Anti-Money Laundering (AML) Compliance Manual

This Anti-Money Laundering ("AML") and Bank Secrecy Act ("BSA") Compliance Manual describes the policies, procedures, and internal controls that ADPAYGO ("Absolute M Transfer", "the Company", "we", "us") follows to detect and prevent money laundering, terrorist financing, and other financial crimes. It is written to reflect the actual functions built into our money-services system and is designed to satisfy the requirements of FinCEN, the U.S. Office of Foreign Assets Control (OFAC), and the Florida Office of Financial Regulation (OFR). This manual was last updated on January 1, 2026.

Every employee, agent, and officer must read, understand, and follow this manual. Failure to follow these procedures may result in disciplinary action, and violations of the BSA can carry serious civil and criminal penalties for both the Company and the individual.

1. Legal framework

As a registered Money Services Business ("MSB") and licensed money transmitter, Absolute M Transfer is subject to:

- The **Bank Secrecy Act (BSA)** and its implementing regulations (31 CFR Chapter X);
- The **USA PATRIOT Act**, including customer identification and information-sharing rules;
- **FinCEN** registration, reporting (CTR, SAR), and recordkeeping requirements;
- **OFAC** economic sanctions programs and the Specially Designated Nationals (SDN) list;
- **Florida Chapter 560** (Money Services Businesses) and Florida OFR licensing rules;
- The **Remittance Transfer Rule (Regulation E, Subpart B)** for consumer disclosures and receipts.

2. Registration and licensing

Absolute M Transfer maintains its FinCEN MSB registration and its Florida money-transmitter license current at all times, and renews them on schedule. Copies of the registration, license, and related regulatory records are stored in the **Legal Documents → Compliance & Audit Records** area of the system so they can be produced quickly during an examination.

3. The AML Compliance Officer

The Company designates a qualified **AML Compliance Officer** who is responsible for the day-to-day operation of the AML program. The Compliance Officer's duties include:

- Keeping this manual up to date and making sure the program is followed;
- Reviewing transactions that the system places **In Review**, and approving, holding, or rejecting them;
- Investigating possible OFAC/sanctions matches flagged by the system;
- Filing Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) with FinCEN on time;
- Making sure every employee completes AML training and records their acknowledgment;
- Arranging the independent review of the program.

In the system, the Compliance Officer holds the **Compliance Officer** role, which grants access to the review queue, the OFAC/sanctions tools, the audit log, and the compliance records.

4. The pillars of our AML program

Our program is built on the required pillars: (1) a designated Compliance Officer; (2) written policies, procedures, and internal controls (this manual and the system controls described below); (3) ongoing employee training; (4) independent testing/review; and (5) risk-based customer due diligence.

5. Customer identification and KYC

Before we process transactions, we identify our customers using the **Customers** module of the system. For each customer we collect and store:

- Full legal name, residential address, date of birth, and phone/email;
- A government-issued photo identification number (driver's license, state ID, passport, or consular ID), including the issuing authority and expiration date;

- Occupation and, where relevant, Social Security or tax identification number.

Staff use the **ID capture / document upload** feature to store a clear image of the customer's identification and any supporting documents directly on the customer record. Identification must be current (not expired) and must match the person conducting the transaction. Customer records are retained and can be searched at any time.

6. Customer due diligence (CDD) and enhanced due diligence (EDD)

We apply a risk-based approach. For most customers, standard due diligence (verifying identity and understanding the expected type and size of activity) is sufficient. We apply **enhanced due diligence** — asking additional questions about the source and purpose of funds and, where appropriate, requiring senior/compliance approval — when we see higher-risk indicators, such as unusually large amounts, frequent transfers just under reporting thresholds, transfers to higher-risk destinations, or a customer who is reluctant to provide information.

7. OFAC and sanctions screening

The system screens the names of senders and recipients against the OFAC Specially Designated Nationals (SDN) list and other sanctions lists using the built-in **OFAC / Sanctions** tools. Screening happens when a transaction is created, and staff can also run a name check on demand. The sanctions lists stored in the system are kept up to date.

If the system reports a possible match, the transaction is **stopped** and referred to the Compliance Officer, who reviews the details to decide whether it is a true match or a false positive. We do **not** process any transaction involving a confirmed sanctioned party, and we take the actions required by OFAC (including blocking or rejecting funds and reporting to OFAC) when required.

8. Transaction monitoring, signatures, and the review queue

All transactions flow through the **Transactions** module and move through clear statuses (for example Pending, Processing, In Review, In Hold, Sent, Paid, Cancelled, Defective, and Corrected), so activity can be tracked from start to finish.

Two important internal controls are built into the system:

- **Customer signature on the receipt.** Every transaction is signed by the customer (the "Sign Receipt" step) before it is completed, creating a signed record of the

transaction and the required disclosures.

- **Compliance review at $3,000 and above.** Any transaction of **US$3,000 or more** is first signed by the customer and then automatically placed **In Review**, so the Compliance Officer examines it before it is released. This also supports the funds-transfer ("Travel Rule") recordkeeping requirements that apply at the $3,000 level.

9. Currency Transaction Reports (CTR)

When a customer conducts one or more **cash** transactions that together exceed **US$10,000 in a single business day**, the Company must file a Currency Transaction Report (FinCEN Form 112) within 15 days. The system flags transactions where the funding method is cash and the total reaches the **$10,000** threshold so staff and the Compliance Officer are alerted. Staff must never help a customer break a large amount into smaller amounts to avoid this report — this is illegal "structuring" and must be reported.

10. Suspicious Activity Reports (SAR)

The Company files a Suspicious Activity Report (FinCEN Form 111) when it knows, suspects, or has reason to suspect that a transaction of **US$2,000 or more** involves funds from illegal activity, is designed to evade the BSA, has no lawful or business purpose, or involves the use of the Company to facilitate criminal activity. SARs are filed within **30 days** of detection. SAR filings are **strictly confidential**: employees must never tell a customer that a SAR has been or may be filed. Any employee who notices a red flag must report it to the Compliance Officer immediately.

11. Recordkeeping and the audit log

We retain all required records for at least **five (5) years**. This includes transaction records, customer identification and documents, signed receipts, CTR and SAR filings, and funds-transfer records of $3,000 or more. The system's **Audit Log** records key actions taken by staff (who did what and when), which gives us a reliable, tamper-resistant history for examiners. Regulatory documents (license, registration, contracts) are kept in the **Compliance & Audit Records** area.

12. Batches, payers, and agents

Outgoing payments are organized through the **Batches** and **Payers** modules, and each batch shows the paying bank and payment details so funds are sent correctly and can be reconciled. Business is also conducted through **Agents**. All agents are expected to follow this manual, complete AML training, and apply the same

identification and screening steps. The Compliance Officer oversees agent activity and reviews it as part of the program.

13. Foreign currency and reais purchases

Purchases of foreign currency (including Brazilian reais) are recorded in the **Reais Purchases** module, and the related bookkeeping is captured in the **Accounting** module. These records support accurate exchange-rate handling and a clear audit trail of the Company's own funding activity.

14. Employee training

All employees and agents complete AML/BSA training through the system's **Training** module when they are hired and at least once every year. Training covers how to identify customers, how to spot red flags, the CTR and SAR rules, OFAC screening, and how to use the controls described in this manual. Each person records an **acknowledgment** that they completed the training, and these acknowledgments are stored as part of our records.

15. Independent review

The Company arranges an **independent review** of the AML program on a periodic basis (at least every 12–18 months, based on risk). The review is performed by someone who is not the Compliance Officer and does not report to that person. The results are documented, shared with management, and any weaknesses are corrected promptly.

16. Red flags to watch for

- A customer who refuses to provide identification or gives information that seems false;
- Transactions structured to stay just under $3,000 or $10,000;
- A customer who seems to be sending money on someone else's behalf or being directed by another person;
- Unusual concern about reporting or recordkeeping requirements;
- Transfers that do not match the customer's known profile or stated purpose;
- A sender or recipient whose name may match a sanctions list.

When in doubt, staff must escalate to the Compliance Officer before completing the transaction.

17. Consumer disclosures and receipts

For remittance transfers we provide the disclosures and receipts required by the Remittance Transfer Rule, including the transfer amount, fees, exchange rate, the amount to be received, and the customer's cancellation and error-resolution rights. The signed receipt generated by the system is retained as part of our records.

Questions? Contact us

If you have questions or concerns about this document, please contact us:

- **Phone:** 407-555-6677
- **Mail:** ADPAYGO, ATTN: Customer Service, Miami, FL

© 2026 Absolute M Transfer. All rights reserved.

An · Phone: (689) 351-7171

Use · Mail: ADPayGo, 5605 International Dr, Orlando, FL 32819