving Technologies: Understand the role of PETs and PPTs in the digital age, (December 2023),

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf; Shuang Wang, Muhammad Asif, Muhammmad FarrukhShahazad, Muhammad Ashfaq, “Data privacy and cybersecurity challenges in the digital transformation of the banking sector,” *Computers and Security* vol. 147 (December 2024), https://doi.org/10.1016/j.cose.2024.104051

99. Tim Geppert, Stefan Deml, David Sturzenegger, Nico Ebert, “Trusted Execution Environments: Applications and organizational challenges,” Frontiers in Computer Science, vol.4 (July 7, 2022), https://doi.org/10.3389/fcomp.2022.930741