Eight Sharp Capital, LLC (“Qyon”) Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) Policy

UPDATED AS OF MAY 17, 2021

1. Firm Policy

It is Qyon’s policy to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by working with our financial software provider Sila Inc. (“Sila”) and banking partner(s) to comply with all applicable requirements under the Bank Secrecy Act (“BSA”), the USA PATRIOT Act (the “Patriot Act”), and their implementing regulations.

Money laundering means any activity that is meant to conceal or disguise the origins of criminally derived proceeds to appear to constitute legitimate assets. A criminal will typically achieve money laundering in three stages. At the "placement" stage, the criminal converts cash generated by illicit means into monetary instruments or deposits it into accounts maintained by otherwise legitimate businesses at financial institutions. At the "layering" stage, the criminal transfers or moves the funds into other accounts or other financial institutions to put greater distance between the money and its criminal origins. At the "integration" stage, the criminal reintroduces the funds into the economy, using them to purchase legitimate assets or fund other criminal activities or legitimate businesses.

Financial technology firms that process transactions for their customers are uniquely situated in an evolving technological, financial, and regulatory landscape. Such a firm must always anticipate that its customers or their counterparties could be attempting to launder funds obtained elsewhere or generate illicit funds on the financial technology platform itself, such as attempting to create an account using inaccurate information from people who do not authorize such act or even from people who do not exist.

Unlike money laundering, terrorist financing does not necessarily involve the proceeds of criminal conduct. The funding sources of terrorist financiers are often legitimate. Terrorist financing typically involves an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of terrorist financing can include charitable donations, foreign government sponsors, business ownership, and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can look similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

This Bank Secrecy Act and Anti-Money Laundering Policy ("BSA/AML Policy") and our procedures and internal controls for implementing the policy are designed to ensure compliance with all applicable laws and regulations. We will review and update this BSA/AML Policy on a regular basis and put in place appropriate procedures and internal controls to account for both regulatory changes and changes in our business.

2. Compliance Officer Designation and Duties

Qyon has designated Samuel Carvalho Gaudencio as its Compliance Officer, who is fully responsible for maintaining a program with procedures and internal controls appropriate to give effect to this BSA/AML Policy. Samuel Carvalho Gaudêncio has a working knowledge of the BSA, the Patriot Act, and their implementing regulations and is qualified by experience, knowledge, and training, being an attorney for over 15 years, and being Qyon's M&A, Tax and Compliance Officer in Brazil.

The Compliance Officer will be responsible for overseeing communication and training for employees and monitoring the firm's compliance with all obligations, including those directly applicable to this firm under the BSA and indirectly applicable through our banking partner. The Compliance Officer will also ensure the firm keeps and maintains all necessary transaction records and timely file both: notices of potentially suspicious transactions with Sila and our banking partners; and reports of currency received in a trade or business and Foreign Bank and Financial Accounts Reports ("FBARs") with the Financial Crimes Enforcement Network (FinCEN) when appropriate. The Compliance Officer is vested with full responsibility and authority to implement and enforce this BSA/AML Policy.

Qyon will provide Sila with the Compliance Officer's contact information, including his name, title, mailing address, email address, and phone number. Qyon will promptly notify Sila if there is any change to the Compliance Officer position, his contact information, or the BSA/AML Policy itself.

3. Giving AML Information to Financial Partners

We will respond to any demand made by our financial software provider Sila or our banking partner(s) pursuant to a FinCEN BSA § 314(a) request concerning accounts and transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in the demand. We will respond to any such demand within 3 business days unless otherwise specified by Sila or our banking partner(s). Demand should be made to the Compliance Officer at the contact information provided. Unless otherwise stated in the demand, we are required to search those documents outlined in FinCEN's FAQs. If we find a match, the Compliance Officer will report the match and all relevant documents to Sila or our banking partner (whomever made the demand).

If our Compliance Officer searches our records and does not find a matching account or transaction, he will indicate as such in response to Sila's or our banking partner's demand.

We will maintain documentation that we have performed the required search by the documents we are authorized by law to process and search of public records. The Compliance Officer will review, maintain, and implement procedures necessary to protect the security and confidentiality of demands for information made by Sila or our banking partner pursuant to a FinCEN BSA § 314(a) request similar to the procedures we use to protect our customers' nonpublic information.

4. Checking OFAC Listings

Before a customer opens an account, and on an ongoing basis, the Compliance Officer will check to ensure the customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. Since the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. The Compliance Officer will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and document the review.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and, if necessary, block the customer's assets and file a blocked assets or rejected transaction form with OFAC within 10 days. We will also immediately call the OFAC Hotline at 800-540-6322.

5. Customer Identification Program

Qyon has established, documented, and is committed to maintaining a written Customer Identification Program ("CIP"), which includes procedures for Know-Your-Customer/Business ("KYC/KYB") compliance. We will collect certain minimum customer identification information from every customer who opens an account on our platform. We will: apply risk-based measures to verify the identity of each customer who opens an account; record customer identification information and our verification methods and results; provide adequate CIP notice to customers stating why we need identification information to verify their identities; and compare customer identification information with the OFAC SDN List.

a. Required Customer Information

Before an individual or business customer opens an account for access to our platform, the Technology GRC (Governance, Risk and Compliance) Officer will collect the following information: full name, street address, phone number, and email address. If there is a mismatch involved with verifying the minimal information provided above or before the customer may be granted platform access to send or receive more than $299 a week in aggregate or maintain money balances, we will additionally collect the following information as required by law (if not already collected preliminarily):

(1) birthdate (for an individual); and
(2) an identification number or other documentary ID, which—
  (a) for a U.S. person, will be a taxpayer identification number ("TIN"); and
  (b) for a non-U.S. person, will be one or more of the following: a TIN, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

b. Customers Who Refuse to Provide Information

If a prospective or existing customer either refuses to provide the information described above when prompted or appears to have intentionally provided misleading information, Qyon will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our Compliance Officer will be notified so that we might consider notifying Sila and our banking partner(s).

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will form a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information provided. The Compliance Officer will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief as to the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means, or both. Qyon has developed a plataform to perform KYC/KYB verification, accessing public records, government agencies and public database. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means if we are still uncertain about whether we know the true identity of the customer.

To verify the identity of our customers by documentary means, we may request:
(1) for an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; or
(2) for a business entity or organization, documents evidencing its legal existence, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

While we may rely on a government-issued ID as verification of a customer's identity, we will consider any clear evidence of fraud in determining whether we can form a reasonable belief as to the customer's true identity.

We will use non-documentary methods of verification if: the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard; we are unfamiliar with the documents presented by the customer; we do not have face-to-face contact with the customer; or other circumstances indicate potential increased risks that we will be unable to verify the customer's true identify through documentary means.

To verify the identity of our customers by non-documentary means, we may:

(1) independently verify the customer's identity by comparing the information with information obtained from a consumer reporting agency, public database, or other source;
(2) check references with other financial institutions; or
(3) obtain a financial statement.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with our Compliance Officer, notify Sila and our banking partner.

We will also identify customers that pose a heightened risk of not being properly identified. We will take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient: obtaining information about beneficial ownership, individuals with authority or control over such account, requesting videochats or selfies with original government issued ids.

d. Verification Failure

When we cannot form a reasonable belief as to the true identity of a customer, we will: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify a customer's identity fail; and (4) determine whether it is necessary to necessary to notify Sila and our banking partner.

e. Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and results

of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

f. Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers: a pop up notice when the Customer opens the App

> **Important Information About Procedures for Opening a New Account**
> To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.
>
> **What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.**

6. Customer Due Diligence Procedures

Qyon has established, documented, and is committed to maintaining written Customer Due Diligence ("CDD") procedures, which are reasonably designed to identify and verify beneficial owners of our customers that are business entities or organizations. We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions to Sila and our banking partner, and, on a risk basis, maintain and update customer information.

At the time of opening an account for a legal entity customer, Compliance Officer will identify any individual that is a beneficial owner of the legal entity customer by identifying any individuals who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with significant responsibility to control, manage, or direct a legal entity customer. We will collect the following information for each beneficial owner:

(1) full name;
(2) birthdate (for an individual);
(3) street address; and
(4) an identification number or other documentary ID, which—
    (a) for a U.S. person, will be a taxpayer identification number ("TIN"); and
    (b) for a non-U.S. person, will be one or more of the following: a TIN, passport number and country of issuance, alien identification card number, or

number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

For verification, we will describe any document on which we relied and note the type, any identification number, place of issuance and, if any, date of issuance and expiration. We will also describe any non-documentary methods and the results of any measures undertaken.

Depending on the facts and circumstances, a customer risk profile may include such information as:

- The type of customer;
- The account or service being offered;
- The customer's income and net worth;
- The customer's domicile;
- The customer's principal occupation or business; and
- In the case of existing customers, the customer's history of activity.

7. Suspicious Transactions and BSA Reporting

a. Notifying Financial Partners of Suspicious Transactions

To help usher compliance with our banking partner's BSA obligations to file Suspicious Activity Reports ("SARs") with FinCEN, we will notify Sila and our banking partner(s) of any transactions (including deposits and transfers) that a customer conducts or attempts on our platform involving $5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect, or have reason to suspect the transaction:

(1) involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

(2) is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;

(3) has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or

(4) involves the use of our platform to facilitate criminal activity.

We will also notify Sila and our banking partner(s) in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. We will retain copies of any such notices we provide to Sila and our banking partner, along with any supporting documentation for five years from the notification date. We will not notify any person involved in the transaction that we have notified Sila and our banking partner(s) of the relevant transaction except as specifically permitted by BSA regulations.

b. Reports of Currency Received in a Trade or Business

If we have knowledge of a currency transaction or multiple currency transactions that, in aggregate, amount to more than $10,000 conducted by or on behalf of the same person during any one business day, the Compliance Officer is responsible for electronically filing a report with FinCEN on FinCEN/IRS Form 8300, pursuant to 31 C.F.R. § 1010.330.

c. Foreign Bank and Financial Accounts Reports

Our Compliance Officer is responsible for electronically filing a Foreign Bank and Financial Accounts Report ("FBAR") with FinCEN on FinCEN Form TD-F 90-22.1 for each foreign financial account aggregately valued at $10,000 at any point in the previous calendar year if we have an ownership interest in—or signatory authority over—the account pursuant to 31 C.F.R. § 1010.350.

8. BSA/AML Recordkeeping

Our Compliance Officer and his or her designee is fully responsible for ensuring our BSA/AML records are maintained properly. As part of this BSA/AML Policy, we will create and maintain notifications of suspicious activities made to Sila and our banking partner, reports of currency received in a trade or business, [*FBARs*], and all relevant documentation on customer identity, verification, and funds transmittals. We will maintain suspicious activity notices and accompanying documentation for at least five years. We will keep other documents according to existing BSA regulations and other recordkeeping requirements.

9. Training Programs

We will develop ongoing employee training under our Compliance Officer's leadership and in consultation with senior management. Our training will occur on at least an annual basis. It will be based on our size, customer base, and resources and be updated as necessary to reflect any new developments in the law. Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, notifying Sila and our banking partner of suspicious activity); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the persons trained, the dates of training and the subject matter of their training. We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

10. Evaluating BSA/AML Policy Programs and Procedures

Qyon has designated Technology GRC Officer, Jonathan Vita, to internally review and test our programs and procedures implemented under this BSA/AML Policy at least every two years. We may also identify a qualified third party to independently review and test our BSA/AML Policy programs and procedures if circumstances warrant. After we have completed internal review or independent testing, Technology GRC Officer will report the findings to audit committee. We will promptly address each of the resulting recommendations and keep a record of how any noted deficiency was resolved.

11. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts under the Compliance Officer's supervision. We will also review the AML performance of supervisors as part of their annual performance review. The Compliance Officer's own accounts will be reviewed by Mauricio Ferreira Frizzarin.

12. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of this BSA/AML Policy and the programs and procedures implemented thereunder to the Compliance Officer. If, however, the alleged violations implicate the Compliance Officer, the employee shall report to the audit committee chair. Such reports will be confidential, and the employee will suffer no retaliation for making them.

13. Senior Manager Approval

Senior management has approved this BSA/AML Policy in writing as reasonably designed to achieve and monitor Qyon's ongoing compliance with BSA requirements and to satisfy our conditions of partnership with Sila and our banking partner. This approval is indicated by signatures below.

DocuSigned by:

23DE3716AE764AD...

Signed: Mauricio Ferreira Frizzarin

Title: Manager

Date: May 17, 2015