1. Executive Summary

Securitize is the leading digital asset securities company. As a FINRA member Broker-Dealer and the first SEC-registered Transfer Agent operating with digital asset securities, Securitize is one of the most regulated firms in the entire digital assets industry.

Securitize has an excellent track record for providing comprehensive compliance services to a vast array of digital assets companies. Our proprietary investor passport, Securitize iD, is globally recognized and built upon Securitize's battle-tested KYC/KYB/AML/CFT compliance program, allowing Securitize iD to be trusted by almost 400K registered investors and over 200 issuers to date.

Securitize is backed by top investors from both traditional and digital finance; our backers include blue-chip financial institutions like Morgan Stanley, Banco Santander, MUFG and Nomura Securities, as well as the leading digital asset and blockchain investors, such as Blockchain Capital, Coinbase Ventures, Ripple, Borderless Capital, Blockchain.com Ventures, Ava Labs, Kenetic and Fenbushi. We are bringing together traditional and digital asset stakeholders from across the globe.

Securitize asks the Aave Governance community to appoint Securitize as a whitelister for one of more deployments of Aave Arc based on the following criteria:

- Highly regulated entity with years of digital assets compliance experience.
- Existing Securitize iD product already provides KYC/KYB/AML/CFT services to almost 400K investors through Ethereum, Avalanche and Algorand wallet integrations, with Polygon coming soon.
- Distributed version of Securitize iD based on blockchain attestations was created to preserve the decentralized nature and integrity of DeFi protocols.
- Full satisfaction of whitelister requirements set forth in the Aave Arc white paper.
- Securitize iD Intro and Description

Securitize is renowned for pioneering the issuance, management and trading of digital asset securities using its robust business ecosystem, consisting of an SEC-registered Transfer Agent (TA), FINRA member Broker-Dealer (BD), Alternative Trading System (ATS) operator, Investment Advisor acting as an Alternative Asset Manager (AAM) and its proprietary investor passport, Securitize iD, which securely facilitates digital identity services for both individuals and institutions worldwide.

Launched in late 2019, Securitize iD quickly became the preferred mechanism for providing digital asset securities issuers and investors with Know Your Customer (KYC), Know Your Business (KYB), Anti-Money Laundering (AML), Countering Financing of Terrorism (CFT), and other compliance services, and has since then grown 30X to almost 400K registered users. With Securitize iD, verified user wallets can participate freely in online activities using digital assets, which will help digital asset communities like Aave achieve regulatory compliance so that they can focus on matters closer to their core mission.

Some distinct benefits of Securitize iD include:

- Fast and Unique Verification:

Securitize iD allows users to complete identity verification in a one-time process that can be carried out in minutes. They can then reuse their identity, ensuring consistency in their records and user satisfaction.

- KYC for Individuals:

Securitize iD supports a high-grade investor KYC which includes selfie identity and government-issued photo identification (ID).

- Entity KYB:

Securitize iD supports verification of businesses, complying with all the requirements of Knowing Your Business, including but not limited to, ultimate beneficial owners, organization incorporation documents, and KYC of legal signers.

- API First:

Securitize iD can connect with any platform to integrate a KYC/KYB verification flow easily with any business's current processes.

- Ongoing Monitoring - Nightly Screening:

A nightly screening is conducted on all users that have been onboarded through Securitize iD. Users are screened against various domestic and foreign government sanction watchlists, including OFAC, European Union, Interpol, and more.

- Ongoing Monitoring - Documentation Review:

Securitize iD keeps the user's documentation valid and up to date by automatically prompting users to upload a new government-issued photo ID, should it expire.

Similar to Aave, the number of Securitize iD users has increased exponentially since the beginning of 2020.

Securitize iD has already been used by over 200 issuers of digital asset securities; two notable Securitize iD client integrations, Exodus and Centrifuge, are representative of Securitize's ongoing collaborations with digital asset companies and DeFi providers.

On May 5, 2021, Exodus, a company that allows its users to secure, manage and exchange digital assets in a single wallet, successfully raised $75 million with the first fully tokenized equity offering for a Reg A+ security. Securitize helped enable this groundbreaking offering by acting as Exodus' digital blockchain-based transfer agent, a function underpinned by Securitize iD. Securitize iD was also used to collect the required investor information and perform compliance checks.

Through Securitize's application program interfaces (APIs), Securitize iD was fully integrated with Exodus' wallet software to create investor profiles for the Reg A+ offering, as shown in the following screenshot from Exodus' "Exodus Shares App tutorial" video on YouTube.

In a press release discussing the historic digital assets offering, Exodus went as far as to tell investors that their Securitize iDs would "be essential to the future availability of Exodus shares." Securitize iD also proved an essential integration for Centrifuge's Tinlake pools, creating a so-called "hybrid finance (HyFi) solution."

Centrifuge Inc., a Berlin-based fintech company, is unlocking DeFi liquidity for real world assets with Centrifuge network's investment application, Tinlake, which functions as a pool-based marketplace online. Special purpose vehicles (SPVs) are legally structured behind most Tinlake pools and pool investments are usually classified as private placements with regulators. Since private placements have regulatory requirements, Centrifuge hired Securitize for investor accreditation, onboarding, compliance checks, and subscription document signing, all of which were facilitated using Securitize iD.

The following graphic from Centrifuge's 'Onboarding Guide" documentation illustrates the investor onboarding flow for Tinlake pools.

Securitize iD is clearly a critical component of Tinlake's automated KYC and SubDoc signing process.

Exodus and Centrifuge are just two of many Securitize iD client integrations to date, with more in the pipeline. Borrowing from business author Jim Collins' "Flywheel Concept," the refinement of Securitize's compliance services and blockchain technology these past several years made Securitize iD rapidly scalable, easily adaptable and highly configurable.

With almost 400K KYC'd users to date, the Securitize iD "flywheel" is now spinning toward DeFi communities like Aave with Securitize iD for DeFi.

1. Blockchain Attestation and Integration with DeFi Protocols

Securitize acknowledges the need for creating an ID system that bonds well with the mechanics and ethos of DeFi protocols, while also providing the compliance services necessary to meet requirements of existing and future regulations.

Innovators are working toward the definition and implementation of a global on-chain identity registry. Most notable are the efforts of organizations like the Decentralized Identity Foundation (DIF) and the World Wide Web Consortium (W3C), standardization proposals such as the Ethereum Network's ERC725-Identity and ERC735-Claims, and countless products and services offered by businesses in the private sector.

A true global on-chain identity registry must be standardized and openly accessible through the internet, which prevents the siloing of identity information. Unfortunately, a viable global implementation doesn't exist at this moment in time and likely won't until well into the future; current on-chain proposals and products only lead to the creation of more identity silos veiled by the term "decentralized."

Securitize believes that a two-part approach is most ideal. We plan to work closely with the relevant organizations and technology leaders to contribute to the future creation of a global on-chain identity registry. However, we recognize that this will be a collaborative effort over the long term that requires further development of Web3. In the meantime, we created Securitize iD for DeFi, which consists of an extremely simple mechanism for bringing validated digital identities to the DeFi ecosystem.

When designing Securitize iD for DeFi, we sought to:

- Make it easy for external entities and their customers to use.
- Minimize the economic burden of transacting with complex and data-intensive on-chain processes on the distributed ledger (e.g., Ethereum Gas Fees).
- Protect user data and preserve their privacy.
- Provide DeFi protocols with on-chain validation for users' KYC/KYB, accreditation, and qualification status, among other inputs from external validators, such as Securitize's compliance services.

Securitize iD for DeFi will provide many useful lessons — from a technical, business and user experience perspective — for the digital assets industry to draw upon. If adopted by permissioned/whitelisted versions of DeFi deployments, like Aave Arc, Securitize iD for DeFi can serve as an important piece to the globally decentralized identity infrastructure of Web3 tomorrow.

The following diagram is a general overview of participants, technologies and interactions that will occur when whitelisting Aave Arc's users with Securitize iD for DeFi.

After logging into their wallet, Aave Arc users will create a Securitize iD, which requires following a simple 5 step KYC process.

Securitize's (DSGlobalInvestorRegistryService) smart contract manages the additions of whitelisted Aave Arc users and provides the mechanisms for interacting with Aave Arc deployments.

On-Chain Attestation

After an Aave Arc user has been KYC'd, their wallet and Securitize iD account are linked; an on-chain attestation, which is based on the user's public wallet address, will then be issued.

Aave Arc users will subsequently be able to:

- View their on-chain attestations with Securitize iD (https://id.securitize.io)
- Remove the attestation, by invoking the RemoveClaim method

Signing into Aave Arc

Once an Aave Arc user has an on-chain attestation, their Ethereum wallet address will be granted distinct permissions (e.g., supply, borrow, liquidate) to transact on Aave Arc.

Users can interact with Aave Arc via web sign-in and on-chain validation from smart contracts.

Web Sign-in

Users can access Aave Arc with their public wallet address through a Web3 gateway, such as MetaMask.

1. In this example scenario, users can access Aave Arc via MetaMask, and Aave Arc would check the user's public wallet address.
2. With this public address, Aave Arc can connect to Securitize's (DSGlobalInvestorRegistryService) smart contract to confirm that the user has been whitelisted by Securitize.

Thus Securitize iD for DeFi is interoperable. Once a user's wallet has been KYC'd by Securitize, the same wallet can be used with any other protocol or application that integrates with our on-chain attestation model; users do not need to go through the KYC process again, facilitating the necessary network effects for a compliant and feature-rich DeFi ecosystem.

1. Full Satisfaction of Aave Arc's Whitelister Requirements

Aave Arc is an attempt at easing institutional and regulatory concerns surrounding DeFi. Specifically, Aave hopes that Aave Arc can help institutions, a risk-conscious but DeFi curious group, become comfortable enough from a compliance standpoint to start using DeFi applications and services en masse.

Aave's Founder, Stani Kulechov, previously elaborated on this vision, stating "I think the larger vision of the Aave Arc market is to create a more comfortable risk appetite for institutions to participate in decentralized finance before, for example, having the risk appetite to participate towards the permissionless decentralized finance, which is the bigger vision offering."

So, how can Aave Arc help make Kulechov's institutional DeFi dream a reality?

When designing Aave Arc, additional smart contracts were added to the underlying software of Aave Protocol V2 to enable whitelisting functionality for a permissioned blockchain environment. Since Aave Arc is derived from the same software as Aave Protocol V2, Aave Arc's users can engage in transactions similar to those offered on the permissionless version.

The distinction lies in Aave Arc's whitelisting requirement, a process that all users must undergo — passing KYC/KYB checks, being onboarded in line with suitable disclosures, terms and prerequisites, and having their Ethereum wallet address(es) granted distinct permissions (e.g., supply, borrow, liquidate) — before being able to participate in network activities. Moreover, Aave Arc transactions are subject to AML/CFT screening and monitoring. These compliance processes and procedures are all carried out by an appointed whitelister.

As outlined in the Aave Arc white paper, whitelisters are also responsible for:

- Maintaining KYC and customer due diligence documentation for such users to ensure continued compliance;

- Conducting any other necessary compliance checks as required by (i) the jurisdiction for a particular deployment of Aave Arc or (ii) the standard operating procedures that whitelisters employ; and
- Ensuring that any deployment of Aave Arc has AML/CFT and other regulatory and compliance standards applied, including KYC requirements to permit users to engage in transactions on the protocol.

Whitelisters are ultimately in charge of determining the particular terms and conditions of service needed for users to be successfully whitelisted, onboarded, and eventually granted permission to act as suppliers, borrowers and/or liquidators on Aave Arc.

Only certain entities will meet the criteria necessary to be selected as a whitelister to deployments of Aave Arc by Aave Governance.

According to the Aave Arc white paper, a whitelister needs to be a regulated entity that:

1. Employs KYC/KYB principles in accordance with FATF guidelines to identify and accept their clients;
2. Has robust AML/CFT compliance programs; and
3. Is currently in good standing with an active license/registration in the entity's operating jurisdiction

Securitize satisfies all criteria necessary to be appointed as a whitelister, namely:

- We are a highly regulated entity, with a FINRA member Broker-Dealer and the first SEC-registered Transfer Agent operating with digital asset securities.
- Our KYC/KYB processes and procedures adhere to FATF guidelines, which is a requirement for conducting our existing digital asset securities business.
- We have a diversified team of experienced financial and technology professionals that allow Securitize to readily review, adopt, and deploy platform changes as the regulatory landscape shifts.
- Securitize iD already provides KYC/KYB/AML/CFT to almost 400K investors.
- Due Diligence is performed as part of the initial user onboarding process and continued via on-going monitoring designed to capture event driven red flags.
- Certified trace examiners conduct our wallet whitelisting and on-going monitoring procedures.
- A nightly screening is conducted on all Securitize iD users. Screenings are done against over 100 watchlists, including FinCEN, OFAC and PEP.
- Jurisdictional controls help to manage compliance with international regulations.
- Verification of individuals and in the case of legal entities, their legal signers and beneficial owner(s).
- Securitize and its affiliates are subject to assessments and examinations by independent auditors and regulatory bodies; the company policies that govern cybersecurity, the handling of personally identifiable information, and internal controls are tested annually to certify competence.

Written Supervisory Procedures

Securitize has developed "Written Supervisory Procedures" reasonably designed to ensure compliance with the highest standards and the applicable regulation. These procedures define the components that make up our compliance program. Such components in-take, review, and verify investor information, serving as a baseline to ensure we apply a rules-based approach to our business decisions.

KYC/AML Policy

Securitize's KYC/AML Policy is discussed below.

Initial Account Creation - The applicant must provide his or her first and last name, email address and country (or state) of residence. Upon providing the country of residence, the applicant will be presented with and must agree to country-specific terms and conditions, forward-looking statement disclaimer, acknowledge risk factors, etc.

Registration Email / Email Confirmation - Upon entering the information provided above, the applicant is sent an automatic email to the email address they provided. Next, the applicant is required to verify the email address and is then directed back to the issuer's site. The applicant is provided with a link that directs the applicant to the Company's privacy policy and terms of service, which the investor must review and click to agree.

(1) Investor Information

Applicant Personally-Identifiable Information - Investors are then prompted to upload their identification, i.e., driver's license

or passport, which auto-populates most of the fields needed to complete KYC. The account holder will select whether to invest as an individual or entity. They also must provide their tax identification number.

Securitize uses documentation validation to verify the investor's identity and watchlist, database and adverse media screening inclusive of OFAC, PEP (see below for PEP definition) and other various foreign and domestic government watchlists as well as social security number verification for US applicants.

Securitize uses a third-party service provider to verify social security numbers input by US applicants. SSN mismatch, PO Box address input and any nexus to fraud per the name, email, DOB and SSN input by the US applicant is reviewed as part of the validation process. The Company uses a third-party service provider to screen investors against various foreign and domestic government watchlists, databases and open-source media for adverse information and to verify the investor identity. This serves as an identity verification tool that validates government-issued photo IDs and conducts a liveness test by having the investor move their face as prompted.

Biometric scanning is used to compare the facial image of an account holder's face ("Selfies" taken from the liveness test) with the photo in the government-issued photo ID to confirm if the two faces are the same individuals. The government-issued photo ID is reviewed for potential fraud and validity.

In addition to identity verification, the third-party platform provides watchlist and adverse media screening. Our process includes screening investors against a large variety of domestic and foreign government watchlists, government databases and scrubs the internet for adverse information. A PEP is a natural person or close relative thereof, that holds a senior, prominent and or important position, with substantial authority over policy, operations or the use or allocation of government-owned resources.

Some examples of PEPs are:

1. Heads of State, heads of government and ministers
2. Senior judicial officials who sit on bodies whose decisions are not subject to further appeal
3. Heads and other high-ranking officers holding senior positions in the armed forces
4. Members of ruling royal families with governing responsibilities
5. Senior executives of state-owned enterprises, where the state-owned enterprise has genuine economic or political importance
6. Senior officials of major political parties
7. Mayors of cities with a population of one million people or more

For individuals' applications, the individual must provide the above-aforementioned information in addition to the following documentation:

- Government-issued photo IDs
- Must not be expired and the name, facial image and ID number must be clear and visible.
- Screenshots of a government-issued photo ID are not acceptable.
- Acceptable forms of government-issued photo ID include a passport, U.S. driver's license or ID card for all U.S. citizens.
- Must not be expired and the name, facial image and ID number must be clear and visible.
- Screenshots of a government-issued photo ID are not acceptable.
- Acceptable forms of government-issued photo ID include a passport, U.S. driver's license or ID card for all U.S. citizens.
- A passport or national ID card from members of the European Union or Japan.
- Passports for all other foreign nationals.

In an attempt to keep all IDs up to date, the investor will be automatically prompted via email to re-upload a valid government-issued photo ID when their ID on file expires.

(2) Liveness

The applicant is prompted to complete a "liveness test" by moving their face as prompted in a circle on the screen. The technology takes screenshots from the video and uses this to review the face against the Identification document used during onboarding. Both the applicant's face and ID must be clear and visible.

(3) SSN Check

For U.S. investors, Securitize uses a third-party vendor to verify the applicant's SSN and to check against any applicant input addresses including a PO Box. Additionally, the third-party vendor checks against any potential nexus to fraud.

After the documentation is provided through the Securitize iD portal, the information will be sent via an API. The Director of Compliance or Director of Compliance's designee will review the control panel daily to review any potential findings that have been identified. The Director of Compliance or the Director of Compliance's designee will either mitigate the findings and approve the applicant, request additional information, or reject the applicant. All documentation is retained for a minimum of 5 years in accordance with Bank Secrecy Act standards. Applicants may request to delete their information in accordance with General Data Protection Regulation. This will be handled on a case-by-case basis by the Director of Operations. The Director of Operations may grant exceptions to the above requirements on a case-by-case basis.

Possible outcomes from the review are but are not limited to:

1. Approve
2. Request Additional Information (ex. ID is blurry or liveness failed)
3. False Positive-Approve (Name mismatch, age mismatch, region mismatch. etc.)
4. Confirm but Mitigate (ex. Investor was charged with fraud 10 years ago)
5. Confirm and reject. (ex. The investor was identified on a government watchlist)

NOTE: Only Legal, Compliance and specific employees on a need-to-use basis will have access to the Securitize iD Onboarding Platform ("SiD Onboarding Platform").

The Director of Compliance will only grant SiD Onboarding Platform access to employees who:

1. Have been fingerprinted in accordance 17f-2(a)(1)(ii) (See Procedure ID: 4.0 - Fingerprinting Procedures) and;
2. Have a legitimate business use case for the SID Onboarding Platform.

Access to the SiD Onboarding Platform provides the following:

1. Ability to approve or reject investors
2. Ability to read and write compliance notes on the investor's account
3. Ability to view KYC reports and documents submitted by the investor

Securitize takes reasonable and prudent steps to combat money laundering and terrorist financing and minimize our exposure to the risk associated with such activities.

As part of a robust AML compliance program, Securitize seeks to ensure that its policies and procedures identify suspicious transactions. Our supervisory processes assess whether the account holder has engaged in activities deemed to be outside the scope of ordinary trading or sensible financial decision-making. Securitize has the regulatory responsibility to report suspicious activity and provide sufficient detail in reports to law enforcement agencies to make the reports helpful in investigating reported suspicious transactions.

Securitize has developed, implemented, and maintained effective AML programs that address the ever-changing strategies of money launderers. Our compliance program is critical in deterring and preventing these types of activities. Money laundering and criminal activity can exploit loopholes and other weaknesses in our markets to launder criminal proceeds, finance terrorism, or conduct other illegal activities, and, ultimately, hide the actual purpose of their activity, so hypervigilance and strong internal controls are critical to preventing bad actors access to legitimate institutions.

Securitize is required to comply with Office of Foreign Asset Control ("OFAC") sanctions programs. OFAC is the arm of the U.S. Department of the Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction and other threats to the national security, foreign policy, or economy of the United States. OFAC acts under Presidential national emergency powers and authority granted by specific statutes to impose controls on transactions and freeze assets under U.S. jurisdiction. U.S. persons must comply with OFAC regulations, including all persons and entities within the United States and all U.S. incorporated entities.

The aforementioned policies and procedures are foundational to Securitize's battle-tested KYC/KYB/AML/CFT compliance program. Securitize iD for DeFi brings the benefits of our compliance services onto the blockchain. Therefore, Securitize iD for DeFi offers Aave Arc a novel approach to digital asset compliance and its on-chain attestation system aligns closely with the current usage and ethos of DeFi.

1. Conclusion

As outlined in detail throughout the proposal, Securitize clearly satisfies all criteria necessary to be appointed as a whitelister for Aave Arc.

Therefore, once elected, Securitize will:

- Maintain KYC and customer due diligence documentation for such Aave Arc users to ensure continued compliance;
- Conduct any other necessary compliance checks as required by (i) the jurisdiction for a particular deployment of Aave Arc; or (ii) the standard operating procedures that whitelisters employ; and
- Ensure that the deployment of Aave Arc that we are responsible for has AML/CFT and other regulatory and compliance standards applied, including KYC requirements to permit users to engage in transactions on the protocol.

Securitize recognizes that other whitelisters will participate in Aave Arc deployments. We plan to engage in discussions with said whitelisters to figure out the best alignment for increasing Aave Arc pool liquidity.

Securitize thanks the Aave community for the opportunity to submit this governance proposal. We look forward to your decision and are available to answer any questions or comments related to Securitize, Securitize iD and/or Securitize iD for DeFi.