Add Fireblocks as a whitelister on Aave Arc

Summary

Fireblocks asks the Aave Governance community to approve the appointment, adoption, and authorization of Fireblocks LLC, a Fireblocks company, as a “whitelister” for one or more deployments of Aave Arc.

Proposal

Fireblocks is on a mission to bring more institutional participants into DeFi.

Today, Fireblocks serves more than 600 customers and has secured over $1.25 trillion in digital assets. Fireblocks’ technology has become trusted by the leading institutional crypto players and the world’s biggest banks to secure digital assets, develop new yield generating strategies, and improve capital efficiency. As the initial whitelisting partner for Aave Arc, Fireblocks can offer institutions the same secure and scalable rails used to transfer and store digital assets to access permissioned DeFi environments.

DeFi is considered by institutional users to be one of the more complex markets to navigate across security, compliance, and risk perspectives. We are eager to be at the forefront of this transformational opportunity with Aave Arc by extending access to even our most compliance-conscious customers, who would otherwise avoid DeFi over compliance or regulatory concerns.

Fireblocks’ R&D, compliance, and legal teams have developed a new whitelister framework for permissioned DeFi. This framework meets both enterprise-grade requirements for accessing DeFi and adheres to Aave Arc’s whitelister governance criteria. This deployment will set the precedent for new organizations joining Aave Arc, simplify the process for onboarding new whitelisters, and ensure everyone is following best practices defined by the whitelister community.

Detailed Description of Proposal

Aave Arc is a “permissioned” version of the software underlying V2 of the Aave protocol that employs an additional smart contract layer to only allow “whitelisted” or “permissioned” users to engage with the protocol.

Each Aave Arc deployment will launch with one or more “whitelister.” Only regulated entities that (a) employ KYC/KYB principles in accordance with FATF guidelines to identify and accept their clients; (b) have robust AML/CFT compliance programs; and (c) are currently in good standing with an active license/registration in the entity’s operating jurisdiction will be accepted as “whitelisters” on deployments of the Aave Arc.

“Whitelisting” is the gatekeeping function performed by whitelisters on users of Aave Arc. The term refers specifically to the process of:

- Conducting KYC/KYB checks on the user;
- Onboarding the user with appropriate disclosures, terms, and conditions; and,
- Granting specific permissions (e.g., borrow, supply, liquidate) to the Ethereum wallet address(es) provided by the user.

Aave Arc whitelisters are granted “guardian” status like the Aave protocol V2 guardian role with the ability to collectively, make and enforce decisions around gatekeeping parameters. This will enable whitelisters to establish and revise, as necessary, whitelisting standards for deployments of Aave Arc to ensure that they remain current with regulatory requirements and the needs of users.

Approving one or more whitelisters is a crucial step towards establishing a permissioned deployment of the Aave protocol that meets the requirements of institutional users that may be otherwise unable to participate in the Aave protocol. The Aave arc community is being asked to evaluate and vote on whether Fireblocks LLC should be approved as such a whitelister and begin the process of whitelisting users of an Aave Arc deployment.

We believe that Fireblocks LLC, a Fireblocks company, satisfies all the qualification requirements to be a whitelister. We have performed a detailed analysis and documented it here for the consideration of the Aave Governance community.

Approval of Fireblocks LLC can potentially also facilitate the integration of other “whitelisters” and institutions into instances of the Aave protocol. This may have multiple benefits, including the creation of sustainable governance practices for Aave Arc whitelisters and whitelister customers, as well as the enablement of benefits to the ecosystem, such as the onboarding of regulated fiat on/off ramps and protocol deployments connected to debit cards, high yield savings accounts and other innovative fintech products.

Next Steps

Aave Governance community to vote YES/NO for the appointment and authorization of a Fireblocks company to the role of “whitelister” in one or more permissioned deployments of the Aave protocol.

Deployment of the Aave protocol and the commencement of onboarding institutional users through the “whitelisting” process adopted by approved whitelisters.

Fireblocks: Qualifications to be a Whitelister

Requirements of a Whitelister:

Only regulated entities that (a) employ KYC/KYB principles in accordance with FATF guidelines to identify and accept their clients; (b) have robust AML/CFT compliance programs; and (c) are currently in good standing with an active license/registration in the entity's operating jurisdiction will be accepted as "whitelisters" on deployments of the Aave Arc.

Fireblocks LLC is qualified to be a whitelister for Aave Arc because: (a) a licensed/registered entity in its operating jurisdiction; (b) subject to KYC/KYB principles in accordance with FATF guidelines; and (c) required to adopt, and has adopted, a robust AML/CFT compliance program. This section progresses by addressing each required elements in turn and concludes that Fireblocks LLC is qualified to perform the services of a whitelister.

Fireblocks LLC is a registered "money services business" in good standing with FinCEN and licensed to offer money transmission services in one or more of the 50 United States.

Fireblocks LLC, a Delaware limited liability company, (the "Company") was formed in October 2020 for the purpose of providing certain money transmission services in conjunction with, and as a complement to, the "software as a service" ("SaaS") business operated by the Company's direct and indirect owners, Fireblocks, Inc. and Fireblocks Ltd., respectively. On April 13, 2021, Fireblocks LLC registered as a "money services business" ("MSB") with the Financial Crimes Enforcement Network ("FinCEN"), the U.S. federal regulatory agency responsible for administering and enforcing U.S. anti-money laundering ("AML") and counter financing of terrorism ("CFT") laws for "financial institutions," a category that includes MSB. The Company's MSB registration is in good standing (registration #31000187180862

), and Company will maintain that registration in accordance with 31 CFR 1022.380 renewal requirements at the end of every two (2) years.

In addition to the foregoing, various U.S. jurisdictions require licensure for the Company to offer certain services, often under applicable "money transmitter" statutes. Fireblocks LLC has obtained, and is in the process of obtaining, state Money Transmission Licenses ("MTLs"), as required by each state statute based on the activity the Company intends to conduct (if any) in each state (NMLS ID: 2066055). The Company's plans for pursuing MTLs vary by jurisdiction and are subject to change. Please refer to FinCEN's MSB registry for additional information on the MTL activities of Fireblocks LLC.

Fireblocks LLC is subject to KYC/KYB principles that are in accordance with FATF guidelines.

- Fireblocks LLC is subject to KYC/KYB Principles

The Bank Secrecy Act ("BSA") is the cornerstone of the United States' money laundering control system. The USA PATRIOT Act amended the BSA by strengthening its AML and CFT monitoring requirements for financial institutions. As amended, the BSA requires, among other things, that financial institutions implement a risk-based compliance program with at least the following four components: (1) designation of a responsible person; (2) development and adoption of internal policies, procedures and controls, including "know your customer" ("KYC") / "know your business" ("KYB") identification requirements; (3) training of relevant employees; and, (4) independent testing to review of the efficacy of the compliance program.

FinCEN administers the BSA and issues and enforces compliance program regulations for financial institutions, including MSBs. On May 11, 2016, FinCEN published its final Customer Due Diligence requirements (the "CDD Rule") and amended the Bank Secrecy Act regulations to clarify and strengthen customer due diligence requirements for covered financial institutions. The CDD Rule imposed explicit ongoing customer due diligence and monitoring requirements and introduced a new requirement for financial institutions to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. Arguably, the CDD Rule amounted to the addition of a fifth compliance program requirement in the form of risk-based procedures for conducting ongoing customer due diligence in addition to point-in-time diligence at onboarding.

In addition to federal and state CFT/AML regulations, the Company 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, as well as 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 KYC/KYB Principles to which Fireblocks LLC is Subject are FATF Compliant

The United States is one of 39 countries that are members of the Financial Action Task Force ("FATF"). FATF is an inter-governmental body that sets international standards to prevent money laundering and terrorist financing. As a member country, the United States is part of a core group committed to the dissemination of global standards on AML/CFT best practices ("FATF Recommendations") and their implementation through legislative and regulatory reform. In addition to setting standards, FATF monitors countries to ensure that they implement FATF Recommendations fully and effectively and holds countries that do not comply to account.

In FATF's most recent evaluation report on the United States, adopted in March 2020, FATF favorably noted FinCEN's adoption of the CDD Rule, including its requirements for legal entity beneficial owner verification and ongoing customer due diligence and monitoring. In recognition of the United States' progress in strengthening its measures to fight money laundering and terrorist financing, FATF upgraded their rating of the United States' KYC/KYB standards for identifying customers. In sum, FATF rated the United States as compliant, largely complaint, or partially compliant with 36 out of 40 FATF Recommendations. In its August 11, 2021, consolidated assessment of ratings, FATF evaluated the United States as being moderately to highly effective at combating money laundering and terrorism financing in 10 of 11 assessment categories.

Fireblocks LLC has a robust AML/CFT compliance program.

Fireblocks LLC has implemented a robust compliance program with policies and procedures that are risk-based and reasonably designed to comply with Fireblocks' obligations under the U.S. anti-money laundering statutes as well as applicable sanctions programs. The formal compliance program adopted by the Company consists of five key components: (1) the appointment of a qualified BSA/AML Officer; (2) written compliance policies and procedures, including an AML program manual and risk assessment; (3) external audit and internal testing; (4) a risk-based customer identification and due diligence program; and (5) training appropriate to each employee, officer, and director (the "Compliance Program"). All potential Fireblocks LLC account holders are required to meet or exceed the minimum requirements of the Compliance Program at account opening and on an ongoing basis to access services provided by Fireblocks LLC.

- Appointment of a Qualified BSA/AML Officer

Fireblocks LLC appointed Peter Singer as the BSA/AML Officer for the Company. Prior to joining the Company, Mr. Singer served in multiple senior and executive compliance roles, including as Chief Compliance Officer, in the cryptocurrency, payments, and fintech industries. In these roles, Mr. Singer was responsible for ensuring that these companies adhered to state and federal regulations for MSBs and implemented strong controls to prevent fraud and financial crimes. Mr. Singer holds the Certified Anti Money Laundering Specialist certification (CAMS) and the Certified Fraud Examiner (CFE) designation.

- Written Compliance Policies and Procedures

Fireblocks LLC has adopted a comprehensive Compliance Program in writing. The written Compliance Program is commensurate with the nature and volume of services provided by the Company and incorporates policies, procedures and internal controls reasonably designed to assure compliance with applicable law, including procedures for:

- Collecting and verifying customer identity, including for legal entity customers and their beneficial owners;
- Performing enhanced due diligence and ongoing monitoring;
- PEP screening;
- Monitoring for suspicious activity;
- Filing reports, including reports of suspicious activity and unresolved "red flags";
- Creating and retaining records;
- Training of appropriate personnel;
- Sanctions screening; and
- Responding to law enforcement requests.

The BSA/AML Officer is responsible for ensuring that the Compliance Program is updated as frequently as necessary to reflect the requirements of law, regulation, and guidance and, in any event, that it is re-evaluated at least once annually in connection with the Company's risk assessment process.

- External Audit and Internal Testing

The Company is required to perform an independent review of the Compliance Program to assess its adequacy. The Company will engage a qualified individual or firm to complete such a review no later than the first anniversary of its registration as a MSB, as is commensurate with the risk of the services it offers.

- Risk-Based Customer Identification and Due Diligence Program

As discussed above, the Company has adopted a written Compliance Program that includes, among other things, customer due diligence procedures that require the collection of information sufficient to verify the identity of the customer and, in the case of legal entities, their authorized representatives and beneficial owner(s). In cases where the initial diligence process uncovers "red flags," the Compliance Department is required to perform enhanced due diligence on the customer, which may include additional research or requests for information, or any other steps that the Compliance Department deems necessary. In addition to the diligence performed at account opening, all customers are subject to ongoing monitoring requirements, which may be event driven or periodic and, in any case, are determined and implemented on a risk basis.

Training

The BSA/AML Officer is responsible for ensuring the education and/or training of appropriate personnel concerning their responsibilities under the Compliance Program, including training in the detection of suspicious transactions. The BSA/AML Officer will conduct or will engage a qualified individual or firm to conduct, such trainings no later than the first anniversary of the Company's registration as an MSB.

Conclusion: Fireblocks LLC is Qualified to be a Whitelister for Aave Arc

Based on the foregoing, Fireblocks LLC is qualified to perform the following functions a whitelister for Aave Arc:

- Conducting initial KYC/KYB checks on any potential users of Aave Arc;
- Maintaining KYC and customer due diligence documentation for such users to ensure continued compliance; and
- 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.

Feel free to post here if you have any general questions or comments, and thank you for the consideration.