

**MetraPay Inc
Douglasville, Georgia**

**Anti-Money Laundering Policy
October 1, 2020**

Money Laundering Overview	1
MSB Registration.....	2
Recordkeeping Requirements	2
Third Party Transaction Requirements	3
Currency Transaction Reporting (CTR) Requirements	3
Structuring.....	3
Civil and Criminal Penalties	3
Suspicious Activity	4
Suspicious Activity Examples	4
Enhanced Due Diligence for New Accounts	5
Enhanced Due Diligence – Other Factors.....	5
Procedures for Detecting Money Laundering.....	5
Office of Foreign Assets Control (OFAC).....	6
Terrorist Financing Prevention	6
Procedures for Monitoring Compliance with this Policy	7
Compliance Officer Training and Responsibilities.....	7
Submission of SAR or CTR by Compliance Officer.....	8
Employee Training and Responsibilities	8
Internal Suspicious Activity Tracking Report	9

Anti-Money Laundering Program MetraPay Inc.

This AML Compliance Program contains policies and procedures to help MetraPay officers and agents comply with United States Federal and state specific Anti-Money Laundering (AML) and Prevention of Terrorist Financing Regulations.

The establishment of this anti-money laundering (AML) Compliance program will enable MetraPay achieve the following goals within the organization and across any appointed agents or representatives:

- Detect and prevent money laundering and terrorist financing.
- Comply with the USA PATRIOT Act and the Bank Secrecy Act (BSA) recordkeeping and reporting requirements
- Designate, in writing, a Compliance Officer for the Business
- Train all employees, at least annually, on anti-money laundering compliance
- Monitor all transactions continually and report all “suspicious activity” as prescribed in this Program to the federal government
- Maintain all records MetraPay is required to keep by law
- Have an independent review performed at least annually

The management and board of directors of MetraPay Inc. (MetraPay) are committed to combating money laundering within its operations. MetraPay will actively search for suspicious activity, when it is discovered, a company officer will review it and make a recommendation as to whether a Suspicious Activity Report (SAR) should be filed.

The assigned officer will have ten (10) business days to conduct the review and make his recommendation. All recommendations will be made in writing and forwarded to the Anti-Money Laundering Compliance Officer. The Compliance Officer is responsible for reviewing the investigating officer’s recommendation and determining if an SAR should be filed.

The Compliance Officer will file the SAR with the appropriate legal and regulatory authorities. All supporting evidence for the SAR will be maintained for a minimum of five (5) years, and will be securely stored. The Compliance Officer will report to the board of directors the number of SARs filed each month, along with brief a summary as to dollar amount of the suspicious activities and why they were deemed that way.

Money Laundering Overview

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership or control of illegally obtained money. It is not hard for criminals to obtain currency. However, until the currency is deposited into the banking system, their ability to utilize it is restricted. When banks/remittance companies knowingly accept the cash deposits of criminals, they legitimize (or launder) the proceeds. Accordingly, to

prevent criminals from leveraging the MetraPay platform or illegal transactions, MetraPay officers must be diligent in detecting and reporting suspicious activity.

To help prevent the laundering of cash and to obtain documentation that may be used to prosecute money launderers, the government requires you to maintain records on certain cash transactions. Some transactions also require that reports be filed and maintained.

As a money transmitter, Metrapay is subject to the Bank Secrecy Act (BSA), the USA PATRIOT Act, OFAC, other anti-money laundering laws, and to their reporting and recordkeeping obligations. The BSA requires anyone doing business as a money transmitter to comply with these laws. All businesses and entities that are covered by the definitions above are known as **Money Services Businesses, or MSBs.**

MSB Registration

All MSBs are required to register with the U.S. Treasury Department. MetraPay is registered with the U.S. Treasury Department as an MSB and most of its agents are covered by MetraPay's registration and do not have to register on their own if they do not engage in other services outside of MetraPay that requires MSB registration.

Recordkeeping Requirements

Before completing any Send money transfer, agent must verify the client's identity by examining a valid government issued photo identification that contains the person's name and address, such as a driver's license, passport or other government-issued ID card.

MetraPay must record information regarding money transfer transactions of \$3,000 or more, (\$1,000 or more in some states). All MetraPay transaction records must also be maintained in the online remittance system. These records should be readily accessible if your MetraPay is examined/audited by regulators.

Both sending and receiving agents must obtain and record specific information for money transfers of \$3,000 or more regardless of the method of payment. For money transfer Sends and / or Receives of \$3,000 or more, agent must obtain and record all of the information requested on the online Send/Receive form, including:

- Name
- Address
- Photo of Valid government issued photo ID
- Date of birth
- Occupation
- Transaction date

The maximum send amount per transaction is \$10,000. MetraPay limits customers to a daily maximum aggregated or combined send total of \$20,000.

Third Party Transaction Requirements

If an agent knows that a client is sending or receiving a transaction on behalf of someone else, then the agent must also obtain similar information on that other person. Examples of this could be a relative of an elderly person conducting a receive transaction for the elderly person or an employee for a business conducting the transaction for the business.

Currency Transaction Reporting (CTR) Requirements

MetraPay must file a CTR with the federal government for any transaction greater than \$10,000 in cash in one day. The CTR must be filled within 15 days of the transaction. Agents must treat multiple cash purchases of money orders or money transfers as a single transaction if they have knowledge that they are by or on behalf of the same person and total over \$10,000 during one business day. MetraPay must keep a copy of each CTR for at least five (5) years.

Structuring

Structuring is the illegal act of breaking up a larger transaction into smaller transactions in order to avoid the recordkeeping or reporting requirements. Many money launderers are familiar with the dollar thresholds that require recordkeeping and reporting. Therefore, in order to remain anonymous and avoid the detection of law enforcement officials, they will “structure” their transactions so that the recordkeeping or reporting requirements will not be triggered. Structuring is the act of breaking up a potentially large transaction into several smaller ones to avoid reporting or recordkeeping requirements.

It is illegal for MetraPay customers or agents to structure transactions in order to avoid the recordkeeping or reporting requirements. For example, if a client sends a \$1,500 money transfer in the morning and another \$1,500 money transfer send transaction in the afternoon, he may be structuring his purchases in order to avoid the \$3,000 recordkeeping requirements.

It is also illegal for MetraPay agents or employees to assist anyone in structuring transactions to avoid recordkeeping or reporting requirements. For example, employee or agents may not tell or even imply to a client that they can avoid providing information by conducting a smaller transaction. Some criminals may attempt to trick employees into allowing them to structure transactions by splitting up their activity with several accomplices or by trying to “con” employees with a hard luck story. Employees and agents need to be on the lookout for structuring so that they can prevent it from occurring.

Civil and Criminal Penalties

The government can impose severe penalties against individuals and businesses for violating money laundering laws and regulations. The criminal penalties for an individual can include as much as \$500,000 in fines, up to 10 years of imprisonment, and the loss of business. The government requires strict compliance with these laws and regulations. MetraPay will immediately cancel the contract of any agent or terminate any employee who knowingly or negligently fails to comply with the laws and regulations.

Suspicious Activity

Suspicious activity involves transactions that appear to be structured or do not have any legitimate purpose. You must file a Suspicious Activity Report by Money Services Business (SAR-MSB) on suspicious activity that involves at least \$2,000. Suspicious Activity can vary from one transaction to another based upon all of the circumstances surrounding the transaction or group of transactions. For example, transactions by one client may be normal, because of your knowledge of that client, while similar transactions by another client may be suspicious. Many factors are involved in determining whether the transactions are suspicious, including the amount, the location of your business, comments made by your client, the client's behavior, etc. That is why it is important for you to read this Guide in order to help detect suspicious activity and structured transactions.

The federal government requires filing of a Suspicious Activity Report by Money Services Business (SAR-MSB) for any transaction – or pattern of transactions – that is attempted or conducted with at least \$2,000, that you know, suspect or have reason to suspect:

- Involves funds derived from illegal activity or is intended to hide funds derived from illegal activity;
- Is structured to avoid recordkeeping or reporting requirements;
- Has no business or apparent lawful purpose; or
- Facilitates criminal activity.

MetraPay Compliance Officer may file a SAR-MSB on suspicious activity below \$2,000, but the regulations do not require it. MetraPay Compliance Officer must file a SAR-MSB within 30 days of detection of the suspicious event. The SAR-MSB must be mailed to the address on the SAR form. MetraPay must keep a copy of each SAR-MSB for at least five (5) years. Employees or agents must never tell the customer that MetraPay Filed a SAR-MSB. It is illegal to tell your customer that you are filing a SAR-MSB

The following guidelines quantify the types of suspicious activities that MetraPay will monitor for.

Suspicious Activity Examples

1. A customer says that he wants to send \$4,000 and wants to pay in cash. When you tell the customer that you need to collect his personally identifying information, he asks what amount he can send without showing you his ID. You must file a SAR-MSB on the transaction or attempted transaction.

2. A customer comes in several times on the same day to send money transfers which add up to more than \$10,000. You must file a CTR, if the customer paid more than \$10,000 in cash for the transfers. You should also determine whether a SAR-MSB needs to be filed.
3. A customer sends a \$4,400 money transfer. The next day, the customer sends \$9,400 to the same person. The customer may be structuring his transactions in order to avoid the CTR reporting requirements. You should consider whether a SAR-MSB should be filed.
4. A customer conducts transactions that are unusually large based on their past history, employment, or level of income.
5. A customer asks an employee how to avoid a reporting requirement.
6. A customer threatens or bribes an employee in order to avoid providing information.

The Compliance Officer will file SARs for amounts less than those specified above, if he or she has reason to believe the transaction is tied to an illegal activity.

Enhanced Due Diligence for New Accounts

One of the best ways for MetraPay to avoid being an unknowing accomplice to money launders is to properly identify new customers, when their account is opened. Accordingly, the minimum identification requirements for opening a new account are listed below. If a customer refuses or is unable to provide the requested information within ten (10) business days of opening his or her account, the account will be closed.

The minimum Customer Identification Requirements for new MetraPay customer requires one of the following forms of identification with a picture:

1. U. S. drivers license
2. International Passport
3. Alien registration card

Enhanced Due Diligence – Other Factors

1. Customers that request transfers with \$5,000 or more in cash will be asked to substantiate the legitimacy of the funds. If the customer can't provide sufficient proof (e.g., a payroll stub, a withdrawal receipt from another bank), the transfer will not be processed.
2. Customers that asked to be excluded from CTR reporting will be reported to FinCen via an SAR. Also, their account will be closed.
3. Customers that refuse to provide the necessary information for filing a CTR will be reported to FinCen via an SAR. Also, their account will be closed.

Procedures for Detecting Money Laundering

MetraPay has a computer system, The Remittance Transaction Monitor (RTM), that will enable it to detect most instances of money laundering. The Compliance Officer will print and maintain reports produced by the system to substantiate his opinion that specific activity is, or is not, suspicious.

In addition to using the RTM, all MetraPay employees will receive training once a year on how to identify money laundering operations. (New employees that have direct contact with customers will receive initial training within the first four weeks of employment.) As a part of the training, each Officer or Agent will be given a laminated card that identifies ways to detect and prevent money laundering. Replacement cards will be available from the Compliance Officer.

Office of Foreign Assets Control (OFAC)

OFAC is part of the U.S. Department of the Treasury and is responsible for enforcing U.S. government sanctions programs against countries, organizations and individuals. Sanctions programs typically involve blocking assets to further national security. Many of the sanctioned individuals, commonly referred to as “SDNs,” are drug dealers and terrorists. All U.S. entities are prohibited from conducting any financial transactions with SDNs. You can learn more about OFAC by visiting the Treasury Department’s website at www.ustreas.gov/offices/enforcement/ofac. The site also includes an extensive list of questions and answers to common questions regarding OFAC.

MetraPay has computer programs, Remittance Transaction Monitor (RTM), that review all money transfer senders and receivers against the government watch lists. The RTM will automatically flag transactions matched to SDNs for review by the Compliance Officer. If there are enough similarities, the Compliance Officer can contact the OFAC hotline at 1-800-540-6322 for verification. Unless a transaction involves an exact match, it is recommended that you contact OFAC Compliance before actually blocking transfers/assets.

Terrorist Financing Prevention

Money laundering is most commonly associated with drug dealing and tax evasion, however, terrorists often attempt to launder money in order to conceal their identity and finance their operations. It is critical that MSBs remain alert for any such activity, and take appropriate and immediate action if detected.

If you suspect terrorist financing, you should immediately report the incident to the FinCEN hotline at 1-800-556-3974, which is operated 24 hours a day, seven (7) days a week. You should also file a SAR-MSB on any suspected terrorist activity.

The Financial Action Task Force (FATF) and FinCEN have both issued guidance on financial transactions that may be indicative of terrorist financing at www.fatf-gafi.org and www.finen.gov. Some examples include, but are not limited to:

1. Movement of funds through a country designated by FinCEN or the FATF as “non-cooperative,” that are identified as specially designated nationals by OFAC, or that appear on the United Nation’s list of blocked accounts;
2. Multiple transactions conducted by a group of nationals from countries associated with terrorist activity;
3. Individuals acting on behalf of another money transmitting business that use MetraPay to transfer funds to multiple locations. This may be indicative of unlicensed money transmitters that seek to evade use of the banking system to conduct foreign transfers.

Procedures for Monitoring Compliance with this Policy

A minimum of once a year, MetraPay’s internal auditor or an independent third-party will review the Compliance Officer’s suspicious activity file. The auditor will ensure that all identified suspicious activity was reviewed and appropriately handled. The auditor will also use the Remittance Transaction Monitor System to search for suspicious activity that the Compliance Officer may have missed.

Compliance Officer Training and Responsibilities

MetraPay must designate a Compliance Officer. The Compliance Officer may be an employee who has other duties in the business, but it must be someone in a responsible position. The Compliance Officer is responsible for the business’s day-to-day compliance with the anti-money laundering laws and regulations, and for ensuring the compliance program is updated as needed.

The Compliance Officer is also responsible for overseeing the business’s ongoing education and training program. The Compliance Officer will be responsible for assuring that:

- Policies and procedures are followed
- Procedures are updated as needed
- Training and education are provided
- Reports are properly filed

The MetraPay Compliance Officer will be required to attend two (2) one-day training classes per year. He or she will get to choose the relevant training. The Compliance Officer will also be allowed to subscribe to a BSA newsletter service.

Submission of SAR or CTR by Compliance Officer

The MetraPay Compliance office will leverage the **FinCEN form 109** “Suspicious Activity Report by Money Services Business” to submit an SAR to Financial Crimes Enforcement Network, This form can be located at this address on the IRS website - https://www.irs.gov/pub/irs-tege/fin109_sarmsb.pdf

The Compliance office will leverage the **FinCEN form 104** “Currency Transaction Report” to submit a CTR to Financial Crimes Enforcement Network, This form can be locate at this address on the IRS website https://www.irs.gov/pub/irs-tege/fin104_ctr.pdf

The original copy of CTR must be filed within 15 days of the day of the transaction to:

IRS Detroit Computing Center
Attention: CTR
PO Box 33604
Detroit, MI 48232-5604

A SAR-MSB is a separate requirement from a CTR. Even if you have filed a CTR on a transaction or set of transactions you must also file a SAR-MSB, if you believe the activity is suspicious. Additional examples of potentially suspicious activities involving MSB services can be found at www.fincen.gov/msb_prevention_guide.pdf

Note: Original copy of the SAR-MSB must be filed within 30 days of becoming aware of the activity to:

IRS Detroit Computing Center
Attention: SAR-MSB
PO Box 33117
Detroit, MI 48232-5980

Employee Training and Responsibilities

MetraPay must establish an ongoing training program for all employees who will have any involvement with MSB activities. The educations and training should include instructions on the employees’ responsibilities under the program, as well as the detections of suspicious transactions.

All employees should be required to read this Guide prior to conducting any MSB transactions. In addition, employees should sign this MetraPay Compliance Program or another form of training documentations that is kept in their personnel file. Employees should also receive periodic updates to their training, particularly when there are changes in regulations.

Internal Suspicious Activity Tracking Report

To: (MetraPay compliance officer name goes here):

The following customer has been identified by the MetraPay's compliance system as possibly being involved in money laundering.

Customer name: _____.

Customer account number: _____.

You are the Officer/Agent assigned to work with this customer. The board of directors of MetraPay has assigned you the responsibility of investigating this customer's suspicious activity. This form must be completed and returned to the bank's Compliance Officer by / /

Please answer the following questions for this customer. If necessary, you may contact the customer. However, under no circumstances are you to tell the customer his or her transaction(s) are being investigated for money laundering.

1. Please attach a written summary that describes the circumstances that resulted in this customer having the following transaction(s).

2. Does MetraPay have another customer in this same business, that has comparable transactions? yes: _____ no: _____ .

3. If Yes, please identify: Name: _____

Account number: _____

4. Please attach a written summary that explains why you feel that an SAR should or should not be filed for this customer.

Note: please be advised that "willful blindness" by an officer of money laundering activities is a crime under 18 U.S.C. 1956 & 1957, punishable by fines of up to \$500,000 and incarceration of up to five years.