

## BSA/AML/OFAC Policy

### General Policy Statement:

Altamaha Federal Credit Union's comprehensive Bank Secrecy Act (BSA) / Anti-Money Laundering (AML) Program will include internal policies, procedures, and controls designed to comply with the USA PATRIOT Act of 2001 (PATRIOT Act), the BSA, the Currency and Foreign Transactions Reporting Act, OFAC rules, the Anti-Money Laundering Act of 2020, and all related laws and regulations in order to combat money laundering, terrorist financing, tax evasion and other financial crimes.

### Definitions:

1. **Money Laundering.** Money laundering is the criminal practice of processing "dirty" money through a series of transactions in order to "clean" the funds so that they appear to be proceeds from legal activities. It may not involve currency (cash) at every stage of the laundering process, and generally involves three independent steps (that can occur at the same time):
  - A. **Placement:** Structuring currency deposits in amounts to evade reporting requirements, or commingling currency deposits of legal and illegal activities. Examples:
    - i. Large number of deposits below the reporting threshold.
    - ii. Depositing a refund check from a canceled vacation package or insurance policy.
    - iii. Buying a series of monetary instruments that are collected and deposited at another location.
  - B. **Layering:** Moving funds around the financial system, often in a complex series of transactions. Examples:
    - i. Exchanging monetary instruments for larger or smaller amounts.
    - ii. Wiring or transferring funds to and through numerous accounts in one or more financial institutions.
  - C. **Integration:** Creating the appearance of legality through additional transactions. Example:
    - i. The purchase and resale of real estate or other assets.

2. **Terrorist Financing.** Activities financing a terrorist organization are often funded through legitimate sources, such as: (1) charitable donations; (2) business ownership; and/or (3) personal employment.

**Guidelines:**

1. **COMPLIANCE CULTURE.** To ensure the Credit Union has a strong compliance culture the Financial Crime Enforcement Network's (FinCEN) guidance will be followed, including:
  - A. The Board of Directors, executive and senior management will actively support, understand and be engaged in compliance efforts;
  - B. Managing and mitigating BSA deficiencies and risks will not be compromised by revenue interests;
  - C. Relevant compliance information will be shared throughout the Credit Union;
  - D. Adequate human and technological resources will be devoted to compliance functions;
  - E. Credit Union leadership and staff will understand the purpose of BSA efforts and reporting; and
  - F. The BSA compliance program will be tested by an independent and competent party.
2. **BSA/AML COMPLIANCE PROGRAM.** The Board of Directors will approve the BSA/AML Compliance Program and any changes to it with corresponding documentation in the Board minutes.
  - A. **Compliance Officer.** The BSA/AML/OFAC Compliance Officer (BSA Officer), appointed by the Board, will (i) act as the primary contact person with any applicable federal agency, (ii) periodically review and update the BSA/AML Compliance Program, (iii) ensure that daily transaction records are received and determine if the required reports have been timely and accurately filed and appropriate actions taken; (iv) ensure that staff complies with the BSA/AML requirements; and (v) ensure that adequate record retention procedures are in place.
  - B. **Risk Assessment.** The BSA Officer will oversee the performance of the Credit Union's risk assessment, which identifies and measures the degree of risk for each of the Credit Union's products, services, members and geographic locations, along with the steps that have been taken to mitigate the risks. The risk assessment will be performed at least every 12 to 18 months.

- C. **Internal Controls.** The BSA Officer will develop and implement a system of internal controls and procedures under the oversight of the CEO. The Credit Union's internal controls consist of monitoring, reporting and recordkeeping.
  - D. **Training.** The Credit Union will provide periodic training for employees whose responsibilities involve transactions covered by the BSA, PATRIOT Act, and applicable regulations relevant to their job duties. The Credit Union will also provide periodic training for the Board of Directors and committee members relevant to their volunteer duties. The BSA Officer will ensure that the appropriate staff, including new hires, receives training and that records documenting the training are kept.
  - E. **Audit.** The Credit Union will coordinate an audit which will include independent testing and auditing of the Credit Union's BSA/AML Compliance Program and Customer Identification Program in the annual internal review plan and report its findings to the Board of Directors. This audit will be performed at least every 12 to 18 months.
3. **MONITORING.** The Credit Union will enact procedures to monitor and identify unusual activity.
- A. **Member Due Diligence.** As part of the monitoring process, the Credit Union will enact a member due diligence program in order to: (a) predict the types of transactions in which a member is likely to engage; and (b) determine when transactions are potentially suspicious. This program will be risk-based and will allow the Credit Union to understand the nature and purpose of the member relationship.
  - B. **High Risk Members.** For high risk members, the Credit Union will obtain the following information at account opening and throughout the relationship:
    - i. Purpose of the account.
    - ii. Source of wealth and funds.
    - iii. Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors.
    - iv. Member's (or beneficial owner's) occupation and type of business.
    - v. Financial statements.
    - vi. Residence (if a business, where it is incorporated).
    - vii. Proximity of residence, place of employment or business to the Credit Union.

- viii. Whether international transactions are expected to be routine.
- ix. Explanations for changes in account activity.
- x. Description of business operations, anticipated volume of currency and sales.
- xi. References.

C. **Correspondent and Private Banking Accounts.** The Credit Union does not offer correspondent or private banking accounts.

D. **Money Service Businesses (MSBs).** MSBs include any person doing business, regardless of whether on a regular basis, in one or more of the following: money orders, travelers checks, money transmissions, check cashing and currency dealing or exchange. Must conduct more than \$1,000 in business with one person in one or more transactions on any one day. However, NO activity threshold applies to money transmitters.

As a practice, the credit union will not open accounts for MSB's. However, the credit union will identify cash intensive businesses and routinely verify by the methods below that they do not qualify as an MSB under the definition above.

- i. The Credit Union will review FinCEN's website <https://www.fincen.gov/msb-registrant-search> to determine whether an MSB is required to register, has in fact, registered or renewed its registration.
- ii. Have the accountholder complete an MSB Questionnaire and certify that they do not qualify as an MSB.

E. **Legal Entity Members.** The Credit Union does not offer business accounts to legal entities. However, the Credit Union does offer individuals DBA accounts.

A legal entity customer does not include sole proprietorships, unincorporated associations, or natural person opening accounts on their own behalf. DBA customers/members are excluded from the beneficial ownership rules but all commercial customer/members, including DBA's must be reviewed for unusual activity.

- i. **Beneficial owners** as listed above, means each individual who directly or indirectly (through any contract, arrangement, understanding, relationship or otherwise) owns 25% or more of the equity interests of the legal entity and a single individual with significant responsibility to control, manage, or direct the legal entity (e.g., CEO, CFO, COO, General Partner, etc.). If a Trust is an owner, the beneficial owners would be the Trustee(s).

- ii. Unless otherwise excluded, **legal entity**, as used above, includes a corporation, limited liability company, or other entity created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction.
- iii. If a DBA customer/member is found to have unusual activity, the Credit Union will determine if the owner of the DBA is:
  - 1. Owner of any other accounts, and
  - 2. A beneficial owner of a commercial entity legally chartered in the state of Georgia.
- iv. The Credit Union will review such other accounts for unusual activity and will determine, to the best of its ability, the nature of any other legal entities of which the DBA owner is a beneficial owner.

F. **Monitoring System.** The Credit Union will monitor activity through its core processing system. The Credit Union will ensure, as part of the monitoring process, that it maintains current information about its members. It will conduct ongoing monitoring to identify and report suspicious transactions and will update member information on an as-needed basis, based on risk-based procedures.

#### 4. REPORTING

A. **CURRENCY TRANSACTION REPORT (CTR).** The Credit Union will complete and electronically file a FinCEN CTR, each time a nonexempt member withdraws, transfers, makes a payment with, or deposits cash (currency or coin) of more than \$10,000 within 15 days of the transaction. Multiple transactions by or on behalf of one person in one business day will be consolidated and reported as if the total exceeds \$10,000. A copy of the electronically filed FinCEN CTR will be retained for five years.

- i. CTRs are **not** required to be filed for transactions involving U.S. depository institutions; or federal, state or local government (or any entity exercising governmental authority). As part of the Credit Union's Customer/Member Identification Program (CIP/MIP), the Credit Union will ensure the member's initial eligibility for this exemption and will document the basis for its conclusions.
- ii. **Exemptions – Phase I.** A CTR is not required for transactions involving most corporations or other publicly traded entities (such as partnerships), which are listed on the New York Stock Exchange, the American Stock Exchange, or NASDAQ. In order to obtain the exemption, the Credit Union will file a

Designation of Exempt Person (DEP) form with the U.S. Department of Treasury within 30 days after the first transaction in currency that the Credit Union wishes to exempt.

1. The Credit Union will closely scrutinize members requesting exempt status to ensure that information received from the member is current and reliable, as failure to investigate the member exposes the Credit Union to liability for contributing to the success of a criminal enterprise.
2. At least once per year, the Credit Union will review the eligibility of an exempt member to determine whether such member remains eligible for an exemption. Management will maintain a current list of all members whose transactions are exempt. The list shall include the following information: (a) Member's name, (b) Address, (c) Type of business, and (d) Account number. Tellers must check the exempt list each time a member deposits or withdraws more than \$10,000 (currency and coin). **If members are not exempt, tellers must complete a CTR.**

iii. **Exemptions – Phase II.** For members who qualify as either “non-listed businesses” or “payroll customers,” the Credit Union will file the FinCEN Designation of Exempt Person (DEP) form within 30 days after the first transaction in currency the Credit Union wishes to exempt. To qualify, the member must: (1) maintain an account with the Credit Union for at least two months (or is granted an exception based on a risk-based analysis of the legitimacy of the member's transactions that has been conducted); (2) “frequently engage” in transactions in currency in excess of \$10,000 (which means having actually conducted five (5) or more reportable cash transactions in each full year following the member's initial designation); **and** (3) be incorporated under the laws of the U.S. or any state.

1. At least once per year, the Credit Union will review the eligibility of an exempt member to determine whether such member remains eligible for an exemption. The Credit Union will maintain a system of monitoring the transactions in currency of each exempt customer for any reportable suspicious activity.
2. Certain businesses are *ineligible* for treatment as an exempt non-listed business. Members who engage in multiple business activities may qualify so long as no more than 50% of its annual gross revenues are derived from one or more ineligible business activities. In these cases, the Credit Union will make a reasonable determination based

on its understanding of the nature of the members' business; the purpose of the member's accounts; the actual or anticipated activity in those accounts; or by obtaining additional supporting materials (i.e., tax returns and/or unaudited financial statements). Ineligible activities include the following:

- a. Serving as a financial institution or as agents for a financial institution of any type;
  - b. Purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment or mobile homes;
  - c. Practicing law, accounting or medicine;
  - d. Auctioning or pawning of goods;
  - e. Chartering or operation of ships, buses or aircraft;
  - f. Engaging in gaming (other than licensed pari-mutuel betting at race tracks);
  - g. Engaging in investment advisory services or investment banking services;
  - h. Engaging in real estate brokerage, title insurance activities or real estate closings;
  - i. Engaging in trade union activities; or
  - j. Engaging in any other activity that may, from time to time, be specified by FinCEN.
- iv. At the time a member's ineligibility is discovered, the Credit Union will document its determination of ineligibility and will cease to treat the member as exempt.
- v. **Shared Branch Network.** The Credit Union is a participant in the Shared Branch Network. Credit unions participating in the network are called shared branches. Shared branches handling the cash and coin deposits must verify the identity of the person conducting the transaction and note identifying information, such as driver's license number on the receipt or voucher. Shared branches, by nature of the shared branch agreement, do not issue more than \$2,500.00 in cash to any member on the Credit Union's behalf.

If a member (or someone transacting on the member's behalf) makes a transaction in excess of the CTR filing threshold, the shared branch shall be responsible for

completing the CTR and immediately providing a copy to the Credit Union. The Credit Union shall identify, through its routine review of cash transaction reports, any shared branch network transactions that have not been properly reported to the Credit Union and contact the shared branch for the needed CTR. In either case, it shall be the Credit Union's responsibility to timely file the required CTR.

Likewise, if the Credit Union determines, through its routine review of cash transaction reports, that a member has exceeded the CTR filing threshold by using multiple shared branches in a single day, the credit union will collect the needed information and will timely file the required CTR.

- B. **SUSPICIOUS ACTIVITY REPORT (SAR).** The Credit Union will complete and electronically file a SAR whenever the Credit Union knows or has reason to suspect that any crime or suspicious transaction related to money laundering or a violation of the BSA has occurred. A copy of the electronically filed form, along with any supporting documentation, will be retained for five years.

The Credit Union will report any crime or suspected crime and any suspected computer intrusion electronically using the FinCEN Suspicious Activity Report (SAR), within thirty (30) days after discovery. If no suspect can be identified, the Credit Union may use an additional thirty (30) days to file the report. For suspicious activity that continues, the Credit Union should be filing a SAR at least every 90 days to report that information to law enforcement.

For questions regarding suspicious activity that require immediate attention, call the BSA Regulatory Helpline at 800.949.2732, or to report suspicious transactions that may relate to terrorist activity the Credit Union should call the Financial Institutions Toll-Free Hotline at 866.556.3974 (7 days a week, 24 hours a day) and immediately notify an appropriate law enforcement authority in addition to filing timely a SAR. The Credit Union will maintain a copy of each SAR that it files and the original of all attachments to the SAR for five years. To comply with Section 351 of the PATRIOT Act, except where such disclosure is requested by FinCEN or an appropriate law enforcement or supervisory agency, the Credit Union will not provide any information that would disclose that it prepared or filed a SAR and will cite 31 CFR 1020.320(e) and 31 USC 5318(g)(2)(a) for their refusal. The Credit Union should also notify FinCEN and the NCUA of any request. The Credit Union and any director, officer, employee, or agent of the Credit Union who files a voluntary or required SAR will be protected from liability for any disclosure contained in, or for failure to disclose the fact of such report.

- i. **Sharing SARs and SAR Information.** SARs are confidential. Therefore, the Credit Union will only disclose the SAR filing to fulfill responsibilities consistent with the BSA, such as to the appropriate law enforcement agency, regulator, and the Board, or its designated committee as outlined



in this policy. The Credit Union will not provide information or notification that a transaction has been reported to a person (even if listed above) if that person is involved in the suspicious transaction warranting the SAR.

1. The Credit Union may also share a SAR or SAR information with its affiliates (defined in the Credit Union's Privacy Policy), provided the affiliate is subject to SAR regulation. The Credit Union will ensure that its affiliates keep this information confidential. The Credit Union will **not** share SAR information with an affiliate when the Credit Union has reason to believe that the information may be disclosed to any person involved in the suspicious activity that is the subject of the SAR.
2. Officials, employees, and agents, whether subpoenaed or otherwise requested to disclose a SAR, or the information contained within it, must decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed, and notify FinCEN and the NCUA of the request.

ii. **Reportable Transactions.**

1. **Unusual or suspicious transactions**, such as deposits; withdrawals; transfers between accounts; exchange of currency; loans; extensions of credit; purchases or sales of any stock, bond, share certificate, or other monetary instrument or investment security; any other payments, transfers, or deliveries by, through or to a financial institution; or purchases of depository checks by non-members. The Credit Union will verify the identity of non-members purchasing such items using government-issued identity cards with pictures.
2. **Insider abuse involving any amount.** A SAR will be filed whenever the Credit Union knows, or has reason to suspect, that an official, employee or agent has committed, or aided in the commission of, a criminal violation, regardless of the amount involved.
3. **Transactions aggregating \$5,000 or more where a suspect can be identified.** If it is determined before filing the SAR that the identified suspect or group of suspects used an alias, the information regarding the true identity, as well as the alias identifiers (such as driver licenses or social security numbers, addresses and telephone numbers), will be reported.
4. **Transactions aggregating \$25,000 or more regardless of potential suspects.**

5. **Transactions aggregating \$5,000 or more that involve potential money laundering or BSA violations.** These will be reported when the Credit Union knows or has reason to suspect that the transaction (1) involves funds derived from illegal activities; (2) is designed to evade the BSA; or (3) has no business or apparent lawful purpose.
  - iii. **Exceptions to Reporting Requirement.** The Credit Union need not file a SAR for a robbery or burglary committed or attempted that is reported to the appropriate law enforcement authorities, or for lost, missing, counterfeit, or stolen securities that are reported pursuant to 17 C.F.R.240.17(f)(1).
  - iv. **SAR Decision-Making.** The Credit Union will document SAR decisions, including the specific reason for filing or not filing a SAR. This provides a record of the decision-making process, including the final decision for contemplating, but not filing a SAR.
  - v. **Report to Board or Designated Committee.** Management will notify the Board, or its designated committee, of the Credit Union's SAR activity at least monthly. The Board will be notified of SAR activity immediately if the activity warrants immediate reporting. If the suspect is a director or member of a committee designated by the Board, the Credit Union will only notify the remaining directors, or designated committee members, who are not suspects, or will merely report the number of SARs filed, without providing specific information. The report will provide sufficient information on SAR filings to allow for the Board or designated committee to fulfill their fiduciary duties, while being mindful of the confidential nature of the SAR.
- C. **INTERNATIONAL TRANSPORTATION OF CURRENCY AND/OR MONETARY INSTRUMENT REPORT.** The Credit Union will file a Report of International Transportation of Currency or Monetary Instrument Report (CMIR) if it sends or receives more than \$10,000 in currency or instruments into or out of the United States on its own behalf. The BSA does not require the Credit Union to file a CMIR with respect to currency or other instruments mailed or shipped through the postal service or by common carrier (armored car services), or the transfer of funds through normal banking procedures, which does not involve the physical transportation of currency or monetary instruments. The Credit Union will file the CMIR within 15 days after receipt (Recipients) of the currency or monetary instruments, with the Customs officer in charge at any port of entry or departure or by mail. The Credit Union will file the CMIR if the currency or other monetary instrument does not accompany the person (Shippers or Mailers) entering or departing the United States on or before the date of entry, departure, mailing, or shipping Reports will be filed through FinCen's website.
- D. **FOREIGN FINANCIAL REPORT.** The Credit Union will file a report of Foreign Bank and Financial Accounts Report (FBAR) Form through the BSA e-filing System on or before April 15 of each year for all Credit Union financial account relationships outside the

United States where the aggregate value exceeded \$10,000 during the previous calendar year. The Credit Union will retain FBAR forms for five years.

## 5. RECORDKEEPING

- A. **Cashier's Checks of \$3,000 To \$10,000 purchased with Currency.** The Credit Union will not issue or sell these items unless it verifies the identity of the purchaser. The Credit Union will treat multiple purchases as one purchase if it has knowledge that an individual purchases these items during one business day totaling \$3,000 or more. The Credit Union will record the following information in a monthly chronological log: (a) member name; (b) verification of member's identity; (c) account number; (d) date of purchase; (e) branch where the instrument was purchased; (f) type(s) of instrument(s) purchased; (g) serial number(s), and (h) dollar amount(s) of each instrument(s) purchased. Each Credit Union branch will maintain a separate log. By the fifteenth (15th) of each month, the branch logs will be sent to the BSA Officer to be maintained in a centralized location. The Credit Union will retain the logs for five years.
- B. **Certain Financial Transactions.** The Credit Union will prepare and retain records concerning account documentation and negotiable instruments as required by the BSA. This includes retaining records of: (a) each loan exceeding \$10,000 (except real estate), including the purpose of the loan; (b) certificate and account TINs; and (c) transactions concerning certain account and negotiable instruments. The Credit Union will fulfill these requirements as it makes and retains financial records in its ordinary course of business. The Credit Union will retain all records the BSA requires it to keep for a period of five years.
- C. **Legal Entity Member Records.** The Credit Union will retain records related to the identification of the beneficial owner(s) of the legal entity for 5 years after the date the account is closed. The Credit Union will retain records related to the verification of the beneficial owner(s) for 5 years after the record is made.
- D. **Wire Transfers.** All wire transfers of \$3,000 or more made via Fedwire will include the information below (funds transfers governed by the Electronic Fund Transfer Act, as well as any other funds transfers that are made through an automated clearinghouse, an automated teller machine (ATM), or a point-of-sale system, are excluded from this requirement):
- i. **Credit Union Originated Wire.** When the Credit Union originates a wire transfer, the Credit Union will retain the following: (a) name; (b) address; (c) amount of transfer; (d) date of transfer; (e) any payment instructions; (f) identity of beneficiary's financial institution; and (g) beneficiary's name, address and account number.
    1. **Travel Rule Requirement.** When submitting a transmittal order, the Credit Union will include the following information to the receiver:

- a. Name of transmitter and the account number of the transmitter (if the payment is ordered from an account);
    - b. Address of the transmitter;
    - c. Amount of the transmittal order;
    - d. Date of the transmittal order;
    - e. Identity of the transmitter's and recipient's financial institution;
    - f. As much of the following information of the recipient as possible (name, address, account number and any other specific identifier); and
    - g. Either the name and address or numerical identifier of the Credit Union.
  - ii. **Credit Union Received Wire.** When the Credit Union receives a wire transfer, the Credit Union will do the following: (a) retain a copy of the payment order; (b) verify the beneficiary's name and address; and (c) keep a record of the means used to verify the name and address, along with the person's social security number, alien ID or employee identification number (EIN).
6. **INFORMATION SHARING.** Sections 314(a) and 314(b) of the PATRIOT Act and regulations allow the Credit Union to provide information about specified accounts or transactions in response to requests from FinCEN, and to share information with other financial institutions. The Federal Bureau of Investigation (FBI) may send a National Security Letter (NSL), which will require the Credit Union to share any requested information in the possession of the Credit Union with the FBI.
- A. **Required Sharing with FinCEN – Section 314(a).** The Credit Union designates its BSA Officer as the FinCEN contact person. Upon FinCEN's request, the Credit Union will search its records for a specified individual or entity.
- i. **Certification.** Prior to FinCEN requesting information, the underlying federal law enforcement agency must provide FinCEN with a written certification, that the person named in the request is reasonably suspected, based on credible evidence, of engaging in money laundering or terrorist activity.
  - ii. **Record Search.** Upon receiving a FinCEN request, the Credit Union will search its records to determine whether it maintains or has maintained an account for, or has engaged in a transaction with, each named individual or entity. Unless otherwise specified in FinCEN's request, the search will cover:

1. Current accounts;
2. Accounts maintained/closed during the preceding twelve (12) months; and
3. Transactions and funds transfers conducted during the preceding six (6) months.

The Credit Union is not required to search any account holder's processed checks for payee information related to a named suspect.

- iii. **Report to FinCEN.** If the Credit Union finds an account or transaction identified with any individual, entity, or organization named in a FinCEN request, the Credit Union must report the match to FinCEN by completing the Subject Information Form. The Form only requires the Credit Union to place an "X" next to the particular named subject for which a match was found. The Credit Union will also provide point-of-contact information. The Credit Union will report this information to FinCEN within 14 days of the request via the Secure Information Sharing System (SISS).
  - iv. **Use and Confidentiality of Information.** The Credit Union will **not** use FinCEN information as the sole determination factor in filing a SAR or to determine whether to establish or maintain an account or to engage in a transaction. The Credit Union will **not** disclose to any person, other than FinCEN or the federal law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested information, except to the extent necessary to comply with the request. The Credit Union may share this information under its "Voluntary Information Sharing" policy set forth below. The Credit Union will maintain adequate procedures to protect the security and confidentiality of FinCEN information requests.
  - v. **Right to Financial Privacy Act.** Credit Union responses to FinCEN requests under this Information Sharing policy fall within permissible disclosure exceptions to the Right of Financial Privacy Act.
  - vi. **Documentation.** The Credit Union will store either the search verification document from the web-based 314(a) SISS or the Subject Response List for each transmission.
- B. **Voluntary Information Sharing – Section 314(b).** At this time, the Credit Union does not participate in the voluntary sharing of information as identified in Section 314(b).

- C. **Required Information Sharing with the FBI.** National Security Letters (NSLs) are investigative demands that may be issued by the local FBI office and other federal government authorities to obtain financial records from the Credit Union.
- i. **Security and Confidentiality.** NSLs are HIGHLY confidential, in that not even an examiner will review them. The Credit Union will create and maintain procedures to protect the confidentiality of the existence of any NSLs received. NSLs are NOT to be referenced in any SAR filings.
  - ii. **Questions.** Any and all questions related to an NSL are to be directed to the local FBI field office ONLY.
7. **PRODUCTION OF RECORDS.** In accordance with the PATRIOT Act, within 120 hours after receiving an NCUA information request related to its anti-money laundering compliance or a member or account signer, the Credit Union will provide or make available to NCUA, information and account documentation for any account opened, maintained, administered, or managed in the United States by the Credit Union.
8. **SPECIAL CONCERN TRANSACTIONS.** The PATRIOT Act authorizes the U.S. Treasury Department to issue regulations finding certain countries, areas, or persons to be of “special concern,” and the Credit Union will comply with any special record keeping and reporting requirements as applicable.
9. **CUSTOMER/MEMBER IDENTIFICATION PROGRAM (CIP/MIP).** The Credit Union will undertake reasonable risk-based measures, appropriate for its size and type of business, to (i) verify the identity of any person seeking to open an account, to the extent reasonable and practicable; (ii) maintain a record of the information used to verify the person’s identity, and (iii) determine whether the person appears on any list of known or suspected terrorists or terrorist organizations provided to the Credit Union by any government agency.

**A. Definitions.**

- i. Under the CIP/MIP, an “account” means a formal arrangement established to provide ongoing services or other financial transactions. It applies to traditional accounts such as a checking, share draft, share, certificate account, asset account, and any loan or other extension of credit. An “account” does **not** include a product or service where the Credit Union does not establish a formal relationship with the person, such as: check cashing, wire transfer, sale of a check or money order, an account acquired through acquisition, merger, purchase of assets or assumption of liabilities, or an account opened for an employee benefit plan established under the Employee Retirement Income Security Act of 1974.
- ii. A “customer” (“member” or “person”) includes individuals, and individuals who open a new account for corporations, partnerships, trusts, associations, etc. The

CIP/MIP requires identification verification for customers opening an account and for any individual(s) authorized to open an account for a corporation, partnership, trust, association, guardianship, etc. Both deposit and lending functions are considered account relationships.

**B. Identity Verification.** The Credit Union will create procedures to verify the identity of each member and person who opens an account, to the extent reasonable and practicable, to enable the Credit Union to form a reasonable belief that it knows the true identity of the member or person. If a member or person refuses or is unable to provide the requested information within 30 days of account opening, the account will be closed. Credit Union employees may refuse to open the account until identification to be verified is provided. If a provisional account is opened, the individual will have no access to it until identification is verified.

i. **Required Information.** The Credit Union will create procedures that specify the identifying information that the Credit Union will obtain from each member, beneficial owners of legal entity members or person opening an account. At a minimum, the Credit Union will obtain the following information from an individual or entity prior to opening an account:

1. Name (individual name) or (entity name & any assumed business name);
2. Date of birth (if individual);
3. Address:
  - a. Residence or principal place of business and mailing address (if individual);
  - b. Army Post Office (APO) or Fleet Post Office (FPO) box number or residential or business street address of next of kin or of another contact individual (if individual); or
  - c. Principal place of business, local office, or other physical location (if person is other than an individual, i.e., corporation, partnership, trust, estate, guardianship).
  - d. In states that have established an Address Confidentiality Program (ACP), if the individual participates, the street address of the ACP sponsoring agency.
4. Identification Number:
  - a. For a U.S. person, a TIN, SSN, ITIN, EIN.

b. For a non-U.S. person, one or more of the following:

- i. TIN, SSN, ITIN, EIN;
- ii. Passport number and country of issuance,
- iii. Alien identification card and number, or
- iv. Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing photograph or similar safeguard. If opening an account for a foreign business without an identification number, the Credit Union will request alternative government issued documentation certifying the existence of the business/enterprise.

ii. **Verification.** The Credit Union will follow risk-based procedures for verifying the identity of the member, using the information obtained within a reasonable time after an account is opened. The procedures will describe when the Credit Union will use documents, non-documentary methods, or a combination of both methods.

1. **Verification Through Documents.** For accounts opened in person, the Credit Union will verify the identity of each person or entity through the following documents:

- a. **For Individuals:** unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard (such as a driver's license or passport).
- b. **For Non-Individuals:** documents showing the existence of the entity (registered articles of incorporation or organization, government issued business license; or Partnership Agreement or trust instrument.) All non-individual accounts must have the identity of all beneficial owners of the entity identified and valid SSNs must be provided to the Credit Union prior to account opening.



2. **Lending Transactions.** To prevent fraud, the Credit Union will create procedures to verify member information against the applications it receives and ensure proper authentication of the identity of each individual filing an online loan application.
3. **Documentation.** The Credit Union will create procedures for making and maintaining a record of all verification information obtained. At a minimum, the record must include:
  - a. All identifying information about a member (person) obtained;
  - b. A description of any document that was relied on, 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;
  - c. A description of the methods and the results of any measures undertaken to verify the identity of the member (person); and
  - d. A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.
- iii. **Non-Documentary Verification Methods.** The Credit Union will use nondocumentary methods to verify a member's or person's identity in addition to, or instead of, identification documents, and will create procedures to specify when non-documentary verification methods will be used and the types of non-documentary methods to be used. These methods may include: contacting a member or person; independently verifying the member's or person's identity through the comparison of information provided by the member or person with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement.
- iv. **Verify Identifying Information on Existing Members.** The Credit Union will not verify information about an existing member seeking to open a new account, if it:
  - (a) previously verified the member's or person's identity in accordance with its policies and procedures;
  - (b) continues to have a reasonable belief that it knows the member's or person's true identity;
  - (c) the Credit Union has a reasonable belief that the member, previously identified, is the person who is opening the account; and
  - (d) the verification process is documented on the signature card or comment log within the account or loan file.
- v. **In some cases, identification will be required for current members if original documentation was not obtained with the original opening of the account.**

- C. **Lack of Verification.** If the Credit Union cannot form a reasonable belief that it knows the true identity of a member or person, the account will **not** be opened. Risk will determine final policy decisions when there is a lack of identification verification.
  
- D. **Record Retention.** The Credit Union will retain all identifying information about a member (person) or legal entity beneficial owner(s) obtained for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant. The Credit Union will retain for five years after the record is made:
  - i. A description of any document that was relied on, 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;
  - ii. A description of the methods and the results of any measures undertaken to verify the identity of the member (person); and
  - iii. A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.
  
- E. **Comparison with Government Lists.** The Credit Union will check member and authorized signer names against any list of known or suspected terrorists or terrorist organizations provided by any government agency and designated as such by the U.S. Treasury Department in consultation with Federal regulators. This determination will be made at account opening. If a person's name is on a list, the Credit Union will look to its OFAC procedures for the appropriate action. If there is a match, all further account action will be stopped, and the BSA Officer will be notified. Further investigating will be done before the account opening process resumes. If the Credit Union confirms a legitimate hit on any government list, the Credit Union will immediately notify the proper regulatory agency. The Credit Union will maintain documentation to show that it follows this process.
  
- F. **Notice.** The Credit Union will provide persons with notice that the Credit Union is requesting information to verify their identities, in a manner reasonably designed to ensure that a member or person is able to view the notice before opening an account.

For example, the Credit Union may post a notice in the lobby or on its website, include the notice on its account applications, or use any other form of written or oral notice. The Credit Union will use a notice substantially similar to the following:

- i. **IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT.** To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. What this means for you: When you open an account, we will ask for your name,

address, date of birth, and other information that will allow us to identify you. We also may ask to see your driver's license or other identifying documents.

- G. **Reliance on Another Financial Institution.** The Credit Union may create procedures which specify when the Credit Union will rely on the performance by another financial institution (including an affiliate) or any procedures of the Credit Union's CIP/MIP, with respect to any member of the Credit Union that is opening an account or has established a similar formal relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that:
- i. Such reliance is reasonable under the circumstances;
  - ii. The other financial institution is subject to a rule implementing 31 U.S.C. § 5318(h) and is regulated by a Federal functional regulator; and
  - iii. The other financial institution enters into a contract requiring it to certify annually to the Credit Union that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) the specified requirements of the Credit Union's CIP/MIP.

**Office of Foreign Assets Control (OFAC) Compliance Program.** The Office of Foreign Assets Control Department of the Treasury, is responsible for administering and enforcing a series of laws that impose economic and trade sanctions against targeted foreign governments, individuals, groups and entities in accordance with national security and foreign policy goals and objectives. Any transactions, such as transfers of funds, to or from these countries or to blocked persons are prohibited. The Credit Union is required to block such transfers and accounts and to furnish reports on all blocked accounts and rejected funds transfers to OFAC.

1. **COMPREHENSIVE OFAC SANCTIONS COMPLIANCE PROGRAM.** The Credit Union will create and administer a comprehensive compliance program in order to comply with OFAC requirements and will be administered by the BSA Officer.
  - A. **Disseminate Information and Provide Training.** The Credit Union will provide sufficient information to key staff members in all operations to enable them to recognize and stop suspect transactions. The account representatives and platform staff are the Credit Union's first line of defense. Thus, account officers and those individuals responsible for letters of credit and wire transfers will receive special training. These key staff will be trained to remain aware of the persons and entities on the Sanctions List so that accounts and transactions with regards to those persons are blocked and reported to OFAC.
  - B. **Risk Assessment – Initial Review.** The Credit Union will conduct a comprehensive initial review of its operation in order to ensure that OFAC requirements are being met. This will include, but not be limited to, a review of the following procedures:
    - i. Processing electronic fund transfers;
    - ii. Processing Automated Clearinghouse (ACH) transactions;
    - iii. Cashing or depositing share drafts or checks;
    - iv. Opening new accounts;
    - v. Issuing of money orders, traveler's checks and cashier's checks;
    - vi. Disbursing loan proceeds;
    - vii. Accepting of loan payments;
    - viii. Reviewing the names of co-signors, guarantors, collateral owners and other parties to each transaction;

- ix. Sending and accepting wire transfers;
  - x. Opening and allowing access to safe deposit boxes;
  - xi. Issuing credit cards;
  - xii. Reviewing the names of joint account owners, beneficiaries and other parties who have an interest in property (i.e., personal representatives and those granted power of attorney).
- C. **Risk Assessment – Ongoing Review.** The Credit Union will review new products and services offered by the Credit Union to ensure that OFAC requirements are met.
- D. **Annual Audit.** The BSA Officer will work with the Credit Union’s internal and/or external auditors to develop appropriate systems and audits so that the Credit Union is in compliance with this policy.

## 2. **DETECTION AND VERIFICATION OF PROHIBITED TRANSACTIONS.**

- A. **OFAC Sanctions Lists.** The Credit Union will comply with all FinCEN requirements to review potential members, current members, new accounts, existing accounts, and all transactions against all OFAC Sanctions Lists. These lists change regularly in response to changes in foreign policy. The Credit Union’s staff shall be aware of the persons and entities on the lists and ensure that such accounts and transactions are blocked or rejected as required and reported to OFAC in compliance with OFAC regulations.
- i. **Software.** The Credit Union will purchase available software to screen and “interdict” illicit funds transfers. Such software may filter and contain every name on OFAC lists along with generic words for countries and cities. If feasible, the Credit Union will use such software. If interdiction software is not purchased, the Credit Union will use good faith manual and electronic compliance efforts to comply with OFAC requirements.
  - ii. **Verification.** Prior to blocking or rejecting a transaction, the Credit Union will take reasonable steps to verify that the individual, country or organization detected is in fact the individual, country or organization subject to OFAC restriction, including contacting the OFAC Compliance Hotline ((800) 540-6322 or (202) 622-2490) to verify that blocking or rejecting the transaction of an individual, country or organization is appropriate.

3. **BLOCKING AND REJECTING TRANSACTIONS.** The Credit Union will create a system whereby all blocked and rejected transactions will be reported to OFAC.
- A. **Blocked Accounts and Transactions.** On reasonable assurance that a transaction or account should be blocked, the Credit Union will place a block on the transaction or account. Credit Union staff who places such a block will immediately notify the BSA Officer of the facts and circumstances surrounding the placement of the block.
- I. **Holding Blocked Funds.** All blocked funds will be placed in a segregated, interest-bearing account, which will be subject to any routine service charges assessed to accounts of a similar type.
  - II. **Releasing Blocked Funds.** The Credit Union will **not** release blocked funds to any individual or third party unless the appropriate license is obtained by OFAC.
- B. **Rejected Transactions.** On reasonable assurance that a transaction should be rejected, the Credit Union will reject it. Credit Union staff that rejects a transaction will immediately notify the BSA Officer of the facts and circumstances surrounding the rejection.
4. **REPORTING.** All reports under this section shall be submitted to OFAC using one of the following methods: Email: OFACreport@treasury.gov; U.S. mail: Office of Foreign Assets Control, Sanctions Compliance and Evaluation Division, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, NW, Freedman's Bank Building, Washington, DC 20220; or any other official reporting option, including electronic, as specified by OFAC on its website (<http://www.treasury.gov/ofac>). OFAC strongly prefers to receive reports made pursuant to this section by email or any other official electronic reporting option, as specified by OFAC on its website. <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>.

A. **Blocked Property.**

- I. **Initial Report.** An initial report is required to be filed within **ten (10) business days** from the date that the property becomes blocked. The initial report will include the following information:
  - a. The owner of the account;
  - b. A description of the property that is subject of the blocking;
  - c. The location of the property;

- d. Any account number or other identifying information (check numbers, reference numbers, dates, or other information necessary to identify the property);
- e. The actual or estimated value in U.S. Dollars;
- f. The date the block was placed;
- g. A description of any transaction associated with the blocking, including: the type of transaction; any persons, including financial institutions, participating in the transaction and their respective locations (relevant members, beneficiaries, originators, letter of credit applicants, and their banks; intermediary banks; correspondent banks, issuing banks; and advising or confirming banks); and any reference numbers, dates, or other information necessary to identify the transaction.
- h. The associated sanctions target(s) whose property is blocked (such as a SDN or other blocked person), the location(s) of the target(s) (if known), and, if not evident, a narrative description of the interest(s) of the target(s) in the property; if there is no target or the target is not known, include a referenceto the relevant written communication from OFAC pursuant to which the blocking action was taken;
- i. The legal authority or authorities under which the property is blocked and any action taken with respect to the property (for example, the property has been deposited into a new or existing blocked, interest bearing account, pursuant to OFAC requirements);
- j. The name and address of the Credit Union; and
- k. The name, telephone number, and email address of the contact person at the Credit Union from whom compliance information can be obtained.

If the report involves the receipt of a blocked payment or transfer of funds, the report also will include a photocopy of the payment or transfer instructions received and will confirm that the payment has been deposited into a new or existing blocked account which is labeled as such and is established in the name of, or contains a means of clearly identifying the interest of, the individual or entity subject to blocking pursuant to OFAC requirements.

II. **Annual Report.** A comprehensive report on all blocked property held by the Credit Union **as of June 30** of the current year will be filed annually with OFAC **by September 30**. The annual report will be filed using Form TD-F 90-22.50, Annual Report of Blocked Property or an approved alternative form. A copy of the annual report will be retained by the Credit Union for five (5) years. (See Record Retention Policy). Updated guidance for annual reporting, July 1, 2021, can be found at <https://home.treasury.gov/policy-issues/financial-sanctions/ofac-reporting-system>.

B. **Rejected Transactions.** The Credit Union will send notice of all rejected transactions to OFAC within **ten (10) business days** of the rejection placement. Transactions include wire transfers, trade fine, securities, checks, foreign exchange and goods or services. The report will be filed with the Office of Foreign Assets Control as specified on the website (<http://www.treasury.gov/ofac>). Notice to OFAC will describe the following information:

- a The name and address of the credit union as the person who rejected the transaction;
- b The name and telephone number of the contact person at the credit union who can provide compliance information;
- c The date the transaction was rejected;
- d A description of the rejected transaction, including certain required identifying information;
- e If applicable, the associated sanctions target(s) whose involvement in the transaction has resulted in the transaction being rejected and its location, if known;
- f The actual or if unknown, estimated value of the property in U.S. dollars;
- g The legal authority or authorities under which the transaction was rejected; and
- h A copy of any related payment or transfer instructions or other relevant documentation.

## 5. RECORD RETENTION AND ACCESS TO RECORDS.



- A. **Record Retention Period.** The Credit Union will retain all records, reports, licenses and other materials related to any blocked or rejected transaction for a period of at least **five (5) years** after OFAC authorizes the release of the funds (See Record Retention Policy). If the Credit Union holds property blocked or funds transfers retained pursuant to OFAC regulations, it will keep a full and accurate record of the property, and the record shall be available for examination for the period of time that such property is blocked and for at least **five (5) years** after the date such property is unblocked.
  - B. **Access to Records.** Upon request, the Credit Union will provide OFAC with access to any records relating to a blocked or rejected transaction.
6. **UPDATE OFAC INFORMATION.** The Compliance Officer or other designated individual will periodically visit the OFAC website to keep current with new regulations and listings at <https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>.
- A. The following parties will be checked against the OFAC Sanctions Lists:
    - I. Co-signors, guarantors, collateral owners and other parties to each transaction;
    - II. Joint account holders;
    - III. Beneficiaries; and
    - IV. Others who have an interest in property, such as personal representatives and those granted power of attorney.
  - B. The following transactions are subject to OFAC regulations:
    - I. Processing electronic fund transfers;
    - II. Processing Automated Clearinghouse (ACH) transactions;
    - III. Depositing or cashing share drafts/checks;
    - IV. Opening new accounts;
    - V. Issuing money orders, traveler's checks and cashier's checks;
    - VI. Disbursing loan proceeds;
    - VII. Accepting loan payments;

- VIII. Sending and accepting wire transfers;
- IX. Opening and allowing access to safe deposit boxes; and
- X. Issuing credit cards.

## **7. INTERNATIONAL ACH TRANSACTIONS.**

A. **Credit Union as Receiving Party (RDFI).** The Credit Union will ensure that it identifies international ACH transactions and conducts an OFAC Sanctions List review whenever it receives such an ACH transaction. All of the parties to the transaction will be checked, as well as the remittance data and the correspondent banks PRIOR to posting or returning the transaction.

- I. If there is a match, the Credit Union will notify the Gateway Operator that the funds have been frozen and should not be released to the foreign party. (“Gateway Operator” is defined as the entry point to or exit point from the United States for ACH payment transactions.)

8. **MARIJUANA-RELATED BUSINESSES.** Based on the position of the Federal government and Federal law that marijuana is an illegal substance in the United States and irrelevant to state law, the Credit Union will not provide services to Marijuana-Related Businesses.

## **A. CREDIT UNION RESPONSIBILITIES.**

- i. The Credit Union will review potential business and commercial members to verify that they are not a Marijuana-Related business by requesting such information on its Account Usage Survey completed at account opening.
- ii. The Credit Union will review current business and commercial member’s activity and transactions to ensure that they are not servicing a Marijuana-Related business:
  - a. The credit union will take steps to identify “red flags”;
  - b. In the event that activity or transactions indicate a current member business is engaging in marijuana related business activities the credit union will:
    - 1. File appropriate BSA reporting including, but not limited to, Suspicious Activity Reports;
    - 2. Confirm the activity and/or transactions are related to marijuana;
    - 3. Take steps to close the account(s).

**B. FILING OF SUSPICIOUS ACTIVITY REPORTS.** The Credit Union will file a SAR on activity involving a Marijuana-Related business (including those duly licensed under state law), in accordance with FinCEN’s suspicious activity reporting requirements and related thresholds.

i. **“Marijuana Priority” SAR Filings.** A financial institution filing a SAR on a Marijuana-Related business that it reasonably believes, based on its member due diligence, implicates one of the priorities outlined in FinCen or violates state law will file a “Marijuana Priority” SAR. The content of this SAR should include comprehensive detail in accordance with existing regulations and guidance. Details particularly relevant to law enforcement in this context include:

- a. Identifying information of the subject and related parties;
- b. Addresses of the subject and related parties;
- c. Details regarding the enforcement priorities the financial institution believes have been implicated; and
- d. Dates, amounts, and other relevant details of financial transactions involved in the suspicious activity. Credit unions should use the term “MARIJUANA PRIORITY” in the narrative section to help law enforcement distinguish these SARs.

ii. **“Marijuana Termination” SAR Filings.** If a credit union deems it necessary to terminate a relationship with a Marijuana-Related business in order to maintain an effective anti-money laundering compliance program, it will file a SAR and note in the narrative the basis for the termination. The term “MARIJUANA TERMINATION” must be noted in the narrative section.

**C. RED FLAGS TO DISTINGUISH PRIORITY SUSPICIOUS ACTIVITY REPORTS.** The Credit Union will review “red flags” such as those listed below to distinguish Priority SARs and perform additional due diligence. Red flags unique to Marijuana-Related Businesses include (but are not limited to):

- i. A member appears to be using a state-licensed marijuana-related or hemp-related business as a front or pretext to launder money derived from other criminal activity (i.e., not related to marijuana) or derived from marijuana-related activity not permitted under state law.
- ii. The business is unable to produce satisfactory documentation or evidence to demonstrate that it is duly licensed and operating consistently with state law.
- iii. The business is unable to demonstrate the legitimate source of significant outside investments.

- iv. A member seeks to conceal or disguise involvement in marijuana-related or hemp-related business activity. For example, the member may be using a business with a non-descript name (e.g., a “consulting,” “holding,” or “management” company) that purports to engage in commercial activity unrelated to marijuana but is depositing cash that smells like marijuana.
- v. Review of publicly available sources and databases about the business, its owner(s), manager(s), or other related parties, reveal negative information, such as a criminal record, involvement in the illegal purchase or sale of drugs, violence, or other potential connections to illicit activity.
- vi. The business, its owner(s), manager(s), or other related parties are, or have been, subject to an enforcement action by the state or local authorities responsible for administering or enforcing marijuana-related laws or regulations.
- vii. A marijuana-related or hemp-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.
- viii. The owner(s) or manager(s) of a marijuana-related or hemp-related business reside outside the state in which the business is located.
- ix. A marijuana-related business or hemp-related is located on federal property or the marijuana sold by the business was grown on federal property.
- x. A marijuana-related or hemp-related business’s proximity to a school is not compliant with state law.
- xi. A marijuana-related or hemp-related business purporting to be a “non-profit” is engaged in commercial activity inconsistent with that classification or is making excessive payments to its manager(s) or employee(s).