FinClusive Digital Identity & Compliance-Backed Credentials

Decentralized Identifiers & Verifiable Credentials

May 2024

FinClusive – a provider of Compliance-as-a-Service (CaaS) issues compliance-backed credentials to its partners, customers, and clients as a fully compliant, KYC/KYB verifiable credential and digital identity.

Table of Contents

Introduction

FinClusive, as a global regulatory technology platform, issues Decentralized Identifiers (DIDs) with properties that can enable Self-Sovereign Identity (SSI) along with Compliance-backed Verifiable Credentials (CVC). The DID is based on open standards driven by the World Wide Web Consortium (W3C), the Decentralized Identity Foundation (DIF), and the Hyperledger Project at the Linux Foundation.

FinClusive actively engages with the growing digital identity community. This includes participation in organizations like the Open ID Foundation, Web3ID Coalition, Sovrin Foundation, Trust Over IP (ToIP) Foundation, among others. Our goal is to contribute to the development of globalized standards and protocols that enhance the issuance, protection, and verification/validation of digital identity credentials. This effort is crucial in modernizing anti-money laundering/financial crimes compliance (AML/FCC) operations within the financial services industry. This applies to a range of sectors including traditional finance/TradFi (both banking and non-banking financial institutions), decentralized finance (DeFi), web3 applications, blockchain-enabled networks, and virtual asset service providers (VASPs).

Additionally, as new 'consortia' continue to form, we aim to support them in applying and utilizing DIDs and CVCs. Through our services, we provide comprehensive global know your customer/know your business (KYC/KYB) and due diligence tools. These are essential for both traditional and emerging financial service providers to achieve two critical objectives: maintaining comprehensive financial system integrity controls and promoting secure, privacy-protected financial inclusion efforts.

Furthermore, as new TradFi and DeFi networks continue to emerge, FinClusive's platform plays a key role through our global regulatory policy and technology framework[1], and collaborations with entities like the Frictionless Commerce Foundation (FCF)[2] and the Global Acceptance Network (GAN)[3]. Our goal is to align modernized digital identity applications with essential KYC/KYB and financial crimes compliance (FCC) tools. This approach serves to establish a global 'utility' of regulatory compliance tools under a common and consistent framework. It ensures that diversified financial services are interoperable with continually evolving AML/FCC rules and obligations.

---

[1] FinClusive has led the Compliance and Inclusive Finance Working Group – a global consortia providing a market/industry-led policy initiative for the application of AML/FCC best practices and guidance – *The Rulebook* – to enable the modernized application of AML/FCC tools and with concerted application to the growing non-bank financial services sector, in particular decentralized, alternative financial services, and web3/blockchain-enabled platforms.
Rulebook overview: https://finclusive.com/resources/rulebook
Rulebook full text: https://docs.google.com/document/d/1SswHBZ1pwuIUcePeFe8czOoAOaHE78ij4okXuQq5OW0/edit

[2] The Frictionless Commerce Foundation (FCF) has been initiated by TBD/Block and Circle to align open standards and open-source technologies for financial services and payment applications – including through the use of decentralized financial services networks and payment stablecoins. FinClusive is assisting with the governance elements of the framework as related to AML/FCC applications and the coverage of essential KYC/KYB, identity verification, and monitoring tools: https://www.tbd.website/blog/tbd-partners-with-circle

[3] The Global Acceptance Network (GAN), spearheaded by GenDigital, aims to harmonize universal frameworks regarding verifiable credentials and payments. This initiative seeks to foster trust, credibility, and interoperability among various networks, facilitating the secure exchange of sensitive personal data. It is specifically designed to support activities subject to stringent regulations, such as know your customer (KYC) and identity verification processes, across different counterparties and jurisdictions.

In this regard, FinClusive's Compliance as a Service (CaaS) stack orchestrates and integrates essential functions such as KYC/KYB, client risk scoring, ongoing and automated client monitoring, global watchlist and sanctions screening, and comprehensive customer and enhanced due diligence (CDD/EDD) capabilities. Moreover, when combined with transaction monitoring and other fiat and digital asset/token/wallet screening and analytics tools, CaaS provides a comprehensive approach to regulatory compliance that embeds reusable KYC credentials through its DID/CVC enablements.

"To get financial services right, we need to get identity right. It is vital to building trust in the system. Getting identity 'right' means implementing identity solutions that preserve privacy and security, promote financial inclusion, and protect the integrity of the financial system."

— Jimmy Kirby, Former Acting Deputy Director of the Financial Crimes Enforcement Network (FinCEN)

I. Decentralized Identifier (DID)

Decentralized Identifiers (DIDs) are cryptographically secure identifiers managed directly by their subjects, such as individuals, organizations, etc., eliminating the need for third-party Identity Providers (IdPs). These identifiers allow subjects to prove ownership of their identity through their wallets on mobile devices, web applications, or printed QR codes. Leveraging their DID, subjects can acquire a Compliance-backed Verifiable Credential (CVC) from the FinClusive platform, which they can then use as proof of compliance claims without the need to rerun the checks.

FinClusive's Compliance as a Service (CaaS) platform offers organizations access to global KYC/KYB tools and due diligence capabilities. This service ensures that the credentials issued are supported by thorough background checks and screenings, thereby providing a foundation for these credentials. Consequently, KYC/KYB-backed VCs facilitate a client-centered approach to operability and control, enhancing secure sharing and reusability within financial service provider platforms and across various service providers. This creates an 'Embedded Compliance and Credential' framework that aligns with global AML/FCC standards. Such a framework allows service providers to meet regulatory compliance requirements across all jurisdictions of operation.

DIDs use Decentralized Public Key Infrastructure (DPKI) technology to assign digital identities to entities such as individuals, organizations, and Internet of Things (IoT) devices. DPKI technology shifts the control of identities back to their rightful owners, bringing the power of cryptography to everyday users by delegating the responsibility of public key management to secure decentralized data stores (blockchains and public databases). As a result, DIDs facilitate the creation of a web of trust, enabling anyone and anything to establish trustworthy digital relationships.

II. Verifiable Credential (VC)

Identity records play a crucial role in our daily lives, serving as essential tools for verification and authentication across various domains. A driver's license, for example, is required as proof of eligibility to operate a vehicle. Educational institutions issue diplomas to certify an individual's academic achievements. Passports are used to verify a person's nationality. Moreover, compliance results are employed by financial institutions and service providers for KYC/KYB purposes, among other examples. These documents collectively underscore the importance of reliable identity verification mechanisms in facilitating secure and efficient interactions in society.

VCs form the foundation for verifiable data in the web of trust. They can contain many types of information as well as different types of credentials. Many software providers, private and public institutions, and a wide range of businesses are implementing this technology in their offerings. FinClusive has developed KYC/KYB-backed VCs that can be issued to its partners, customers, and clients (customers' customers). These VCs serve a dual purpose: they provide a means for KYC/KYB verification that is applicable across both centralized and decentralized domains, and they empower users (recipients of the credential) with the ability to grant permission to third-party verifiers. These verifiers can then swiftly and securely confirm the authenticity of an individual's identity and their KYC/KYB status, incorporating privacy safeguards near instantaneously and directly into the process.

FinClusive DID and VC Implementation Model

I. FinClusive Compliance-as-a-Service (CaaS)

FinClusive's CaaS provides a comprehensive full-stack AML/FCC service to regulated and non-regulated financial services engaging both individuals and business entities (clients, users, or subjects). The CaaS service embeds the DID/VC through its KYC/KYB processes and creates a unique identifier called a 'FinCID,' which links to all data associated with a subject stored on the platform. The subject's data encompasses both the attributes scrutinized through due diligence and background checks, evaluated according to their risk level, and all the transaction data produced through various platform services during the lifecycle of engagement with the client.

All financial services providers must establish—with confidence—who their clients are at the time of onboarding and must consistently verify, validate, and monitor these identities throughout the duration of their engagement. These requirements are in place to ensure attributes are continuously known and incorporated into the service providers' Customer Information Program (CIP). This rigorous approach helps protect clients from potential exploitation or compromise, including threats to their personal identity. Notably, reports of suspicious activities related to identity saw an increase of over 15% from

2021 to 2022, highlighting the growing importance of diligent identity verification and monitoring practices.

Data elements encompass a wide array of compliance and financial information, crucial for maintaining regulatory standards and facilitating secure transactions. These include:

- KYC (Know Your Customer) and KYB (Know Your Business) results
- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) results
- Global sanctions and watchlist screens
- Master & Sub-Accounts (in FinClusive's Gateway Services application)
- Value Transfer Details (information on transactions, including fiat and crypto payments, whether through traditional banking channels, blockchain networks, or peer-to-peer (P2P) systems)
- Anti-Money Laundering (AML) & Transaction Monitoring Rules execution
- Legal Entity Identifier (LEIs) validation (or issuance if such LEI does not exist for a particular entity client)
- Associated digital wallets belonging or under the control of the client
- Any other attribute as may be necessary for FinClusive's customers to enable services to their clients

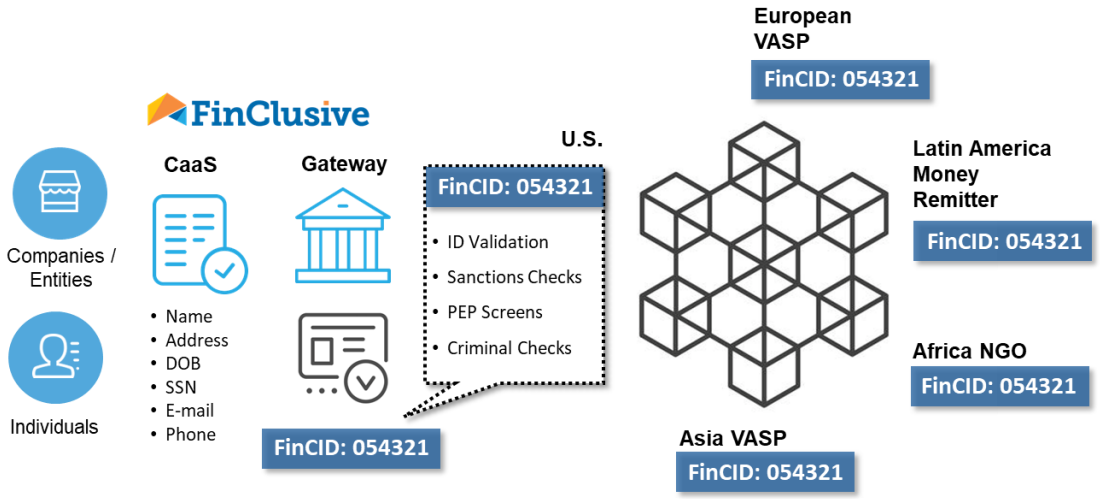
The FinCID is designed to be associated with any 'client-related attribute', encompassing a wide array of data points. This includes, but is not limited to:

- The client's underlying personal/entity identifying information (PII/EII)
- The client's account, digital wallet details, or other relevant transaction facilitation information
- Transaction data and flows
- Affiliate data (counterparties with whom they transact, etc.)

Traditionally, both regulated banks and non-bank Financial Institutions (FIs) are required to conduct KYC, KYB, and various levels of CDD and EDD for the subjects who wish to utilize their services, applying a risk-based approach tailored to the clients' risk profiles. However, there is often a reluctance to depend on KYC/KYB verifications conducted by third parties. Historically, this has led to a scarcity in the sharing or reusing of KYC/KYB and other related screening results among FIs. This lack of interoperability contributes to increased costs and extended timeframes for onboarding a client to an FI or for revalidating clients who may have already undergone KYC/KYB processes or been included in an FI's Customer Information Program (CIP).

To address the challenges associated with the sharing and reuse of compliance information while safeguarding PII/EII, FinClusive has developed and implemented a solution named 'CDD Check Connect'.

CDD Check Connect operates through a multilateral information-sharing agreement between various partners and customers on the FinClusive CaaS platform. It enables Financial Institutions (FIs), regardless of whether they are customers of FinClusive, to securely share compliance data and verify the credentials associated with subject run through KYC/KYB.



Further, the level of DD as determined through the subjects' risk profile further delineates the risk associated with a client and can include levels and types of due diligence from 'basic' (e.g., name match and sanctions screen) to 'enhanced' (e.g., social and adverse media, source of wealth, etc.).

This multilateral/reliance agreement structure has been updated and refined to include standardized language of an AML compliance 'reliance agreement' which is constructed to enable the following:

- **Third-party Financial Institution (FI) Reliance:** A third-party FI can 'rely' on the KYC/KYB/compliance processes of another FI. The FI could be FinClusive itself or another customer of FinClusive utilizing its Compliance-as-a-Service (CaaS), such as a blockchain anchor, multiple product/service offices within one financial institution, multiple networked/cooperative institutions (e.g., credit unions, marketplace participants).
- **Reinforcement of CaaS Use and Value:** The agreement emphasizes the importance and utility of FinClusive's CaaS and its KYC/KYB processes. This is achieved not only through technological application but also through governance and global AML/FCC policies that serve as CaaS' foundation to meet AML/FCC obligations.
- **Support as an EDD and Managed Services Provider:** Where necessary, the agreement positions FinClusive to act as a provider of EDD and managed services. This role is particularly relevant for partners and customers requiring remediation, third-party compliance support, or those under monitoring and/or needing enhanced AML/FCC measures as mandated by regulators or FI partners.

The CaaS platform, designed as a multi-tenant service, simplifies the implementation of CDD Check Connect, prioritizing the confidentiality of subjects' data while facilitating the necessary sharing of compliance outcomes. This sharing is crucial for the verification/validation of a subject in accordance with regulatory requirements. Additionally, CDD Check Connect is structured to ensure that any disclosure of underlying information occurs only with explicit authorization from the customer (originator of the client subject) and/or the client subject themselves.

II. FinClusive DID and VC Solution

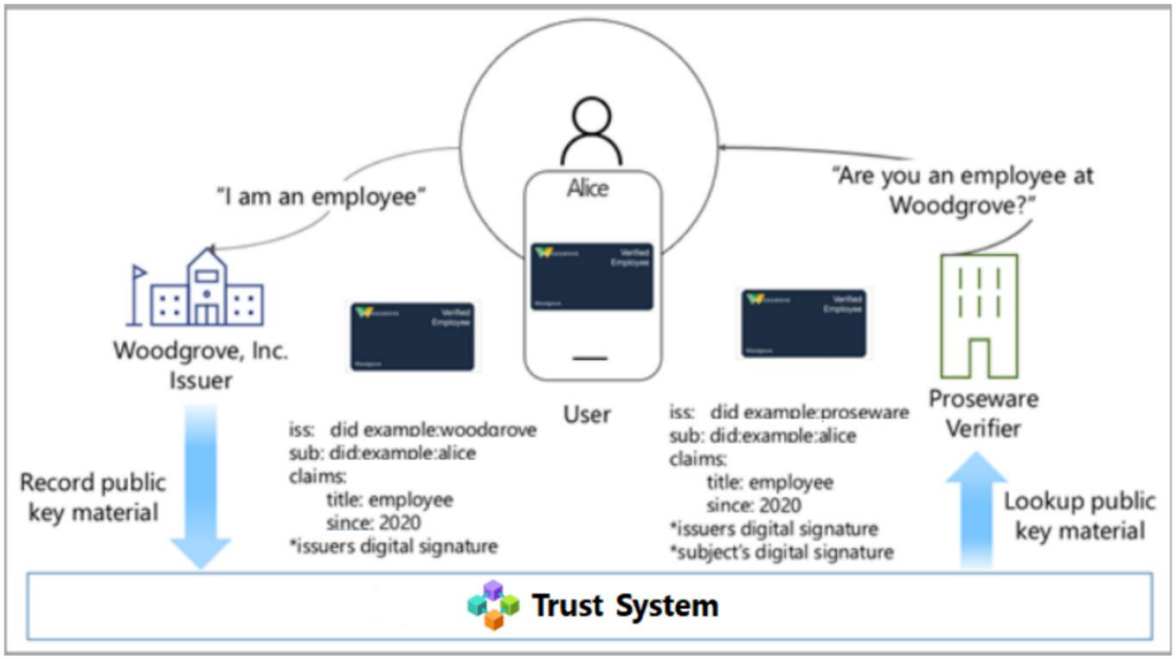
FinClusive leverages its current multi-tenant platform capabilities, CDD Check Connect service, and FinCID to provide a true Decentralized Identity (DID) backed by a KYC/KYB Compliance-backed Verifiable Credential (CVC). FinClusive does not compete directly with existing, or future DID and VC registries. Rather, FinClusive leverages one or more of these registries (where they have adopted the standard specification proposed and implemented by W3C).

As competing standards are aligned more formally, FinClusive's credentials and their application will look to conform to the essential specifications for interoperability, privacy protection, permissioning, and compliance with evolving AML/FCC standards. The solution also supports ongoing monitoring of results so that the credential is a dynamic instrument that protects the onboarding institutions and verifies partners with a valid credential. Moreover, ongoing monitoring is embedded as a part of the CaaS application to support broader CIP requirements associated with all FIs. If at any time, through that monitoring, the acceptability of the credential becomes invalid, the credential can be revoked and made unusable by the client without action from the corresponding issuer or verifier.
The primary objective is to achieve interoperability among multiple providers while ensuring a consistent approach in risk profiling and executing the necessary KYC/KYB actions to manage the risks associated with clients as indicated by the FinCID assigned/issued.

The standard specification consists of the following roles:

III. Definitions of Roles

- **Subject/User:** An individual or entity about whom VCs (attested claims) are issued.
- **Holder:** An entity that holds one or more VCs in a wallet and generates verifiable presentations for verifiers. Typically, the holder is the subject; however, for minors, a parent or guardian may act as the holder.
- **Issuer:** An entity that verifies claims about a subject and issues a VC based on these claims, then sends it to the holder.
- **Verifier:** An entity (or relying party) that receives VCs from a holder and checks the claims made by the issuer, without needing direct interaction with the issuer.
- **Verifiable data registry:** A system that mediates the creation and verification of identifiers, public keys, VC schemas, revocation registries, etc. A blockchain or public database is typically used as the registry and the VCs (asserted claims) are never stored in the registry.



IV. FinClusive (FinCID) – Compliance-backed Verifiable Credential (CVC) Schema and Service

As part of its CaaS platform, FinClusive defines and implements a Compliance Verifiable Schema, which includes, at a minimum, the following elements:

- Compliance Risk Profile Level (see default profiles and declared vs. verified data for DD)
- Issued FinCID
- Creation Date
- Valid Date
- Compliance Status (active, inactive, revoked, etc.)
- Revocation Date
- FinClusive Compliance API URL (to access additional compliance data associated with a subject)

This list will continually be refined and expanded with additional attributes and related compliance outcomes, reflecting the level of risk and the due diligence conducted during the KYC/KYB validation and revalidation processes.

Note: The schema can be enhanced with additional compliance results data as a business determines to be valuable or requires a different level of due diligence.

FinClusive is an *Authorized Issuer* of the aforementioned credential to a subject (individual or entity). Ownership of the compliance credential indicates that the subject has undergone the necessary level of KYC/KYB due diligence and requisite compliance screening. Additional data can be accessed by making a request to the compliance API URL.

- The primary goal is for partner FIs to be provided with the FinCIDs of clients they have onboarded and subjected to KYC/KYB processes, including any necessary adjustments to the DD profile based on the customer's risk and CIP requirements. The FinCID can also serve as a comprehensive DID, and the VC can be delivered directly to a client's wallet for use as needed. This enables clients to present verifiable proof of their legitimacy and KYC/KYB compliance data associated with their FinCID/profile to other FIs.

Based on the level of the compliance profile, the expiry timeline, its associated revalidation status, the compliance status, and the revocation date will be updated automatically. Subjects can store their compliance credentials in their wallets and present them to any verifier, i.e.; an FI or an entity that would like to verify their first-tier compliance status.

- The individual or entity will be notified of their FinCID, which is enabled through delivery and/or verification by FinClusive of their FinCID.
- The verifiers (multiple FIs that need to verify the subject's FinCID) can do so through the compliance API URL and/or by using the CDD Check.

To obtain additional data, the verifier can make a direct request to the API endpoint. The authentication and authorization of the API endpoint, as well as the data returned by the API for both in-network and out-of-network verifiers, are managed through the CDD Check Connect application as follows:

- **In-network (a FinClusive full CaaS customer)** – Full CaaS access includes CDD Check
    - Permission from the originating customer (or client) is required to provide underlying PII/EII. This requires consent from one or both parties, as part of the multilateral agreement mentioned above.
    - Checking of FinCIDs via CDD Check is included as part of CaaS.
- **Out-of-network (not a FinClusive CaaS customer)** – Access only to CDD Check Connect (in UI and via API)
    - Participants can opt for the full CaaS, which would place them under a comprehensive Master Service Agreement (MSA) that includes the provisions of the multilateral agreement.
    - Participants can choose to maintain limited access to CaaS and CDD Check capabilities, incurring a 'dipping fee' for each query to verify/validate a client/subject's FinCID and compliance results.

In-Network Entities

Counterparties not part of FinClusive's multilateral agreement who seek to validate customers compliance verification results by querying CDD Check Connect.

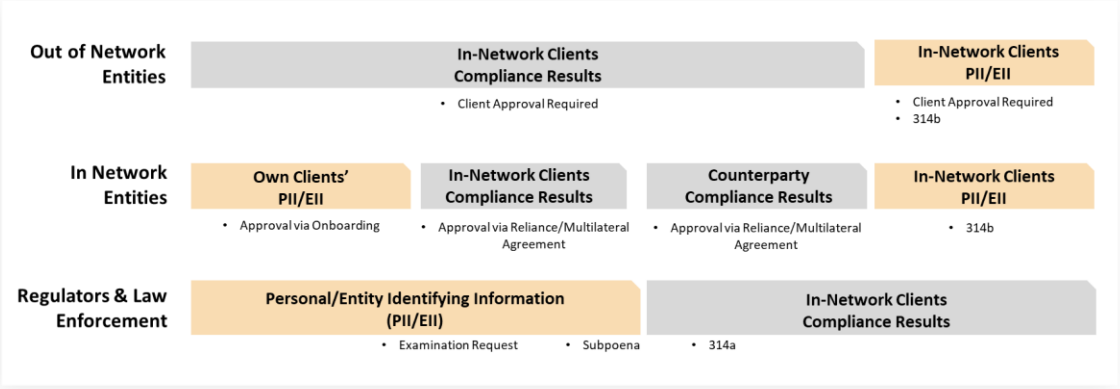
Out of Network Entities

Counterparties not part of FinClusive's multilateral agreement who seek to validate customers compliance verification results by querying CDD Check Connect.

- Clients of customers can 'permission' their verifiable credential to a third party to be verified for their KYC/KYB status

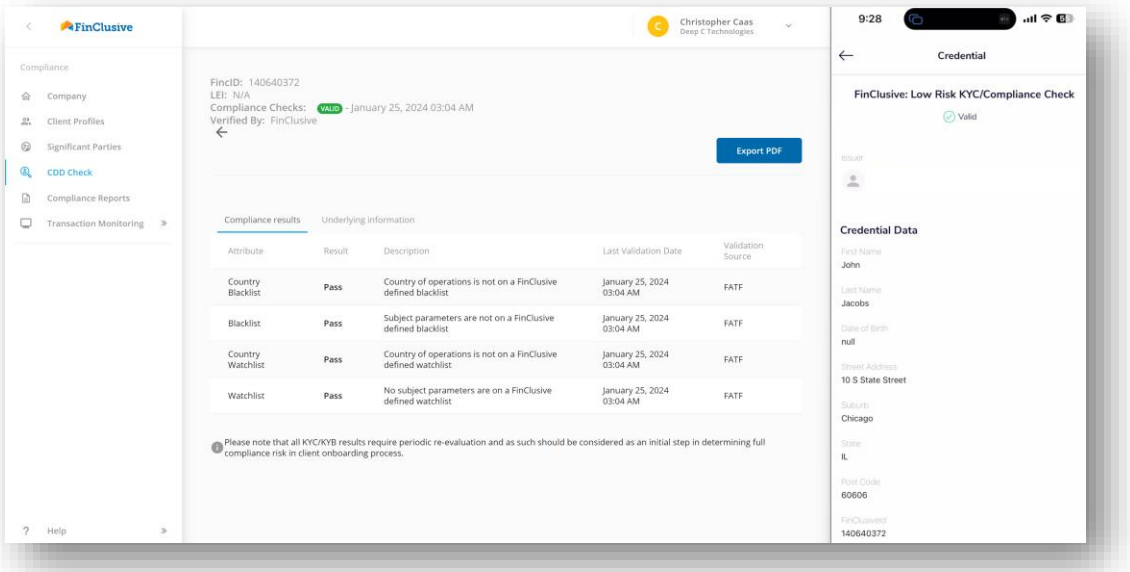
Regulators & Law Enforcement

U.S. and foreign regulatory/law enforcement agencies can query compliance results and/or underlying PII/EII or transaction data related to an investigation based on a bona fide request.

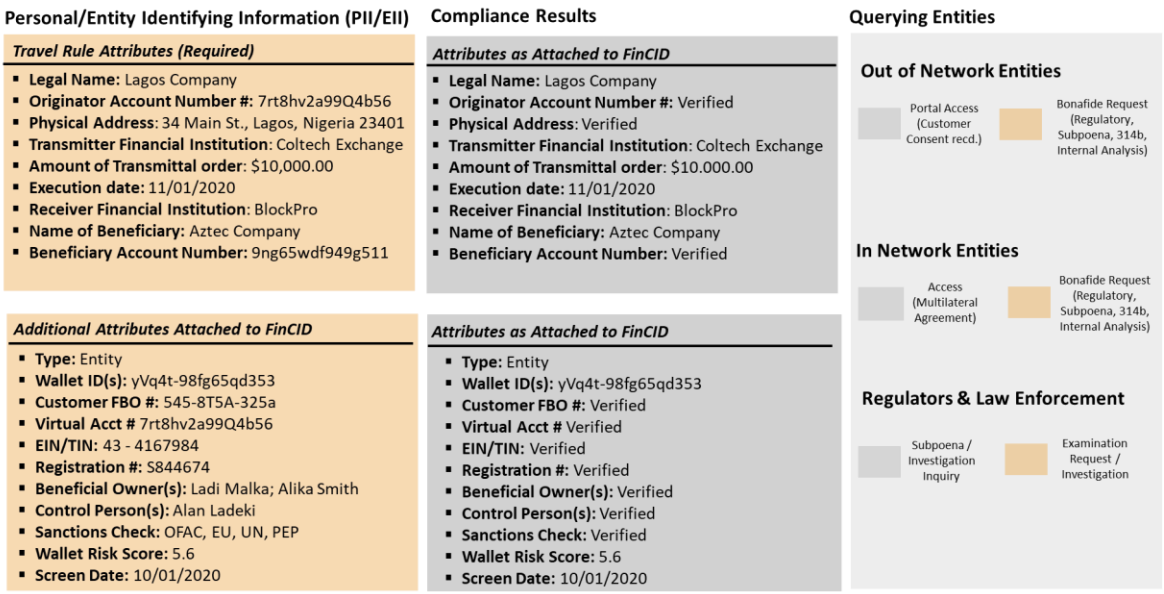


The screenshot below provides an example of the CDD Check Connect results, where no Personal Identifying Information (PII) is shared, only the outcomes of these checks. These are presented in relation to a specific client's risk profile, aligning with the service provider's (issuer or verifier) risk appetite and methodology.

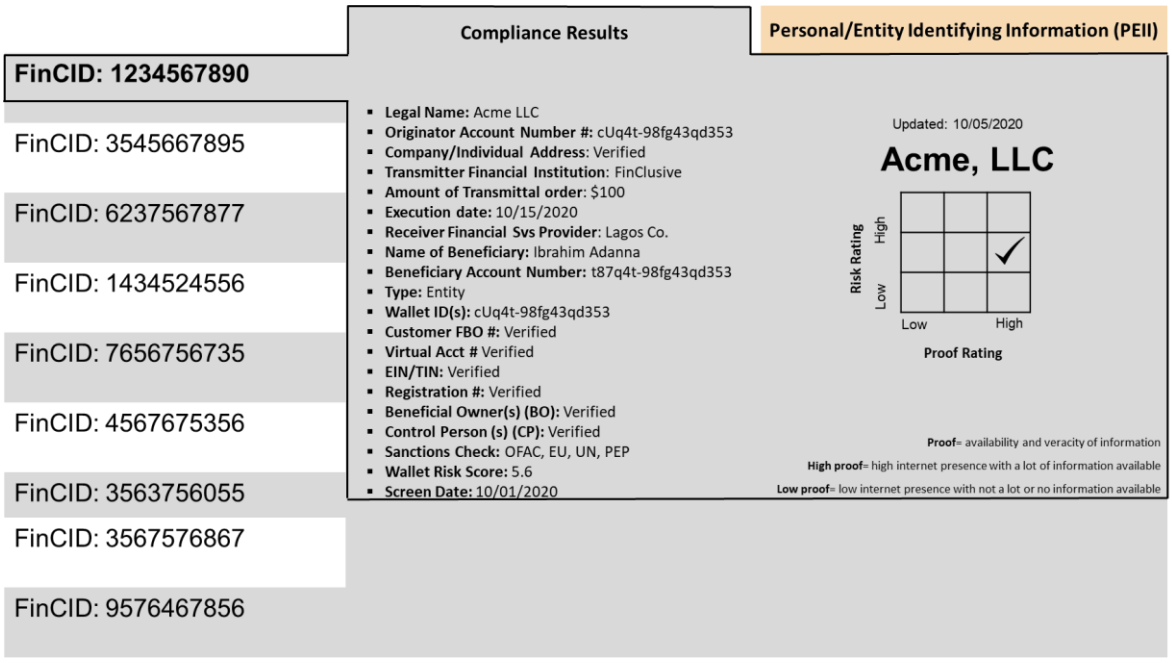
On the right-hand side, you will see the unhosted wallet solution displaying what a valid credential looks like within their wallet.



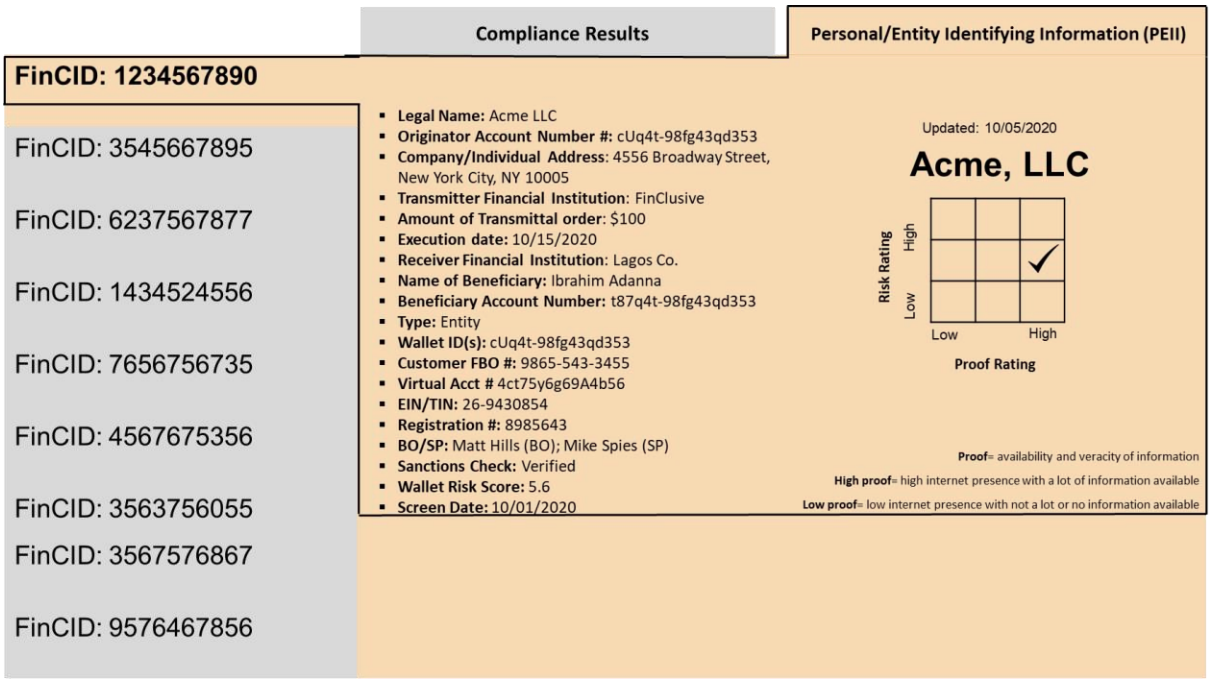
The illustration below shows the exposure of underlying attributes associated with PII/EII against the compliance results. These can be searched by FinCID and managed accordingly within the CPI of the service providers' compliance program.



As displayed to inquiring institutions for verification:



As displayed to the issuer and originator of the client and/or to the client directly:

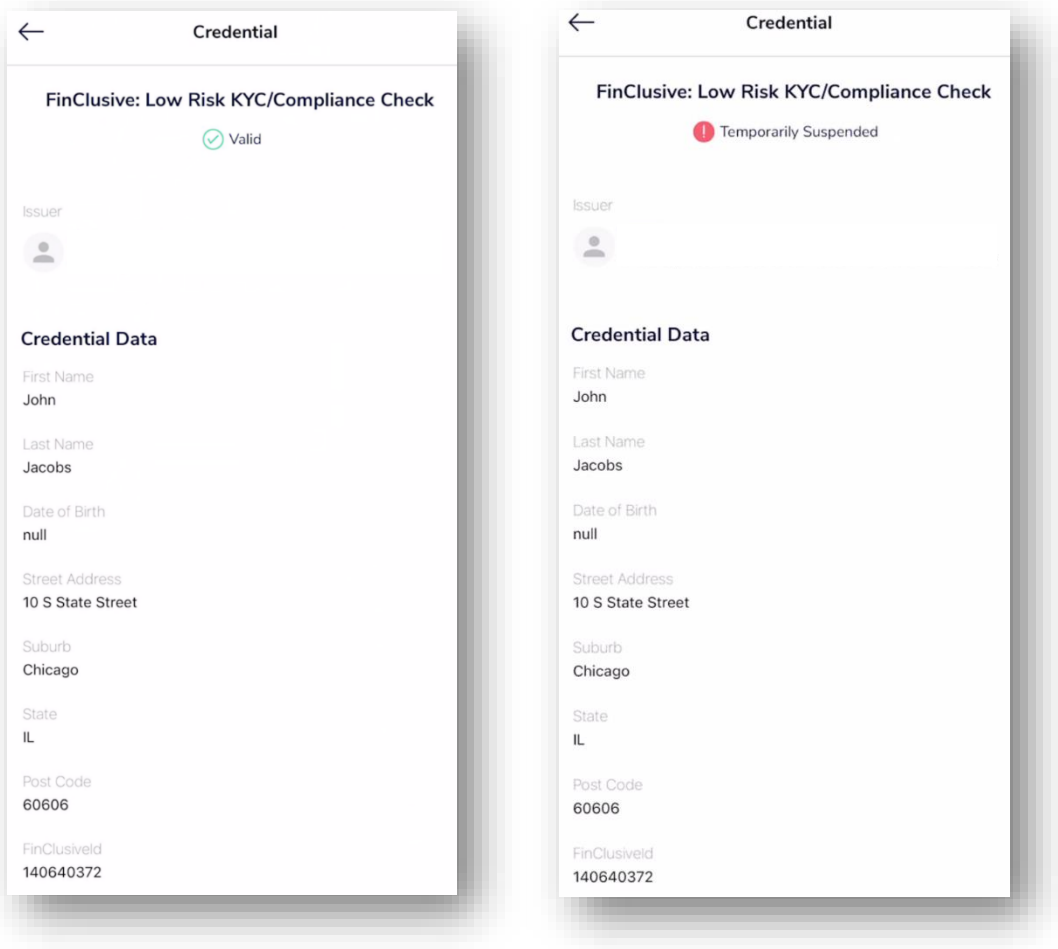


V. Ongoing Monitoring and Revocation

Automated and ongoing monitoring is applied to subjects in a manner that aligns with the specific institution's risk appetite, client risk profiling, and underlying profile. The frequency of this monitoring can be adjusted as needed, but by default, it is set to occur at least every 15 minutes. The scope of the screening can be customized to ensure specific areas are monitored. This may include sanctions, Politically Exposed Persons (PEP), and additional watchlists, wanted lists, and adverse media lists.

If a potential match is identified during the ongoing monitoring or revalidation process, the credential is temporarily placed in a 'suspended' status, marked as 'pending action' by the originating issuer, service provider, or the verifier in the case of client approval. This status allows the issuing institution or individual to review the potential match results and either dismiss it as a false positive or apply additional levels of assurance for the credential to be reinstated to a valid status. Until the credential is restored to a valid status, it cannot be shared or verified.

The screenshots below are examples of the credential in both a valid and a temporarily suspended status.



VI. Wallets and Agents

The role of the user (holder) is central to the ecosystem, offering greater sovereignty over their information and empowering them to manage their digital identity and personal information through digital wallets.

Digital wallets are applications that enable end users to manage their digital credentials and associated cryptographic keys. They allow holders to prove identity-related information about subjects by selectively disclosing attributes of the VCs in a privacy-preserving manner.

The concept of a digital wallet can be differentiated into two types: a simple Wallet and an Agent:

- A Wallet's primary function is to store keys, credentials, and secrets.
- An Agent, on the other hand, is software that manages access to a Wallet and other forms of storage, which may reside in various locations on a network (cloud vs. local). The role of an Agent is more complex, encompassing messaging or interactions with other agents within the decentralized ecosystem.

FinClusive remains agnostic to Wallet implementation to ensure compatibility with any wallet that adheres to the standard specifications outlined above. This approach enables support for wallets available on any registry where FinClusive's compliance credential schema is published.

In the future, FinClusive may explore the development of its own wallet tailored to specific use cases, including payments and other services. Additionally, FinClusive plans to expand its Agent implementation as DID and VC ecosystem evolves. This will facilitate a transition towards more self-sovereign applications of DIDs and VCs.

Conclusion

The implementation of Decentralized Identifiers (DIDs) and Compliance-backed Verifiable Credentials (CVCs) offer transformative benefits that are applicable to the financial services industry and beyond, enhancing security, privacy, and inclusivity globally.

Firstly, DIDs and CVCs facilitate a more secure and user-controlled digital identity verification process. This not only empowers individuals by granting them control over their personal data but also significantly reduces the risks of data breaches and identity theft across industries. For businesses, this translates into robust anti-money laundering (AML) and financial crimes compliance (FCC) frameworks, which streamline operations and save money by mitigating the costly impacts of financial crimes.

Secondly, the universal adoption of these technologies greatly enhances financial inclusion, allowing not just financial institutions but also sectors such as healthcare, education, supply and vendor-value chains, and e-commerce to verify identities easily and securely. This broader applicability promotes economic growth and stability, particularly in regions where traditional services are scarce or absent.

Furthermore, the interoperability provided by global standards for DIDs and CVCs ensures that as diverse new platforms and technologies emerge, they can seamlessly integrate into existing digital ecosystems across all industries. This not only boosts efficiency but also spurs innovation, fostering new business models and service offerings that can thrive within a secure, compliant framework.

In conclusion, while FinClusive spearheads the adoption of DIDs and CVCs within the financial sector, the broader implementation of these identity solutions promises a future where all sectors are more interconnected, transparent, and secure. With enhanced security measures, increased privacy, and streamlined processes, these technologies are poised to save businesses substantial resources while extending their benefits across the global economy, making financial and other services more accessible and trustworthy.

About FinClusive

FinClusive is a global Compliance-as-a-Service (CaaS) infrastructure provider that enables increased financial engagement by facilitating traditional banking's connectivity with emerging technology networks, existing and alternative payment rails, and financial services providers. FinClusive does this primarily by providing a global, full-stack, financial crimes compliance/anti-money laundering (FCC/AML)—Compliance as a Service (CaaS). This globally orchestrated platform brings together numerous best-in-class third party providers, 100s of global data/watchlist/screening and advanced analytics tools, basic to enhanced due diligence providers covering over 170 countries, combined with proprietary client and transaction monitoring rules and tools into a single workflow.

CaaS provides enhanced know your customer/know your business (KYC/KYB) tooling by embedding digitally verifiable compliance-backed identity credentials into both the customer onboarding and transacting processes and automates client verification and monitoring which is interoperable between traditional banking and payments providers and alternative, peer-to-peer, blockchain/web3-based networks. Further, CaaS Gateway Services create a Compliance-Enabled Credentialing Environment (CECE™), whereby traditional and decentralized banking and payment partners can confidently demonstrate compliance with global banking standards and expand their services to businesses, communities and alternative technologies that have been traditionally underserved or unwelcomed within in the global financial system.

For more information, please visit https://www.finclusive.com or contact press@finclusive.com. Follow us on X @FinClusiveCap and LinkedIn.