MATTERCASH INC.
Anti-Money Laundering
Compliance and Supervisory Procedures

Table of Contents

1. Firm Policy
2. General Understanding of Money Laundering

2-1. Placement

2-2. Layering

2-3. Integration

1. AML Compliance Officer Designation and Duties
2. Giving AML Information to Law Enforcement Agencies
3. Checking Government Lists
4. Customer Identification and Verification

a. Required Customer Information
b. Customers Who Refuse to Provide Information
c. Verifying Information
d. Lack of verification
e. Evaluating Customer Information
f. Record-keeping
g. Notice to Customers and Request for AML Certification
6. Employee Background
7. Monitoring Accounts for Suspicious Activity
a. Emergency Notification to the Government by Telephone
b. Red Flags
c. Responding to Red Flags and Suspicious Activity
8. Suspicious Transactions and BSA Reporting
a. Filing for SAR-MSB
b. Currency Transaction Reports (CTR):
Form IRS/FinCEN 8300
c. Money Transfers
d. Metal Transfers
9. AML Recordkeeping
a. SAR-MSB Maintenance and Confidentiality
b. Responsibility for AML Records and SAR Filing
c. Records Required
10. Training Programs
11. Testing the AML Program
12. Confidential Reporting of AML Non-Compliance
13. Purchase and Repurchase of Precious Metals
14. Vault Program
15. Foreign Bank Accounts
16. Senior Manager Approval

1. Firm Policy:
 It is the policy of MATTERCASH INC. to prohibit and actively prevent money laundering and the funding of terrorist or criminal activities. We define money laundering as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

 2. Generally, money laundering occurs in three stages:
 2-1. Placement:

 Currency, precious metal, or gemstones first enter the financial system at the
"placement" stage, where the gains generated from criminal activities are converted into monetary instruments, such as money orders or traveler's checks; into precious metals or gemstones; or deposited into currency accounts or precious metals pool accounts at financial institutions or at companies dealing in precious metals or gemstones.
 2-2. Layering:

 At the "layering" stage, to further separate the money from its criminal origin, funds, precious metals, or gemstones are transferred or moved into other accounts or other financial institutions or into other companies dealing in precious metals or gemstones.
 2-3. Integration:

 At the "integration" stage, currency, precious metals, or gemstones are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

 Money laundering and terrorist finance are illegal. They undermine the security of our society and the viability and success of our business. Non-compliance risks business interruption fines up to $1 million, prison terms up to 20 years per count, forfeiture of assets, heavy legal expenses, and damage to individual and company reputation that may be irreversible.

 It is our policy to encourage all employees to report suspicious activity to the Anti-Money Laundering Compliance Officer. We have adopted this policy to help employees avoid involvement in money laundering and to encourage them to detect and report transactions as required by the Government. Employees who observe suspicious activity but are uncomfortable discussing it with the Anti-Money Laundering Compliance Officer should feel free to discuss the information with a senior manager, confidentially and without fear of retaliation.
 PMB&V's management is committed to preventing involvement in any money laundering or terrorist finance scheme.

 3. AML Compliance Officer Designation and Duties:
 MATTERCASH INC. designates Dale Olmstead as its Anti-Money Laundering Compliance Officer, with full responsibility for the firm’s AML program. Mr. Olmstead is qualified by experience, knowledge, and training, and is the operations manager of MATTERCASH INC. The AML Compliance Officer will be responsible for the firm’s compliance with the AML procedures described in this program, to include assessing the company’s exposure to money laundering, monitoring the firm’s compliance with AML obligations, overseeing communication and training for employees, arranging for regular testing of AML systems and precautions. The AML Compliance Officer will also ensure that
proper AML records are kept. When warranted, the AML Compliance Officer, at his discretion, will ensure Suspicious Activity Reports (SAR’s) are filed.
 The firm will provide all employees with current contact information for the AML Compliance Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number, along with contact information for regulatory and law enforcement offices (See Appendix I).

 4. Giving AML Information to Federal Law Enforcement Agencies:
 Management has designated the AML Compliance Officer to coordinate with Government agencies on matters involving money laundering, terrorist finance and suspicious activity. Employees should refer all Government regulatory or enforcement agency requests for information to the AML Compliance Officer.
 We will respond to and cooperate with the Financial Crimes Enforcement Network (FinCEN) and other Federal or State law enforcement and regulatory agencies. Contact with law enforcement and regulatory agencies and responses to requests for information about accounts or transactions will be handled through the AML Compliance Officer or other designated person. That response will begin by immediately searching our records, at our head office and at affiliates operating in the United States and subject to the AML provisions of the USA PATRIOT Act, to determine whether we maintain or whether we have maintained any account or engaged in any transaction with each individual, entity, or organization named in the request. Upon receiving an information request, we will designate one person to be the point of contact regarding the request and to receive similar requests in the future. Unless otherwise stated in the request, we will search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it immediately. If the request is by FinCEN, we will respond by calling its Financial Institutions Hotline, 866-556-3974 or by completing FinCEN’s subject information form. This form can be sent to FinCEN by electronic mail at www.fincen.gov, or by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time), we will adapt our search accordingly. If we search our records, and if we do not uncover a matching account or transaction, we will reply that we have no records.
 We will not disclose the fact that information has been requested or obtained from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of information requests from, such as those established to satisfy the requirements of Section 501 of the Gramm - Leach Bliley Act (See Appendix II).
 We will direct any questions to the requesting Federal law enforcement agency as designated in the request.
 Unless otherwise requested in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements.
 We will not use information provided to a Government agency for any purpose other than (1) to report as required under the AML regulations; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the firm in complying with any requirement of the AML regulations.

 5.Checking Government Lists:
 Before a holding account is opened (or when required by another State or Federal law, regulation or directive issued in connection with an applicable list), we may check whether a customer or vendor appears on a list of known or suspected money-launderers, terrorists or terrorist organizations issued by any State or Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. We will follow all directives issued in connection with such lists.
The regulations apply to customers and vendors alike, so the term “customers” when used in these AML Compliance and Supervisory Procedures will include both customers and vendors.
 Before opening a holding account, we may check to ensure that a customer does not appear on Treasury’s OFAC “Specifically Designated Nationals and Blocked Persons” List (SDN or OFAC List).We may also check applicants’ credentials against the list of Deceased Persons. Because the OFAC Web Site is updated frequently, we may consult the list on a regular basis. We may also review other such lists made available by United States Government agencies, as well as lists of non-cooperative countries issued by international bodies such as the Financial Action Task Force and the United Nations. We may access these lists through various software programs to ensure speed and accuracy. We may also review existing accounts against these lists regularly, and we will document our review when doing so.
 If we determine a client, or someone with whom the client is transacting business, is on the SDN List or is engaging in transactions with a person or entity located in an embargoed country or region, we will not proceed with the transaction pending clarification and may report it to FinCEN.

 6. Customer Identification and Verification:
 We will collect certain minimum client identification information from each client. We will use risk-based measures to ascertain, document and verify the identity of each client who opens a holding account and is large enough to present a money laundering risk. We will record client identification information and the verification methods and results; provide notice to clients that we will seek identification information and compare client identification information with government- provided lists of suspected terrorists.
 a. Required Customer Information:
 Prior to opening a holding account, we will collect the following client information;
- Full Name
- Telephone Numbers
- Physical Address

- Mailing Address (if different from physical)
- Federal Tax ID Number
- Date of Birth
- Copy of a Valid Government Identification

- Mothers Maiden Name

- Email Address

- Name of Employer or DBA

- Occupation

 If we feel reasonably confident that we have correctly identified the client, we need
not seek further information, although we might choose to do so.
 c. Clients Who Refuse To Provide Information:
 If a prospective or existing client refuses to provide the information described above
when requested, we may obtain this information from other sources. If we are confident that we have correctly identified the client, even without all the information indicated above, we might choose to do business with the person(s), subject to approval by the AML Compliance Officer. If a prospective or existing client provides deliberately misleading information, we will investigate the reason and will not open the holding account or, after considering the risks involved, may consider closing any existing holding account. In either case, the AML Compliance Officer will be notified and will determine whether to report the situation to FinCEN.
 d. Verifying Information:
 Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our clients by verifying and documenting the accuracy of the information we collect. To verify client identity, we will analyze logical inconsistencies in the information we obtain. We might verify client identity through documentary evidence, non-documentary evidence, or both. We will use Government-issued documents to verify client’s 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. In analyzing the verification information, we will consider whether there is a logical consistency within the identifying information provided, such as the client’s name, street address, zip code and telephone number.
 Appropriate documents for verifying the identity of customers include, but are not limited to, the following:
 • A unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver’s license or passport; and
 • A valid government issued Tax ID card such as a social security card.
 We understand that we are not required to take steps to determine whether the document
that the customer has provided for identity verification has been validly issued and that we may rely on government-issued identification as verification of a customer’s identity. If we note the document shows some obvious form of fraud, we will consider this as a factor in determining whether we can form a reasonable belief as to the customer’s true identity.
 We might use any of the following non-documentary methods of verifying identity:
 • Contacting a client;
 • Independently verifying the customer’s identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source;
 • Checking references with other companies financial institutions; or
 • Obtaining 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 restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering or terrorist financing activity, we may file a SAR-MSB in accordance with applicable law and regulation.
 We recognize the risk of not knowing the client’s true identity may be heightened for
certain types of accounts, such as a holding account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction designated by the U.S. as a primary money laundering concern or one that has been designated as non-cooperative by an international body. We will identify clients that pose a heightened risk if not properly identified, and we will take the following additional measures to obtain information about the identity of the individuals associated with the client when standard documentary methods prove to be insufficient:
 1. Confirm the beneficial ownership of the holding account
 2. Verify the identity of individuals with control or authority over the holding account.

 e. Lack of Verification:
 When we cannot form a reasonable belief that we know the true identity of a
client, we will do the following:

 (A) not open a holding account.

 (B) impose terms under which a client may conduct transactions while we attempt to verify the client’s identity.

 (C) close a holding account after attempts to verify client’s identity fail; or

 (D) after consultation with the Company’s Compliance Officer or management, file a SAR (See Section 8-a).
 f. Evaluating Client Information:
 We will perform an initial risk assessment of each new client. We will treat a questionable assessment as an internal “red flag.”
 g. Record-keeping:
 We will document our verification, including all identifying information provided by a
client, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will keep records containing a description of any document that we relied on to verify a client’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 the results of any measures we took to verify the identity of a client. We will maintain records of all identification information for five years after the holding account has been closed; we will retain records made about verification of the client's identity for five years after the record is made.
 h. Notice to Clients and Request for AML Certification:
 If we request information from clients, we will advise them that the firm is requesting information to verify their identities, as required by Federal law. (See Appendix IV)

 6. Employee Background:
 To protect the company from employee complicity in laundering or terrorist finance activity, we will collect and review background information prior to hiring every employee. The areas investigated depend on the sensitivity and seniority of a potential employee.

 7. Monitoring Accounts for Suspicious Activity:
 Managers will monitor customer to detect unusual size, volume, pattern or type of transactions or geographic factors such as whether jurisdictions designated as “uncooperative” are involved, or any of the “red flags” identified in Section 7- b. below. We will review transactions, including money or metal transfers in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that client. The AML Compliance Officer or his designee will be responsible for this monitoring and, at the discretion of the AML Compliance Officer, will report suspicious activities to the appropriate authorities. Included in the information we will use to determine whether to file a Form SAR-MSB are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and will note high-risk clients whose accounts may warrant further scrutiny. Our AML Compliance Officer will conduct an investigation before a SAR is filed.
 a. Emergency Notification to the Government by Telephone;
 Although there is no suspicious activity reporting requirement for precious metals companies under current AML and anti-terrorist finance regulations, we will instruct employees how to report suspicious activity to the AML Compliance Officer and how to contact FinCEN if they feel they must report it directly. Contact information for the AML Compliance Officer, FinCEN and local law enforcement authorities is attached in this plan as Appendix I and will be posted.
 When conducting due diligence or opening a holding account, we will immediately call Federal
law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the holding account holder is engaged in a transaction is listed on the OFAC list, a client tries to use bribery, coercion, or similar means to open a holding account or carry out a suspicious activity, we have reason to believe the client is trying to move illicit cash out of the government’s reach, or we have reason to believe the client is about to use the funds to further an act of terrorism. We will first call the FinCEN Financial Institutions hotline 866-556-3974.
 b. Red Flags:
 Employees will be instructed to watch for the behavior patterns that the Treasury Department summarizes as being symptomatic of laundering situations:
 A. Unusual payment methods, such as large amounts of currency, multiple or sequentially numbered money orders, traveler’s checks, or cashier’s checks, or payment from third parties.
 B. Unwillingness to provide complete or accurate contact information, financial references or business affiliations.
 C. Attempts to maintain a high degree of secrecy, such as a request that normal business records not be kept.
 D. Purchases or sales unusual for the particular client or supplier or type of client or supplier.
 E. Purchases or sales that do not conform to standard industry practice.

 For specific examples of red flags, see Appendix III.
 c. Responding to Red Flags and Suspicious Activity:
 When a member of the firm detects any red flag, he or she will report it to the AML Compliance Officer and will provide all necessary support to investigate the activity. This may include gathering additional information internally or from third-party sources. The AML Compliance Officer may choose to file a Form SAR-MSB. Suspicious activity and red flags, whether reported or not, will be detailed in a written report. The report will be placed in the customer’s file which will be stored electronically for 5 years after the reports was made.

 8. Suspicious Transactions and BSA Reporting:
 a. Filing a Form SAR-MSB;
 We may file FinCEN Form 101, “Suspicious Activity Report by the Money Service Businesses” (SAR-MSB) for any account activity (including deposits and transfers) conducted or attempted through our firm involving (or in the aggregate) $5,000 or more of funds or assets where we know, suspect, or have reason to suspect:

 1) the transaction involves funds or precious metals derived from illegal activity or is intended or conducted in order to hide or disguise funds, precious metals 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) the transaction is designed, whether through structuring or otherwise, to evade the requirements of the BSA regulations,

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

 4) the transaction involves the use of the firm to facilitate criminal activity.
 We would not base our decision on whether to file a SAR-MSB solely on whether the transaction falls above a set threshold. The AML Compliance Officer might file a SARMSB to notify law enforcement of transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, we will notify the government immediately (See Section 8 for contact numbers) and will file a SAR-MSB with FinCEN. All SAR-MSBs will be reported to the Board of Directors and senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-MSB. If we report suspicious transactions by completing a SAR-MSB, we will collect and maintain supporting documentation as required by the BSA regulations. We would file a SAR-MSB no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-MSB. If no suspect is identified on the date of initial detection, we may delay filing the SAR-MSB 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. We will retain copies of any SAR-MSB filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-MSB. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators, upon request. We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR-MSB or the information contained in the SARMSB, except where disclosure is requested by FinCEN or another appropriate law enforcement or regulatory agency, will decline to produce the SAR-MSB or to provide any information that would disclose that a SAR-MSB was prepared or filed. We will notify FinCEN of any such request and our response.
 b. Reporting Currency Transactions:

 Our firm’s policy is to report any and all currency transaction over $10,000, we will file with FinCEN Form 8300 for transactions involving currency receipts that exceed $10,000. Multiple transactions with the same or related parties will be treated as a single transaction if they total more than $10,000 during any one business day or over a longer period if they can be identified as connected. The retention copy of all Form 8300’s will be countersigned by a second person who will be equally responsible for the accuracy of the contents.
 c. Money Transfers
 It is the policy of the company to refuse receipt or remittance of third-party money transfers. The only exception to this policy is in the case of a death of a client where their assets need to be transferred to a beneficiary or inheritor. In the case of death, a copy of the death certificate and a court or probate document declaring the beneficiary must be provided. Additionally, the beneficiary or inheritor will have to go through the same identification checks as if they were opening a new holding account. Should we transfer funds of $3,000 or more to a third party, we will record on the transmittal order at least the following information: the name and address of the transmitter and recipient, the amount of the transmittal order, the identity of the recipient’s financial institution, and the account number of the recipient. If we are unfamiliar with the recipient of a money transfer, we will confirm the recipient or source of funds is not on any Government list of suspicious persons or destinations. With the transmittal order, we will retain the letter of authority from the transmitter instructing us to transfer funds.
 d. Precious Metals Transfers
 It is the policy of the company to refuse receipt or remittance of third-party metals transfers. The only exception to this policy is in the case of a death of a customer where their assets need to be transferred to a beneficiary or inheritor. In the case of death, a copy of the death certificate and a court or probate document declaring the beneficiary must be provided. Additionally, the beneficiary or inheritor will have to go through the
same identification checks as if they were opening a new account. Should we undertake
third party metals transfers, we will confirm the recipient or source of metal is not on any
Government list of suspicious persons or destinations? Money laundering risk is not
necessarily tied to the dollar value of a transaction; however, as a practical matter, we
will focus on transfers of above $5000.
July 18th, 2018
9. AML Record Keeping
a. SAR-MSB Maintenance and Confidentiality.
We will hold SAR-MSBs and any supporting documentation confidential. We will not
inform anyone outside of a law enforcement or regulatory agency about a SAR-MSB.
We will refuse any subpoena requests for SAR-MSBs or SAR-MSB information and
immediately tell FinCEN of any such subpoena we receive. We will segregate SARMSB filings and copies of supporting documentation from other firm books and records
to avoid disclosing SAR-MSB filings. Our AML Compliance Officer will handle all
subpoenas or other requests for SAR-MSBs.
b. Responsibility for AML Records and SAR Filing
Our AML Compliance Officer or his designee will be responsible to ensure that AML
records are maintained properly and that SAR’s are filed within 30 days after discovery
of suspicious activity when the party is known to the company and within 60 days when
the party is not known.
c. Records Required
As part of our AML program, our firm will create and maintain SAR-MSBs, CTRs and
relevant documentation on customer identity and verification (See Section 5 above) and
funds transfers and transmittals as well as any records related to customers listed on the
OFAC list. We will maintain customer identification information and SAR-MSBs and
their accompanying documentation for five years.
July 18th, 2018
10. Training Programs
We will develop ongoing employee training under the leadership of the AML
Compliance Officer and senior management. We require all employees who have
customer contact to undertake a training course upon employment and to receive
refresher courses at least once a year. In addition to employees with customer contact,
certain employees, such as those with compliance and corporate security responsibilities
in a position to detect money laundering if it occurs, may be required to undertake similar
general training.
Our training will include, at a minimum: how to identify red flags and signs of money
laundering that arise during the course of the employees’ duties; what to do once the risk
is identified; employees' roles in the firm's compliance efforts and how to perform them;
the firm's record retention policy; and the consequences (including civil and criminal
penalties) for non-compliance with the anti-money laundering and anti-terrorist finance
laws and regulations..
The training may include educational pamphlets, videos, intranet or internet courses, in person lectures, and explanatory memos.
It is our policy to make all employees aware of money-laundering risk and the company’s
commitment to oppose it.
We will maintain records enumerating the persons that have undergone training, the
dates, and the subject matter of their training.
July 18th, 2018
11. Testing the AML Program
We will conduct a systems test on our AML program annually to confirm the systems
and procedures we establish are being correctly implemented and followed,
documentation is complete, records are being maintained, reports are being filed, staff is
being trained and management is current on AML developments.
The testing of our AML program will be performed by an outside auditor or a manager of
MATTERCASH INC.. If an internal manager, to ensure that he or she remains independent, we
will separate the testing functions from other AML activities by assigning him no duties
related to the administration of the AML program other than the duty to test the AML
programs and systems.
After testing has been completed, the auditor will report his findings to the AML
Compliance Officer. The AML Compliance Officer will respond in writing of remedial
suggestions with deadlines for actions to be taken.
July 18th, 2018
12. Confidential Reporting of AML Non-Compliance
Employees will report any violations of the firm’s AML compliance program to the AML
Compliance Officer unless the violations implicate the Compliance Officer in which case
the employee shall report them to another senior manager. Such reports will be
confidential, and the employee will suffer no retaliation for making them.
Employees may also report their concerns directly to an enforcement agency, such as the
Department of Homeland Security or the FBI. Reporting directly to a government
agency should be a last resort and should take place only if the employee is concerned
that management as a whole is complicit.
July 18th, 2018
13. Purchase and Repurchase of Precious Metals
Purchases of precious metals and alloys (containing 50% or more of precious metals) and
exceeding the threshold described in Section 5-b, will be from companies approved by
the AML Compliance Officer.
MATTERCASH INC. will repurchase metals it has sold to customers.
July 18th, 2018
14. Vault Program
We will provide storage services for customers. Should we use other
vaulting facilities, they will have similar secured facilities, insurance and financial
capability.
All metals are stored on behalf of MATTERCASH INC. customers with MATTERCASH INC. acting as
custodian. The fractional ownerships of the metals are maintained
on/through PMB&V LLC’s proprietary platform.
July 18th, 2018
15. Foreign Bank Accounts:
We have no foreign bank accounts. All payments and receipts are deposited into our
United States bank accounts.
July 18th, 2018
16. Senior Manager Approval
I have approved this Anti-Money Laundering program as reasonably designed to achieve
and monitor our firm’s ongoing compliance with the requirements of the of the USA
PATRIOT Act, the Bank Secrecy Act and other anti-money laundering and anti-terrorist
finance laws and their implementing regulations.
Signed:\_
Title: Dale Glenn Olmstead,
Chief Executive Officer
Date: March, 22nd, 2021