

Anti-Money Laundering Policy and Procedures

Effective: 05/01/2022

Table of Contents

Revision History	3
Background and Introduction	4
Paper.xyz Policy.....	4
Money Laundering	4
Placement	4
Layering	4
Integration	4
Terrorist Financing	4
AML Compliance Person Designation and Duties.....	5
Providing AML Information to Law Enforcement and Other Agencies.....	5
FinCEN Requests Under USA Patriot Act Section 314(a).....	5
Subpoenas	6
Voluntary Information Sharing - 314(b).....	6
OFAC - Office of Foreign Assets Control Listings	6
Customer Identification Program (CIP)	7
Monitoring Accounts for Suspicious Activity	7
Red Flags	7
Cardholder Insufficient or Suspicious Information	7
Efforts to Avoid Reporting and Recordkeeping.....	7
Certain Funds Transfer Activities.....	7
Activity Inconsistent with Normal Cardholder Activity	8
Other Activity.....	8
Responding to Red Flags.....	8
Suspicious Transaction Reporting (SAR) and BSA Reporting.....	8
Suspicious Transaction Reporting (SAR)	8
SAR Decision Making.....	8
SAR Filing.....	9
SAR Maintenance and Confidentiality	10
SARs and Cardholder Notifications	10
Currency Transaction Reports (CTR)	10
Currency and Monetary Instrument Transportation Reports.....	10
Monetary Instrument Purchases.....	10
AML Recordkeeping.....	11
Training Programs.....	11

Company-Wide Training	11
AML/BSA Specific Training	11
UDAPP Compliance	11
Program to Independently Test AML Program.....	11
Evaluation and Reporting	12
Monitoring Employee Conduct.....	12
Internal Effect of Violating Company Policies	12
Confidential Reporting of AML Non-Compliance	12
Additional Risk Areas	12
Approval	13
Minimum Approval Requirement.....	13
Board Approval of this AML Policy	13
Review Cycle.....	13
Review Triggers	13
Periodic Review	13

Background and Introduction

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 anti-money laundering (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.xyz ("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.

The Paper Policy

It is the Paper 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 Bank Secrecy Act (BSA) and its implementing regulations.

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.

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.

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.

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.

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.

The Paper AML policies, procedures, and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures, and internal controls are in place to account for both changes in regulations and changes in our business.

AML Compliance Person Designation and Duties

Paper has designated James Sun as its Anti-Money Laundering Program Compliance Officer ("Director of Risk and Compliance"), with full responsibility for the company's AML program. 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 the Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Compliance Officer is vested with full responsibility and authority to enforce the Paper AML Program.

Providing AML Information to Law Enforcement and Other Agencies

FinCEN Requests Under USA Patriot Act Section 314(a)

Paper will respond to a Financial Crimes Enforcement Network (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 Director of Risk and Compliance 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 Director of Risk and Compliance will structure the search accordingly.

If the Director of Risk and Compliance searches Paper records and does not find a matching account or transaction, then the Director of Risk and Compliance 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 Director of Risk and Compliance 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.

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.

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.

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 cardholders are validated through a Cardholder Identification Process (CIP), which checks their information against the SDN list. If there is an indication of a possible match, the cardholder will not be permitted to open an account. These potential matches are reviewed by the Risk and Compliance team, 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 cardholder database, as described in the OFAC Policy.

Customer Identification Program (CIP)

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.

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.

Red Flags

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

Cardholder 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 cardholder has no discernable reason for using Paper services

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

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 cardholder
- Cardholder loads and immediately redeems the entire value at an ATM

Activity Inconsistent with Normal Cardholder 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 cardholder, but is reluctant to provide information

Other Activity

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

Responding to Red Flags

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

Suspicious Transaction Reporting (SAR) and BSA Reporting

Suspicious Transaction Reporting (SAR)

SAR Decision Making

While there are specific situations when Paper must file a SAR (discussed in the SAR Filing section), there are also times when Paper decides to file or not to file a SAR.

When discussing a potential SAR filing which falls outside of the specific FinCEN SAR filing rules, the SAR Committee will discuss the cardholder(s) activity and determine if the activity requires a SAR to be filed. The documentation of this discussion will be placed in Slack (Paper shared document service) either with the SAR documentation (if a SAR is filed) or in a customer folder (if a SAR is not filed). If a SAR is filed, the cardholder's account will be blocked. If a SAR is not filed, the final disposition of the account will be determined by the Risk and Compliance team and noted in the Slack risk folder.

The SAR Committee consists of representatives from Operations, Risk and Compliance, and Support teams within Paper.

SAR Filing

Paper will file a SAR with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our company involving \$10,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have 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.

Paper will notify the appropriate government agency of potential terrorist financing, as required by law. Paper understands even if we notify a regulator of a violation unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR reporting the violation.

Paper may file a voluntary SAR for any suspicious transaction which is relevant to the possible violation of any law or regulation but is not required to be reported under the SAR rule.

Paper will report suspicious transactions by completing a SAR and will collect and maintain supporting documentation as required by the BSA regulations. Paper will 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, we 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. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins at the time of the suspicious transaction or activity occurred.

Paper will conduct an appropriate review and determine the transaction under review is "suspicious" within the meaning of the SAR requirements and within the 30 or 60-day period. A review must be initiated promptly upon identification of unusual activity, which warrants investigation.

Paper will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR. We will identify and maintain supporting documentation and make such information available to FinCEN, as well as any other appropriate law enforcement agencies, federal or state regulators upon request.

Paper will not notify any person involved in the transaction, which is being reported except as permitted by BSA regulations. Paper understands anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where disclosure is requested by FinCEN, or another appropriate law enforcement or regulatory agency, decline to produce the SAR or to provide any information which would disclose a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

SAR Maintenance and Confidentiality

Paper deems SARs and any supporting documentation confidential. Paper will not inform anyone outside of FinCEN, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR. We will refuse any subpoena requests for SARs or for information that would disclose a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests received. Paper will segregate SAR filings and copies of supporting documentation from other company records to avoid disclosing SAR filings. The Risk and Compliance team will handle all subpoenas or other requests for SARs.

SARs and Cardholder Notifications

If a cardholder's account has been blocked due to a SAR filing, the cardholder will not be notified a SAR was filed. If the cardholder requests information regarding their account, the cardholder should be referred to the applicable section of the Terms and Conditions, which states Paper reserves the right to revoke or cancel their card at any time and without prior notice.

Currency Transaction Reports (CTR)

Paper must file a Currency Transaction Report (CTR) for each deposit, withdrawal, exchange of currency, or other payment or transfer by, through or to Paper which involves a transaction in currency of more than \$10,000 or for multiple transactions in currency of more than \$10,000 when a financial institution 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.

If Paper discovers such transactions have occurred, Paper will file with FinCEN CTRs for currency transactions exceeding \$10,000. Also, Paper will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a CTR if they total more than \$10,000 and are made by or on behalf of the same person during any one business day. Paper will use the CTR form provided on FinCEN's website.

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.

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.

AML Recordkeeping

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

Training Programs

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.

AML/BSA Specific Training

The Director of Risk and Compliance 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.

UDAPP Compliance

The Director of Risk and Compliance is responsible for training members of the Risk and Compliance, Support, and Program Management teams on UDAPP Compliance yearly.

Program to Independently Test AML Program

Paper will have a qualified third party or internal Paper personnel 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

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.

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.

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.

Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm's AML compliance program to the Director of Risk and Compliance unless the violations implicate the Director of Risk and Compliance, 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.

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.

Approval

Minimum Approval Requirement

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

Board Approval of this AML Policy

The Board of Directors of Caves Inc. has approved this AML Policy by way of a Unanimous Written Consent dated **May 25, 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.

Review Cycle

Review Triggers

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

Periodic Review

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