Anti-Money Laundering Policy and Procedures

Effective: 05/01/2022

Table of Contents

1 The Paper Policy

This policy describes the Caves, Inc. (d/b/a "Paper") Bank Secrecy Act, Anti-Money Laundering, Office of Foreign Assets Control Compliance Program ("AML Program").

The AML Program seeks to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) as amended. The compliance goal of Paper is to protect its business from being used to facilitate money laundering, terrorist financing, and related crime to the extent reasonably possible.

Paper has conducted an initial risk assessment that considers the legal, compliance, financial and reputational risks associated with Paper's planned activities, services, customers, counterparties, and geographic location. It has established its AML Program based upon this initial risk assessment.

Paper's AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA requirements and will be reviewed and updated periodically to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in Paper's business. Paper is committed to ensuring compliance with BSA/AML and OFAC standards and ensures that AML compliance personnel are qualified and trained in mitigating money laundering risk.

It is Paper's policy to prohibit and actively prevent money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the BSA and its implementing regulations.

1 Money Laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds in a way to make those proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages.

1 Placement

Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.

2 Layering

At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

3 Integration

At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

2 Terrorist Financing

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include 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 be the same as or 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.

2 Background

1 Bank Secrecy Act

The BSA, also known as the Currency and Foreign Transactions Reporting Act, is legislation passed by the United States Congress in 1970 that requires U.S. financial institutions to collaborate with the U.S. government in cases of suspected money laundering and fraud.

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the United States Department of the Treasury that collects and analyzes information about financial transactions to combat domestic and international money laundering, terrorist financing, and other financial crime.

On October 26, 2001, the USA PATRIOT Act (the "Act") became law (amending certain provisions of the Bank Secrecy Act of 1970). Section 352 of the Act requires every "financial institution" to establish an AML program, which includes at a minimum:

- The development of internal policies, procedures, and controls
- The designation of a compliance officer
- An ongoing employee training program
- An independent audit function to test the program

Paper is a corporation organized under the laws of Delaware, which provides a frictionless checkout solution to end-users. Paper has adopted this AML Policy in collaboration with the financial institution opening the accounts. Paper has implemented the following controls to comply with the BSA and FinCEN regulatory requirements:

- Developed a written AML Program;
- Developed or outsourced to a third party vendor, policies, procedures, and internal controls reasonably designed to assure compliance including:
    - Verifying customer identification;
    - Detecting, preventing, and responding to fraud and attempted fraud;
    - Monitoring transactions for suspicious activity;
    - Designating a AML Compliance Officer to assure the day-to-day compliance with the AML Program;
    - Implementing a training program that requires initial and on-going training to appropriate personnel;
    - Responding to law enforcement requests;
    - Creating partnerships as allowed by law with other financial institutions, regulators, and law enforcement to facilitate information sharing; and
    - Facilitating a periodic independent review of the AML Program

3 Office of Foreign Assets Control

The Office of Foreign Assets Control (OFAC) is a financial intelligence and enforcement agency of the U.S. Treasury Department. It administers and enforces economic and trade sanctions in support of U.S. national security and foreign policy objectives. As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country specific. Collectively, such individuals and companies are called Specially Designated Nationals (“SDNs”). Their assets are blocked, and U.S. persons are generally prohibited from dealing with them.

U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In the case of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

1 AML Compliance Person Designation and Duties

Paper has designated James Sun as its Anti-Money Laundering Program Compliance Officer (“AML Compliance Officer”), with full responsibility for the company’s AML program. Among other duties, the duties of the AML Compliance Officer will include monitoring the company’s compliance with AML obligations, overseeing communication, and training for employees in the areas of AML/BSA compliance. The AML Compliance Officer will also ensure Paper keeps and maintains all required AML records and will ensure Suspicious Activity Reports (SARs) are filed with FinCEN when appropriate. The AML Compliance Officer is vested with full responsibility and authority to enforce the Paper AML Program.

2 Providing AML Information to Law Enforcement and Other Agencies

1 FinCEN Requests Under USA Patriot Act Section 314(a)

Paper will respond to a FinCEN request concerning accounts and transactions a 314(a) Request by immediately searching our records to determine whether Paper maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure website. Paper understands we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. Paper will designate one or more persons to be the point of contact (POC) for 314(a) Requests and will promptly update the POC information following any change in such information. Unless otherwise stated in the 314(a) Request or specified by FinCEN, Paper is required to search those documents outlined in FinCEN's FAQ. If Paper finds a match, the AML Compliance Officer will report it to FinCEN via FinCEN's web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), the AML Compliance Officer will structure the search accordingly.

If the AML Compliance Officer searches Paper records and does not find a matching account or transaction, then the AML Compliance Officer will not reply to the 314(a) Request. Paper will maintain documentation that demonstrates the required search has been performed by printing a search self verification document from FinCEN's 314(a) Secure Information Sharing System and confirming the subject's information has been searched against Paper records. This document will be maintained in Paper Slack risk and compliance folder.

Paper will not disclose any facts which may indicate FinCEN has requested or obtained information, except to the extent necessary to comply with the information request. The AML Compliance Officer will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act concerning the protection of customers' nonpublic information.

Paper will direct any questions regarding the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, Paper will not be required to treat the information request as continuing in nature, and will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

2 Subpoenas

Paper understands the receipt of a grand jury subpoena concerning a customer does not in itself require the filing of a Suspicious Activity Report (SAR). When Paper receives a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If Paper uncovers suspicious activity during our risk assessment and review, the customer's risk assessment will be elevated, and a SAR will be filed in accordance with the SAR filing requirements. Paper understands none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information used to respond to it. To maintain the confidentiality of any grand jury subpoena Paper receives, Paper will process the subpoena according to the Subpoena Response Policy and Procedure. If Paper files a

SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or existence of the subpoena. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity. Please reference Paper Subpoena Policy and Procedure documents for additional details.

3 Voluntary Information Sharing - 314(b)

Paper (using the notice form found on FinCEN's website) has filed for the purposes of subsection 314(b) of the USA PATRIOT Act and 31 CFR 1010.540. Paper will perform this filing each year by submitting the form on an annual basis.

Paper shares information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities which we suspect may involve possible terrorist activity or money laundering. Before we share information with another financial institution, we will take reasonable steps to verify the other financial institution has submitted the required notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions FinCEN makes available. We understand this requirement applies even to financial institutions with which we are affiliated, and we will obtain the required notices from affiliates and follow all required procedures.

4 OFAC - Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, Paper checks to ensure a customer does not appear on the Specially Designated Nationals (SDN) list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. To achieve this, potential customers are validated Customer by checking their information obtained at onboarding and information concerning the customer's subsequent transactions against the SDN list. If there is an indication of a possible match, the customer will not be permitted to open an account or execute a prohibited transaction after opening an account, as applicable. These potential matches are reviewed and blocked, if needed, by the Risk and Compliance team, as described in the OFAC Policy. Any blocked transactions are reported to OFAC, as described in the OFAC Policy.

Because the SDN list and listings of economic sanctions and embargoes are updated frequently, Paper consults them on a regular basis and subscribes to receive any available updates when they occur. Each month, Paper conducts an OFAC rescore against the current customer database, as described in the OFAC Policy.

5 Know Your Customer Program

Paper has established a written Know Your Customer ("KYC") program. Paper will collect the minimum customer identification information required under the BSA from each customer who uses its services, utilize risk-based measures to verify the identity of each customer, record customer identification information and the verification methods and results, and compare customer identification information with government-provided lists of suspected terrorists. As a general matter, Paper will not do business with customers that appear on relevant sanctions lists or have a previous history of financial crime activities.

Based on the risk, and to the extent reasonable and practicable, Paper will ensure it has a reasonable belief that it knows the true identity of each customer by using risk-based procedures to verify and document the accuracy of the information obtained from the customer.

Paper will analyze the information obtained to determine whether the information is sufficient to form a reasonable belief that Paper knows the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

Paper will rely on documentary methods for verifying customers' identities and may rely on electronic verification of the identification documents and identity details as a risk mitigating technique at the time of the customer's registration. Electronic verification is an acceptable method of verifying the customer's identity, and a useful measure in Paper's risk-based assessment.

Paper carries out enhanced due diligence on customers who it identifies as "high risk". Risk rating criteria includes the assessment of geographic location, CIP acceptance criteria, length of relationship, country of residence, and transactional activity. For such customers, follow-up actions may include requesting further identity documents, requesting proof of income, or rejecting the transaction.

If a potential or existing customer either refuses to provide any of the information described above when requested, or appears to have intentionally provided misleading information, Paper will not allow the customer to use its services.

6 Customer Identification Program & Customer Due Diligence

Paper has an established, documented and maintained written Customer Identification Program (CIP). Paper requires and collects certain minimum customer identification information from each customer who opens an account; utilizes risk-based measures to verify the identity of each customer who opens an account; records customer identification information and the verification methods and results; provides the required adequate CIP notices to customers stating we will seek information to verify their identities; and compares customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government.

For natural person customers, Paper will collect the following CIP information at minimum during onboarding: (i) name; (ii) date of birth; (iii) home address; and (iv) Social Security Number or other government identification number.

For legal entity customers, Paper will collect the following CIP information at minimum during onboarding: (i) name; (ii) address; and (iii) taxpayer identification number.

FinCEN'S customer due diligence ("CDD") rule outlines the explicit requirements for financial institutions to identify and verify the identity of the beneficial owners and/or individuals with controlling interest. FinCEN intends that legal entity customers identity its "ultimate" beneficial owner(s) rather than "nominees" or "straw men". The CDD rule defines beneficial ownership as:

> (i) Each individual, if any, who directly or indirectly, owns 25% or more of the equity interests of a legal entity customer; or
>
> (ii) A single individual with significant responsibility to control, manage or direct a legal entity customer, including an executive officer or senior manager (e.g. CEO, CFO, COO, Managing Member, General Partner, President, Vice President or Treasurer); or any other individual who regularly performs similar functions.

Paper will collect the minimum CIP information for natural persons listed above for each beneficial owner of a legal entity customer.

Generally, Paper shall retain all records relating to the identity of a customer for a period of at least five (5) years after the relevant customer account is closed. The AML Compliance Officer is responsible for establishing and maintaining a record retention schedule.

7 Monitoring Accounts for Suspicious Activity

Paper will monitor account activity for unusual size, volume, pattern or type of transactions, accounting for risk factors and red flags which are appropriate to our business. Monitoring will be as described in the AML Workflow document.

Monthly audits will be performed on the daily monitoring activities to ensure monitoring is being completed in a timely and effective (providing clear notes) manner.

1 Red Flags

Red flags which may signal possible money laundering or terrorist financing include, but are not limited to:

1 Customer Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents which cannot be readily verified
- Reluctant to provide complete information about the nature of their account activity
- Refuses to identify a legitimate source of funds, information is false, misleading or substantially incorrect
- The background is questionable or differs from expectations based on activities
- The customer has no discernable reason for using Paper services

2 Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide the information needed to file reports or fails to proceed with a transaction
- Tries to persuade an employee not to file required reports or not to maintain required records
- "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements
- The unusual concern with the Paper compliance with government reporting requirements and AML policies

3 Certain Funds Transfer Activities

- ACH transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason
- Many small, incoming ACH transfers or deposits which are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history
- ACH activity which is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent account purpose
- Unusually high levels of transactions for a single customer
- Customer loads and immediately redeems the entire value at an ATM

4 Activity Inconsistent with Normal Customer Activity

- Transactions patterns show a sudden change inconsistent with normal activities
- Unusual transfers of funds among accounts without any apparent account purpose
- Maintains multiple accounts, or maintains accounts in the names of family members

- Uses multiple funding cards
- Appears to be acting as an agent for another customer, but is reluctant to provide information

5 Other Activity

- Customer attempts to fund their account with a bank card which has been reported lost or stolen by the financial institution
- New account customers using four (4) or more funding cards
- Customers sharing funding cards

2 Responding to Red Flags

Paper responds to red flags (also referred to as Risk Flags) as described in the AML Workflow documentation.

8 BSA Reporting

1 Suspicious Activity Reports (SAR)

For the purpose of facilitating Paper's partner bank's compliance with its obligation to file Suspicious Activity Reports (SARs) with FinCEN, Paper will report relevant transaction information to its partner bank to the extent required by the contract between Paper and its partner bank.

Generally, financial institutions must file a SAR with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through the financial institution involving $10,000 or more of funds or assets (either individually or in the aggregate) where it knows, suspects or has reason to suspect:

- The transaction involves funds derived from illegal activity or is intended or conducted 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;
- The transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;
- The transaction 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, the possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
- The transaction involves the use of the firm to facilitate criminal activity.

Financial institutions must collect and maintain supporting documentation for a SAR as required by the BSA regulations and file a SAR no later than 30 calendar days after the date of the initial detection of the facts which constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, it may delay filing the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection.

2 Currency Transaction Reports (CTR)

For the purpose of facilitating Paper's partner bank's compliance with its obligation to file Currency Transaction Reports (CTRs) with FinCEN, Paper will report relevant transaction information to its partner bank to the extent required by the contract between Paper and its partner bank.

Generally, financial institutions must file a CTR for each deposit, withdrawal, exchange of currency, or other payment or transfer by, through or to the financial institution which involves a transaction in currency of more than $10,000 or for multiple transactions in currency of more than $10,000 when it knows the transactions are by or on behalf of the same person during any one business day, unless the transaction is subject to certain exemptions. "Currency" is defined as "coin and paper money of the United States or of any other country," which is "customarily used and accepted as a medium of exchange in the country of issuance." Currency includes U.S. silver certificates, U.S. notes, Federal Reserve notes, and official foreign banknotes, which are customarily used and accepted as a medium of exchange in a foreign country.

3 Currency and Monetary Instrument Transportation Reports

Paper prohibits both the receipt of currency or other monetary instruments which have been transported, mailed or shipped to us from outside of the United States and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier. Paper will file a CMIR with the Commissioner of Customs if Paper discovers the company has received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time (on one calendar day or, if to evade reporting requirements, on one or more days). Paper will also file a CMIR if we discover the company has physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier currency or other monetary instruments of more than $10,000 at one time (on one calendar day or, if to evade the reporting requirements, on one or more days). Paper will use the CMIR form provided on FinCEN's Web site.

4 Monetary Instrument Purchases

Paper does not issue bank checks or drafts, cashier's checks, money orders, or traveler's checks in any amount for sale.

9 AML Recordkeeping

It is the policy of Paper to follow its Records Retention Policy. This policy complies with existing BSA and other recordkeeping requirements.

10 Training Programs

1 Company-Wide Training

Paper employees are required to participate in a yearly training program which currently has five components:

- Ethics
- Compliance Essentials
- Anti-Money Laundering

- Introduction to PCI-DSS Compliance
- Information Security Awareness

Paper also holds weekly Operations meetings that cover updates on all aspects of operations, including risk and compliance-related matters.

2 AML/BSA Specific Training

The AML Compliance Officer is responsible for training members of the Risk and Compliance team. For training documentation, please reference the BSA/AML Training document.

Additionally, training will include how to identify red flags and signs of money laundering while completing transaction monitoring and what to do when risks are identified.

The Risk and Compliance team also has weekly meetings with sponsorship banks to discuss the results of monitoring for the week.

3 UDAPP Compliance

The AML Compliance Officer is responsible for training members of the Risk and Compliance, Support, and Program Management teams on UDAAP Compliance yearly.

11 Program to Independently Test AML Program

Paper will have a qualified and independent third party assess its AML/BSA program annually. The testing of the Paper AML/BSA program must include (at a minimum):

- Evaluation of the overall integrity of Paper procedures for BSA reporting and recordkeeping requirements
- Evaluation of the implementation and maintenance of Paper CIP
- Evaluation of Paper customer due diligence requirements
- Evaluation of Paper transactions (with an emphasis on high-risk areas)
- Evaluation of Paper training program
- Evaluation of Paper method for identifying and reporting suspicious activity
- Evaluation of Paper response to previously identified deficiencies

1 Evaluation and Reporting

After Paper has completed the independent testing, the Risk and Compliance team will report its findings to senior management. The Risk and Compliance team will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

12 Monitoring Employee Conduct

There are personal obligations for every member of Paper management and staff.

- It is an offense to assist anyone you know or suspect to be, laundering money generated by any serious crime. Assistance can be provided by, for example, opening an account, accepting deposits, making transfers, making payments, or overriding company systems or policies.
- The financing of terrorism is also covered by two separate offenses: the collection of funds and making funds available. These offenses include receiving or providing funds while knowing or

suspecting they might be used for terrorism and making funds or financial services available for terrorist activities.

- If you know or suspect a transaction is related to any serious crime, including terrorist financing, you must report it to provide a defense against a charge of knowingly assisting a criminal to launder the proceeds of their crime.
- If you form a suspicion of money laundering or terrorist financing in the course of your employment or business activity, you must report it, even if you are not handling the instruction, transaction, or funds in question.

1 Internal Effect of Violating Company Policies

Any member of management or staff found to knowingly violate a company policy or procedure is subject to disciplinary action including immediate termination and being reported to the authorities. Compliance with company policies is mandatory and a material condition to employment.

2 Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm's AML compliance program to the AML Compliance Officer unless the violations implicate the AML Compliance Officer, in which case the employee shall report to the Paper President. Such reports will be confidential, and the employee will suffer no retaliation for making them.

13 Additional Risk Areas

Paper has performed a Risk Assessment to review all areas of its business to identify potential money laundering and other risks that may not be covered in the procedures described in this manual. Please see the Risk Assessment for more information. The Risk Assessment will be updated periodically. The update will reflect any changes, inherent risks, and the control environment of Paper. Updates will be made as Paper adds or changes products offered, new geographic risks, geopolitical events, and economic conditions.

14 Approval

1 Minimum Approval Requirement

This document must be approved by the AML Compliance Officer and Paper Board of Directors to become effective.

2 Board Approval of this AML Policy

The Board of Directors of Paper has approved this AML Policy by way of a Unanimous Written Consent dated August 15, 2022 as reasonably designed to achieve and monitor our company's ongoing compliance with the requirements of the BSA and the implementing regulations under it.

3 Review Cycle

1 Review Triggers

This document must be reviewed and approved any time material policy change is made.

2 Periodic Review

In the absence of any Review Triggers, this document must be reviewed on an annual basis.