Family First Credit Union
BSA Policies and Procedures

Table of Contents

Family First Credit Union
Deposit Account Policy
Bank Secrecy Act /Anti-Money Laundering Policy

General Policy Statement:
The 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 0f 2001, the BSA, the Currency and Foreign Transactions Reporting Act, OFAC rules, and all related laws and regulations to combat money laundering, terrorist financing, tax evasion and other financial crimes.

The Compliance Officer along with the Compliance Specialist is responsible for managing BSA Compliance for the Credit Union. The Compliance/BSA officer is Wanda Norman. Wanda has the following designations: CUCE (Credit Union Compliance Expert) and BSACS (Bank Secrecy Act Compliance Specialist).

Guidelines:
BSA/AML Compliance Program
The Board of Directors will approve the BSA/AML Compliance Program and any changes to it.

Compliance Officer. The BSA/AML/OFAC Compliance Officer appointed by the Board, will:

- ✓ Be the designated person for managing BSA Compliance,
- ✓ Act as the primary contact person with any applicable federal agency,
- ✓ Periodically review and update the BSA/AML Compliance Program,
- ✓ Ensure that daily transaction records are received and determine if the required reports have been timely and accurately filed and appropriate actions were taken;
- ✓ Ensure that staff complies with the BSA/AML requirements;
- ✓ Ensure that adequate record retention procedures are in place.

Risk Assessment. The Compliance 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.

Internal Controls. The Chief of Finance and Compliance Officer will develop and implement a system of internal controls and procedures for the oversight of the Supervisory Committee. The Credit Union's internal controls consist of monitoring, reporting, and recordkeeping.

Training. The Credit Union will provide periodic training for employees whose responsibilities involved 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 Compliance Officer will ensure that the appropriate staff, including new hires, receives training and that records documenting the training are kept.

Audit. There will be an 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.

Customer Identification Program (CIP)

Identity Verification

The Credit Union will verify the identity of each member (current or new) and person who opens an account including one who is joint, 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 opening the account. If a member or person refuses or is unable to provide the requested information within ten 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.

Required Information

Employees will follow the procedures for collecting information to identify each new and current member opening an account. At a minimum, the Credit Union will obtain the following information from an individual or entity before opening an account:

A. Name (individual name) or (entity name & any assumed business name);

B. The current credit union member number of the existing member;

C. Date of birth (an individual);

D. Address:
   i. Residence or principal place of business and mailing address (if individual);
   ii. Army Post Office (APO) or Fleet Post Office (FPO) box number or residential or business street address of next of kin or another contact individual (if an individual); or
   iii. Principal place of business, local office, or other physical location (if a person is other than an individual, i.e. corporation, partnership, trust, estate, guardianship).
   iv. Identification Number:
   v. For a U.S. person, a TIN, SSN, ITIN, EIN.
      a. 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.

Legal Entity Member

The Credit Union will identify and verify legal entity members, including all beneficial owners, consistent with the CIP. The Credit Union will update beneficial ownership information on their members on an event-driven basis, when in normal course monitoring, they detect information that may be relevant, such as a potential change in the ownership structure or unexplained change in activity.

A. **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).
B. 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.

The Credit Union will identify the beneficial owners of each legal entity at the time a new account is opened. The process will commence as follows with documentation being obtained from the legal entity;

C. New Account Survey
D. Verification of Tax Identification Number (TIN) or Employee Identification Number (EIN)
E. Articles of Incorporation
F. Letterhead from the legal entity identifying the beneficial owners

Credit Card Account

In connection with a person who opens a credit card account, the Credit Union may obtain the identifying information about a person by acquiring it from a third-party source (i.e. credit reporting agency) before extending credit to the person.

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.

Verification through Documents

For accounts opened in person, the Credit Union will verify the identity of each person or entity through the following documents:

1. **For Individuals**: un-expired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard (such as a driver's license or passport).

2. **For Non-Individuals**: documents showing the existence of the entity (registered articles of incorporation or organization, a government issued business license; or Partnership Agreement or trust instrument.) All non-individual accounts must have the identity of all authorized agents of the entity identified, and valid SSNs must be provided to the Credit Union before account opening.

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 filing an online loan application.

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:

1. All identifying information about a member (person) obtained;
2. 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;
3. A description of the methods and the results of any measures undertaken to verify the identity of the member (person); and
4. A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

vi. **Non-Documentary Verification Methods**. The Credit Union will use non-documentary 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 another source; checking references with other financial institutions and obtaining a financial statement.

vii. **Account Closure**. When a provisional account is opened

without obtaining documents, all attempts will be made to retrieve the required documentation to confirm the person's identity. If this information is not obtained within 30 days, the account will be closed, and funds will be returned to the current account owner(s). Any exceptions to this procedure must be approved by Branch Management, based on the non-documentary verification obtained.

viii. **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 by 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.

Lack of Verification

The Credit Union will create procedures to determine its actions if it cannot verify a new member's or person's identity through documentary or non-documentary means. Depending upon the type of account requested; the Credit Union may permit limited transactions, while identity is being verified. After ten days, 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 or if opened, it would be closed. Risk will determine final policy decisions when there is a lack of identification verification.

Reporting Requirements

Currency Transaction Reporting (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.

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.

1. **Exemptions 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 (TD F 90-22.53) with the U.S. Department of Treasury within 30 days after the first transaction in currency that the Credit Union wishes to exempt.

i. 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.
ii. 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 member deposits or withdraws more than $10,000 (currency and coin). **If members are not exempt, tellers must complete a CTR**.

B. **Exemptions II** - For members who qualify as either "non-listed businesses" or "payroll customers," the Credit Union will file FinCEN Form 110 within 30 days after the first transaction in currency the Credit Union

want 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.

i. 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.
ii. 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.

Suspicious Activity Reporting

The Credit Union will complete and electronically file a SAR (Suspicious Activity

Report) 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.

Any suspicious activity will be reported to the Compliance Department via the Unusual Activity report. The Compliance Officer or Compliance Specialist will research the unusual activity and decide on whether to file a SAR.

A SAR is to be verified by both Compliance Officer and Compliance before it is submitted electronically in BSAE-filing to ensure all pertinent information is included in the report.

The decision to file a SAR or not file a SAR will be documented and retained along with any supporting documentation for five years.

The Credit Union will report any crime or unsuspected 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 questions regarding suspicious activity that require immediate attention, call the BSA Regulatory Helpline at (800) 949-2732, or 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 the SAR for five years. To comply with Section 351 of the PATRIOT Act, except where such disclosure that it prepared or filed a SAR and will notify FinCEN 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, for failure to disclose the fact of such report.

Sharing SARs and SAR Information

SARS's are confidential. Therefore, the Credit Union will only disclose the SAR filing with the appropriate law enforcement agency, regulator, and the board, or it's designated committee as outlined in this policy.

- ✓ The Credit Union may also share a SAR or SAR information with its affiliates. 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 party involved in the suspicious activity that is the subject of the SAR.

- ✓ 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 of the request.

Reportable Transactions

1. **Suspicious large deposits**, even if $10,000 or less, consisting of numerous items or out-of-area items.
2. **Unusual or suspicious transactions**, such as deposits; withdrawals; transfers between account; exchange of currency; loans; extensions of credit; purchases or sales of any 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 from identity cards with pictures.
3. **Insider abuse involving any amount**. A SAR is 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.
4. **Transactions aggregating $5000 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 drivers' Licenses or social security numbers, addresses and telephone numbers), will be reported.
5. **Transactions aggregating $25,000 or more regardless of potential suspects**.
6. **Transactions aggregating $5000** 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 is (1) involves funds derived from illegal activities; (2) is designed to evade the BSA; or (3) has no business or apparent lawful purpose.

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).

Report to Board of Directors or Designated Committee

The Compliance Officer 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 the 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.

Report of International Transportation of Currency or Monetary Instruments Family First Credit Union will timely file a Currency or Monetary Instrument Report (CMIR) if it physically transports, mails or ships, or causes to by physically transported, mailed, or shipped currency and/or monetary instruments in excess of $10,000 at one time into or out of the United States.

Family First Credit Union will file a CMIR if it receives currency and/or monetary instruments in excess of $10,000 at one time that have been transported, mailed, or shipped to the credit union by a member from outside the United States, except if the transfer of funds is through normal banking procedures that do not involve the physical transportation of currency or monetary instruments. The Credit Union will file the CMIR on or before the date of entry, departure, mailing, or shipping. Reports will be sent to: Commissioner of Customs, Attention: Currency Transportation Reports Washington, DC 20229.

Foreign Financial Report

The Credit Union will fill a Foreign Bank and Financial Accounts Report (FBAR) form (Treasury Form TD F 90-22.1) with the IRS on or before June 30 of each year for all Credit Union financial account relationships outside the United States that exceed
$10,000 during the previous calendar year. The Credit Union will retain FBAR forms for five years.

Suspicious Activity on accounts

Closing Accounts due to Suspicious Activities

Management may decide to close accounts with suspicious activity especially if the credit union suffers a loss of any kind. The decision to close the account will be fully documented, communicated to the member, and approved by a Manager.

Suspicious activities include:

- Structuring
- Terrorist Financing (unless instructed by FinCEN to keep the account open)
- Fraud
- Money Laundering
- False records
- Other suspicious activities

Maintaining Accounts at the request of Law Enforcement

If the Government or Law Enforcement requests an account remain open, the following procedures will be followed:

1. A written request obtained from the requestor and maintained for record.
2. Verify the request is submitted by the appropriate authority.
3. Verify the request contains the reason for maintaining the account.
4. Verify the appropriate timeline for keeping the account open.

Record Retention

Checks, Drafts, Cashier's Checks, $3,000 to $10,000 in 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 purchase 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 Compliance Officer to be maintained in a centralized location. The Credit Union will retain the logs for five years

Certain Financial Transactions

The Credit Union will prepare and maintain 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 five years.

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):

1. **Credit Union Originates 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.

2. **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; and

F. As many of the following information of the recipient as possible (name, address, account number and any other specific identifier).

3. **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).
4. **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.

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.

1. **Required Sharing with FinCEN – Section 314(a).** The Credit Union designates its BSA Compliance Officer as the FinCEN, contact person. Upon FinCEN's request, the Credit Union will search its records for a specified individual or entity.
2. **Certification**. Before 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.
3. **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:
   A. Current accounts;

   B. Accounts maintained/ closed during the preceding twelve (12) months; and

   C. 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.

5. **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 will place an "X," on the 314(a) form, 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 e-mail to patriot@fincen.treas.gov, directly on FinCEN's Web site (www.fincen.gov/314a), or by calling 1-866-556-3974.

   A. **Use and Confidentiality of Information**. The Credit Union will **not** use FinCEN information in 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.

   B. **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.

   C. **Voluntary Information Sharing – Section 314(b).** The Credit Union may share information with other financial institutions or association of financial institutions regarding individuals, entities, and countries for purposes of detecting, identifying, or reporting activities that it suspects may involve money laundering or terrorist activities. If the Credit Union engages in this type of information sharing, it will not be liable to any person under any state or federal law or regulation or under any contract or other legally enforceable agreement, for such sharing, or for any failure to provide notice of such sharing, to an individual, entity, or organization that is identified in such sharing.

      ii. **Certification**. If the Credit Union intends to share this information, it will submit a completed FinCEN Notice, either by accessing FinCEN's website, www.fincen.gov and entering the appropriate information or by mailing the completed

certification to: FinCEN,
P.O. Box 39, Mail Stop 100, and Vienna, VA 22183. Each certification is effective for one year beginning on the certification date. The Credit Union will submit a new certification annually.

iii. **Security and Confidentiality**. The Credit Union will create and maintain procedures to protect the security and confidentiality of shared information. This information will be used only to detect, identify, and report on activities that may involve terrorist or money laundering activities or to determine whether to establish or maintain an account or to engage in a transaction. If the Credit Union suspects terrorist activity or money laundering, it will call FinCEN and, if appropriate, file a SAR.

D. **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.

ii. **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.

iii. **Questions**. Any and all questions related to an NSL are to be directed to the local FBI field office ONLY.

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.

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.

Record Retention
The Credit Union will retain all identifying information about a member (person) 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:

A. 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;

B. A description of the methods and the results of any measures undertaken to verify the identity of the member (person); and

C. A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

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 Compliance 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.

Monitoring In-House Reports

The following reports will be reviewed and monitored daily for fraudulent and illegal activities. Reports will be signed by the reviewer and stored for a period of 5 years. All such transactions will be reported immediately to Management, Board of Directors and the proper authorities. The Monetary Instrument Log will be verified by the Compliance Officer or a designated person monthly to ensure suspicious activity is researched.

Share Accounts and Loans

- BSA Report
- Kiting Report
- Excessive Transactions
- Security Overrides
- Monetary Instrument Log

Visa Platinum Credit Cards

- Daily Foreign Transactions Report
- Daily Authorization Activity Report
- Lost/Stolen Report
- Activity on Blocked Accounts Report
- Outstanding Temporary Stolen and Blocked Accounts Report
- Stolen Account Report

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:

Field of Membership

The field of membership for Family First Credit Union includes the employees and retired employees of the Fulton County Board of Education, Fulton County Private schools, Fulton County municipalities, and Atlanta Public School system.

Family First Credit Union field of membership shall include persons related by blood, adoption, or marriage to or living in the same household with a person having a common bond as well as persons and surviving spouses of persons who are no longer within the common bond but who were members of the credit union in good standing when they left.

The following are examples of those eligible for membership:

- Mother (in-laws, step)
- Father (in-laws, step)
- Sister (in-laws, step)
- Brother (in-laws, step)
- Son (step and adopted)
- Daughter (step and adopted)
- Aunt
- Uncle
- Cousin
- Grandmother
- Grandfather
- Grandchildren
- Nieces
- Nephews
- Surviving Spouses

Family First Credit Union Bank
Secrecy Act Policy Procedures
Completing the CTR
Currency Transaction Report

Family First Credit Union will file a Currency Transaction Report (CTR) with the IRS within 15 days of a transaction in currency of more than $10,000 (unless exempt). Multiple currency transactions are treated as a single transaction if the credit union has knowledge the transactions are by or for one person (structuring) totaling more than $10,000 during any one business day.

The Bank Secrecy Act compliance officer will review and countersign all CTR forms completed by any member of the staff or board. The compliance officer will file the completed CTR form electronically via http://bsaefiling.fincen.treas.gov.

Procedures

1. All employees must read and understand the Family First Credit Union's policy on the Bank Secrecy Act.
2. Credit Union Tellers/Personnel will report transactions to the Compliance Dept. that qualify for a CTR (Currency Transaction Report). The Compliance Department will electronically file the CTR in BSA E-Filing.

3. Transactions include deposits, withdrawals, exchange of currency, or other payments that appear to be suspicious. This also includes multiple transactions in the same day which total more than $10,000 in currency.
4. Acceptable identification is listed as follows:
    a. Picture ID
    b. Valid Driver's License
    c. Valid Passport
    d. Alien Identification
    e. Credit Union Signature Card
5. The CTR must be filed within 15 days of the transaction.
6. Complete the Currency Transaction Report form online.
7. Complete the Designation of Exempt Person form when applicable.
8. Send the completed form(s) to the Compliance Department.
9. A CTR is to be verified by the Compliance Officer and/or Compliance Specialist before it is submitted electronically in BSAE-filing to ensure all pertinent information is included in the report.
10. The Compliance Department will file the CTR for electronically
11. The original CTR forms will be stored electronically for at least five years.
12. Supporting documentation will be maintained on file for at least five years.

Family First Credit Union Bank
Secrecy Act Policy Procedures
Completing the SAR
Suspicious Activity Report

Suspicious Activity Report (SAR)

The Credit Union will 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.

The Credit Union will report any crime or unsuspected 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 questions regarding suspicious activity that require immediate attention, call the BSA Regulatory Helpline at (800) 949-2732, or 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.

SARs are confidential. Therefore, the Credit Union will only disclose the SAR filing with the appropriate law enforcement agency and the board, or it's designated committee as outlined in this policy. 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 the NCUA of the request.

Family First Credit Union is required to make this report following the discovery of:

- Insider abuse involving any amount
- Violations aggregating $5,000 or more where a suspect can be identified
- Violations aggregating $25,000 or more regardless of a potential suspect
- Transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.
- Computer Intrusion

Management will determine if there are other times when it is appropriate to file a SAR. If the decision is made not to file a Suspicious Activity Report, the Compliance Officer or Compliance Specialist will:

- Verify the questionable transactions or activity

- Written document explaining decision not to file a SAR with signatures

- Date of activity and date of decision

Procedures

1. All employees must read and understand the Family First Credit Union's policy on the Bank Secrecy Act.
2. Credit Union Tellers/Personnel will complete an **Unusual Activity Report** when applicable and attach supporting documentation.
3. Forward the **Unusual Activity Report** along with the supporting documentation to the Compliance Officer.
4. Complete the Report of International Transportation of Currency or Monetary Instruments when applicable.
5. The Compliance Officer will determine if a SAR should be filed.
6. Upon approval, a SAR will be electronically filed via http://bsaefiling.fincen.treas.gov.
7. The original SAR report will be stored electronically.
8. Supporting documentation will be kept on file for at least five years.

Reporting to Management and Board Members

The Compliance Officer will report to Management and the Board of Directors monthly and quarterly on the number of SAR's reported for that period. The monthly and quarterly reports will be kept on file for a period not less than five years. The report lists the following information:

✓ Date SAR was reported

✓ Suspicious Activity and basic information

✓ Total Dollar Amount involved

✓ Impact on Financial Soundness

Family First Credit Union Bank
Secrecy Act Policy/Procedures
USA Patriot Act
(CIP)
Customer Identification
Program

The Credit Union will undertake reasonable risk-based measures, appropriate for its size and type of business, to verify the identity of any person seeking to open an account, to the extent reasonable and practicable; maintain a record of the information used to verify the person's identity, and determine whether the person appears on any list known or suspected terrorists or terrorist organizations provided to the Credit Union by any government agency.

Family First Credit Union understands the Customer Identification Program (CIP) requires the credit union to follow these basic steps when a member and or account owner opens a new account or when a new member is added to an existing account:

- Provide CIP disclosure
  - Lobby/Office display
  - Verbally
- Obtain basic information about the member
  - Name
  - Date of Birth
  - Address
  - Identification Number
- Verify the identity of the member using Deluxe Detect
- Run the following checks on members opening any kind of account. Maintain copies of
  - **Deluxe Detect screen**
  - **OFAC**
- Any discrepancies in information should be resolved and documented in the member application file. (see procedures for documenting and resolving discrepancies on verifications)
- Copies of verifications are maintained with account agreement/signature card.
- Retain records for 5 years after the account has been closed.

Legal Entity Member

When opening a legal entity account the following documentation must be attained in order for the account to be opened in addition to following the steps for the CIP for 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).

In addition, the following documents must be collected and scanned into record for the legal entity member:

- ✓ New Account Survey
- ✓ Verification of Tax identification Number (TIN) or Employee Identification Number (EIN)
- ✓ Articles of Incorporation
- ✓ Letterhead from the legal entity identifying the beneficial owners, beneficial owners will be verified through the credit union's CIP requirements.

General Provisions

Applicability

The Customer Identification Program policy applies to:

- Any new member opening an account at Family First Credit Union
- Any new or current member added to an existing member's account

The Customer Identification Program policy does not apply to existing members of Family First Credit Union as long as:

- Existing members' identity was previously verified according to the current standards and is on file
- Employee of Family First Credit Union has a reasonable belief he or she knows the identity of the member

Member Notice

A notice (see attached notice) shall be given to new account owners in any of the following ways:

- Oral notice is given to new account owners, in person or on the phone
- Lobby Notice
- Signs at Member Service Representative desks
- Notice posted on new account pages of Family First Credit Union website (www.ffcuga.com)

Document Identification

Document Identification includes requiring any of the following (listed in order of preference):

- Unexpired Government Issued Driver's License
- Unexpired Government Issued Identification Card
- Passport
- Student Identification Card
- Other National Identification Document
- For persons other than an individual (such as a corporation, partnership or trust), documents showing the existence of the entity such as:

- Certified articles of incorporation
- Government issued business license
- Partnership agreement, or
- Trust Instrument

Non-Document Identification

Non-Document Identification includes any of the following:

- Contact new member's employer
- Check references at other financial institutions
- Contact new member's family member
- Compare member information against credit report, public database or another source.
- Utility bill showing member's name and address

Special Circumstances – Lack of Verifications

In situations where Family First Credit Union cannot form a reasonable belief regarding the identity of a new account owner (either due to lack of document identification or non-document verification) the staff at Family First Credit Union will:

- Not open the account
- Open the account, however; the member will only be allowed to perform deposit transactions while the credit union attempts to verify the member's identity
- If attempts to verify the member's identity have failed, the account will be closed within 10 days of the date of opening.

Comparison with Government Lists

Family First Credit Union will cross check the name(s) of any new member against any list of known or suspected terrorists or terrorist organizations issued by any Federal Government Agency and designated as such by Treasury in consultation with the Federal functional regulators. This determination will be made at the time the account is opened. Family First Credit Union will follow all Federal directives issued in connection with such lists. Any member whose name appears on any of the above-mentioned lists might not be permitted to open an account at Family First Credit Union.

Risk Weighting Members

The credit union has developed a process for risk weighting members. This will include a monthly report listing members that have transactions that fall in at least one of the risk types listed below. The member's account will be rated as low, medium, or high based on the historical information on the account. A New Member Profile will be completed for new memberships and will be the first evaluation of the risk associated with the account. Transactions will be evaluated according to the risk types determined by the credit union. **An initial risk will be given to the membership within one month of account opening.**

The monthly member risk report will be reviewed by the Compliance Department. Transactions are evaluated, and the appropriate risk rating is applied to the membership with each review.

Medium and High Risk rated accounts will be monitored for suspicious and fraudulent activity within the Compliance Department monthly. A quarterly report of activity will be included with the Quarterly BSA Report for executive and board review.

Risk Rating levels:

- Low (0 risk type)
- Medium (one risk type)
- High (two or more risk types)

Risk Types:

- Alert from CRA (Community Reinvestment Act)
- CTR (Currency Transaction Report)
- Deluxe Detect
- Excessive Deposits
- Excessive Withdraws

- IAT Alerts (International ACH Transaction)
- Notice alert by member
- OFAC/ID Failed
- Suspicious Documents
- Suspicious Personal Information
- Suspicious Activity/ SAR (Suspicious Activity Report)
- Wire Alert

Procedures for Collecting Basic Information for a New Account

Collecting Basic Information

Any current member or person requesting to open a new account or become joint on an account with Family First Credit Union must provide the following basic information **before** opening an account:

- First and Last Name as it appears on the social security card
- Date of Birth
- Address, which shall be:
    - For an individual, a residential street address;
    - For an individual who does not have a residential street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential street address of next of kin or of another contact individual; or
    - For a person other than an individual (such as a corporation, partnership or trust), a principal place of business, local office or other physical location; and
- Identification Number
    - United States citizen
        - Social Security Number
    - Non-United States citizen
        - 9-Digit Individual Tax Identification Number
        - Passport Number
        - Alien Identification Card Number (Green Card)
        - Document Number and Country Issuing any "other document" showing evidencing nationality or residence and bearing a photograph or similar safeguard.

If the current member or person is in the process of applying for an SSN or the card is not available, Family First Credit Union will accept a letter from the Social Security Administration documenting the card has been applied for or reissued. The credit union will require the member to produce the card within three months of account opening. In the case of an infant or adopted minor, the account will be monitored on a monthly basis by a member service representative. The credit union will contact the parents each month until the card is presented to the credit union. Failure to comply within three months will result in the closing of the account.

Verifying Basic Information

When a current member or person opens an account or is added as a joint member, Family First Credit Union staff will use both "document and non-document" methods to verify the identity of all new account owners. If an account is requested through the mail or the internet, it will not be opened until document information, and a signed account card is received.

Money Laundering Red Flags for opening accounts

Designated Family First Credit Union staff is responsible for opening new accounts and verifying potential member's identity. This also includes gathering required data and identity potential money laundering red flags prior to opening an account.

The following transactions or activities may not necessarily be indicative of money laundering if they are consistent with a member's legitimate business. Many of the "red flags" involve more than one type of transaction.

1. **Minimal, vague or fictitious information provided.** Minimal, vague or fictitious information provided that cannot be readily verified.
2. **Lack of identification or references.** Individual attempts to open an account without references or identification gives sketchy information or refuses to provide the information needed by the credit union.
3. **Non-local address.** The individual does not have a local residential address, and there is no apparent legitimate reason for opening an account with the credit union.
4. **Members with multiple accounts.** A member maintains multiple accounts at the credit union or at different banks for no apparent legitimate reason. The accounts may be in the same names or in different names with different signature authorities. Inter-account transfers are evidence of common control.

All suspicious activity and transactions should be reported immediately to the Compliance Officer or to an Officer of the Credit Union.

A thorough investigation is made of activities and/or transactions to determine appropriate action to take.

1. No action was taken,
2. SAR form completed, or
3. Inform local or federal authorities

IN GENERAL, to assure the credit union's compliance with the Bank Secrecy Act, all of the officers of the Board and all members of the credit union staff shall be ever watchful to recognize and report to the proper board of staff member any unusual cash activities or any other activity that may fall within the bounds of the Bank Secrecy Act, the Money Laundering Control Act of 1986, and any amendments or regulations.

Family First Credit Union
Deposit Account Policy
OFAC Policy and Procedure Guide

Introduction
The office of Foreign Assets Control (OFAC) of the Department of the Treasury administers and oversees a series of laws that impose economic sanctions against hostile targets to further U.S. foreign policy and national security objectives. OFAC is responsible for promulgating, developing, and administering the sanctions for the Treasury under eight federal statues.

The OFAC laws and regulations promote national and international security by requiring assets freezing of oppressive governments, international terrorists, narcotic traffickers, and other specially designated persons. It is the policy of Family First Credit Union to comply with the requirements set forth by OFAC.

Summary of OFAC Regulations
Family First Credit Union will monitor all financial transactions performed by or through us to detect those that involve any entity or person subject to the OFAC laws and regulations.

For most situations, Family First Credit Union should accept deposits and funds subject to OFAC regulations, but freeze the funds and accounts, so that absolutely no funds can be withdrawn (blocking). However, a few situations require the credit union to reject the transaction or funds instead of accepting and blocking them. Exact regulations vary, in accordance with requirements imposed by the eight federal statues and the specific sanctions. A detailed description of specific regulations for each program is available on the official OFAC web site: www.treas.gov/ofac.

The compliance officer is responsible for overseeing compliance with the OFAC laws and regulations.

Transaction Subject to OFAC
Every type of financial transaction should be reviewed for OFAC compliance including, without limitation, the following:

- Deposit accounts (checking, savings, etc.)
- Loans
- Lines of credit
- Letters of credit
- Wire transfers
- ACH transfers
- Depositing or cashing checks
- Purchase of bank checks or cashier's checks
- Loan payment

- Guarantors and collateral owners
- Trust account
- Credit Cards
- Safety Deposit Box entry

The names of all parties to a transaction should be checked against the list of names of individuals, entities, geographical locations or countries that have been identified by OFAC. This includes, but is not limited to the following (as applicable):

- Beneficiaries
- Collateral Owners
- Guarantors/Cosigners
- Receiving Parties
- Sending Parties
- Deputies and/or Agents of Safe Deposit Boxes
- Non- Credit Union members cashing checks in excess of $3000.00.

Family First Credit Union will verify the identity of persons benefiting from the following types of transactions by conducting an individual name search on the SPECIALLY DESIGNATED NATIONALS AND BLOCKED PERSONS list using the following URL:

https://www.treasury.gov/ofac/downloads/sdnlist.pdf

Compliance Procedures

Check Current and New Members

Family First Credit Union will check all of the names in its member database as well as each new member. Furthermore, the credit union will re-check our database weekly, which is performed by our data processor, currently CUnify.

If a name is determined to be a true match, appropriate action must be taken to block (or reject, if applicable) the transaction, and then file the appropriate report with OFAC. All accounts for the matched name should immediately be frozen and placed in a

blocked account so that no funds can be withdrawn from these open accounts. In all cases an appropriate company officer, usually the compliance officer, should be notified immediately. The name of the member, the transaction and account details will be needed to file the appropriate report.

Specific Transaction Handling

If the transaction is a deposit, Family First Credit Union is to accept the funds and immediately place the funds in a blocked account so that no funds can be withdrawn. This applies unless it is one of the few transactions that are to be rejected, in which case the credit union should refuse to take the funds and proceed with the transaction. If the transaction is a transfer of funds (by, through or to the Credit Union), then the credit union is to accept the funds, but instead of transferring them put them into a blocked account so that no funds can be withdrawn. Again, this applies unless it is one

of the few transactions that are to be rejected, in which case the credit union should refuse to take and proceed with the transaction.

In general, the member should be advised immediately of the blocking of the account or funds.

Suspicious Activity on accounts

Closing Accounts due to Suspicious Activities

Management may decide to close accounts with suspicious activity especially if the credit union suffers a loss of any kind. The decision to close the account will be fully documented, communicated to the member, and approved by a Manager.

Suspicious activities include:

- Structuring
- Terrorist Financing (unless instructed by FinCEN to keep the account open)
- Fraud
- Money Laundering
- False records
- Other suspicious activities

Maintaining Accounts at the request of Law Enforcement

If the Government or Law Enforcement requests an account remain open, the following procedures will be followed:

5. A written request obtained from the requestor and maintained for the record.
6. Verify the request is submitted by the appropriate authority.
7. Verify the request contains the reason for maintaining the account.
8. Verify the appropriate timeline for keeping the account open.

Interest on Blocked Funds

Any funds placed in a separate blocked account will collect reasonable commercial interest as mandated by OFAC regulations. This regulation applies regardless of whether it is the credit union's policy to pay interest on these accounts or not. (i.e., credit union policy is to not pay interest on accounts with a balance below $100. the blocked fund's account has a balance of $98. Per OFAC regulations, the credit union must pay reasonably commercial interest on this account).

Special Licensing

If Family First Credit Union desires OFAC to consider releasing funds that have been blocked, it is possible to apply for a specific license. The credit union must provide certain information including, without limitation, the following:

- Name of the blocked entity/account holder
- Amount of blocked funds
- Date of blocking
- Copies of documentation related to the underlying transaction
- Documentation of the transaction

- Justification for the release of funds

Important OFAC Reports

There are a number of important reporting requirements for OFAC. However, the most important are:

1. Any transaction that has been blocked or rejected must be reported to OFAC within ten business days, from the date the property became blocked (see the OFAC Submission Report).
2. An annual report of all property blocked as of June 30 are due by September 30 of each year. (See the Annual Report of Blocked Property).
3. OFAC requires the retention of all reports and blocked or rejected transaction records for five years.

Please refer to the Appendix for a sample OFAC Submission report as well as for the Department of the Treasury's OFAC reporting documentation.

OFAC Submission Reports

Any transaction that has been blocked or rejected must be reported to OFAC within ten business days.

Blocked Transaction Reporting Information

1. The Credit Union's name and address (as holder of the account)
2. The name, title and phone number of the person that OFAC should contact for further information regarding the transaction or account.
3. Full information about the transaction including:
    a. Full name of the owner or account party
    b. A description of the property
    c. The location of the property
    d. Type of transaction, account or description of the property
    e. Amount (actual or estimated)
    f. Date of transaction
    g. Date of report filing
    h. Status and location of the account
    i. Any information necessary to identity the property
4. Confirmation that the property has been placed into a clearly identifiable, new or existing blocked account containing the name or (or interests of) the entity subject to blocking.
5. Name and phone number of the contact Compliance Officer.
6. A photocopy of any written instruction received concerning the transaction.

Rejected Transaction Reporting Information

1. Full information about the transaction including:
    a. Name and address of the Transferee Credit Union
    b. Date of the transfer
    c. The amount of the transfer
    d. Basis for rejection
2. A photocopy of the payment and/or any transfer instructions received

3. Name and phone number of the contact Compliance Officer at the Transferee Institution.

In addition to a submission report, the Credit Union must also submit photocopies of any applicable transfer/payment instruction, and confirmation that the funds are placed in a clearly marked account upholding the name/Interests of the entity subject to blocking.

Demonstrating OFAC Compliance

To ensure compliance, Family First Credit Union will have a clear and thorough policy and procedure manual, educate and train their employees accordingly, and possess an efficient, in-depth compliance system that allows for the proper handling of all transactions and members.

In a further demonstration of OFAC compliance, Family First Credit Union will maintain a list of all the false positive matches to help to identify other false positive matches in the future and to help demonstrate that we are checking our current member list and transactions for potential OFAC matches.

OFAC Violations

If Family First Credit Union believes it may have violated OFAC laws or regulations, we will contact the OFAC Counsel immediately.

OFAC may take the following factors into consideration when determining whether to levy civil or criminal penalties for an OFAC violation:

1. The extent of Family First Credit Union's compliance efforts
2. The comprehensiveness of the OFAC compliance policies and procedures.
3. How long Family First Credit Union monitors transactions for compliance with the OFAC regulation and laws (e.g. whether it uses interdiction software, etc.).

Annual Independent Audit

An annual independent audit to verify Family First Credit Union's system of internal controls and test for ongoing compliance with the OFAC regulations will be conducted by a designated auditor (internal audit, supervisory committee, CPA firm, etc.). A written report of this audit will be signed, dated and maintained for review by the NCUA examiners, with copies sent to management, the BSA compliance officer, and the supervisory committee.

Paperwork Reduction Act Statement

The paperwork requirement has been cleared under the Paperwork Reduction Act of 1980. The Office of Foreign Assets Control of the Department of the Treasury requires this information be furnished pursuant to 50 U.S.C. 1701 and CFR Parts 500 to 600. The information collected will be used for U.S. Government planning purposes and to verify compliance with OFAC Regulations. The information will be held confidential. The estimated burden associated with this collection of information is 4 hours per respondent of the record keeper. Comments concerning the accuracy of this burden

estimate and suggestions for reducing this burden should be directed to the Compliance Programs Division, Office of Foreign Assets Control, Department of the Treasury, Washington, D. C. 20220, and the Office of Management and Budget, paperwork Reduction Project (1505-0164), Washington, D.C. 20503. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number assigned by OMB.

In General, to assure the credit union's compliance with the Office of Foreign Assets Control, all of the officers of the Board and all members of the credit union staff will review the procedure for monitoring accounts an annual basis. The compliance officer will ensure proper training is provided to the credit union staff annually.

Family First Credit Union

Deposit Account Policy
OFAC Policy and Procedure Guide
Individual Name Verification

Family First Credit Union will verify the identity of persons benefiting from the following types of transactions by conducting an individual name search on the SPECIALLY DESIGNATED NATIONALS AND BLOCKED PERSONS list using the following URL.

https://www.treasury.gov/ofac/downloads/sdnlist.pdf

Every type of financial transaction should be reviewed for OFAC compliance including, without limitation, the following:

- Deposit accounts (checking, savings, etc.)
- Loans
- Lines of credit
- Letters of credit
- Wire transfers
- ACH transfers
- Depositing or cashing checks
- Purchase of bank checks or cashier's checks
- Loan payment
- Guarantors and collateral owners
- Trust account
- Credit Cards
- Cashed checks
- Safety Deposit Box entry

The names of all parties to a transaction should be checked against the list of names of individuals, entities, geographical locations or countries that have been identified by OFAC. This includes, but is not limited to the following (as applicable):

- Beneficiaries
- Collateral Owners
- Guarantors/Cosigners
- Receiving Parties
- Sending Parties
- Deputies and/or Agents of Safe Deposit Boxes
- Non- Credit Union members cashing checks in excess of $3000.00.

Family First Credit Union
Deposit Account Policy
Member Due-Diligence and Monitoring Program

MONITORING

Fulton Teachers Credit Union will enact procedures to monitor and identify unusual activity. The Compliance Officer or a designated employee is responsible for monitoring the system for fraudulent and suspicious activity.

Unusual account activity is monitored daily by the Compliance Officer or a designated employee with the following CUnify reports:

1. **Security Overrides** – review transactions made by staff outside their normal system parameters.

2. **Excessive Transactions** – Transactions in excess of $10,000

3. **BSA Report** – cash-in, cash-out, and cashed check information on accounts. All aggregated totals of $3000.00 and above for a member are reported. Transactions are lobby and drive-thru, drop-box mail, and ATM transactions.

4. **Kiting Report** – Same transactions for a member with a minimum deposit, withdrawal, or draft of $1,000.00. This report searches for transactions that may indicate kiting activity within the credit union.

5. **OFAC Report** – currently working with CUnify to begin monitoring (07/17).

6. **Monetary Instrument Log** – reviewed monthly to detect possible money laundering activity. A sale of any Official Check, FlashCard, or Gift Card with a Value between $3000.00 and $10,000.00 is recorded.

Family First Platinum Credit Card reports are monitored daily by the Compliance Officer or a designated employee to manage risk and expose unusual and fraudulent activity.

1. **Daily Foreign Transaction Listing** – monitor transactions outside the US.

2. **Daily Authorization Activity** - monitor cash transactions that may qualify for CTR reporting. Look for $1.00 authorizations which may be an indicator of fraud.

3. **Maintenance Lost/Stolen Report** – review accounts reported as stolen or lost. These accounts should not have activity once reported.

4. **Activity on Blocked Accounts** – the following actions should be taken: transfer transaction to the new account; contact cardholder to discuss charge with them and determine validity or submit institution chargeback to Fidelity National Information Services.

5. **Outstanding Temporary Stolen Blocked Accounts** – back up from Activity on Blocked Accounts

6. **Stolen Account Report** – review accounts with an S/S block. These accounts are not being investigated for fraud.

7. **SF Stolen Account Report** – accounts on this report are blocked and are currently being investigated for fraud.

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. For high-risk members, the Credit Union will obtain the following information at account opening and throughout the relationship:

(i) The purpose of the account.

(ii) Source of wealth and funds.

(iii) Beneficial owners, if any.

(iv) Member's (or beneficial owner's) occupation type of business.

(v) Residence

(vi) Proximity of residence, place of employment or business to the Credit Union.

(vii) Explanations for changes in account activity.

Family First Credit Union
Deposit Account Policy
Electronic Fund Transfer Act Policy

Purpose
The Electronic Fund Transfer Act as implemented through Regulation E was enacted to protect the rights of individuals with regard to transfers of funds involving electronic access to accounts through the use of automatic teller machines, point-of-sale terminals, and preauthorized transfers to and from accounts. The regulation requires Family First Credit Union to make certain disclosures for electronic funds transfers relating to limitations on the transfers, fees charged for making a transfer, the error resolution process, and the potential liabilities of the member, as well as those of the credit union.

Policy Statement
It is the policy of Family First Credit Union to comply with the requirements of Regulation E. All required disclosures will be clear and readily understandable, in writing, and in a form, the member may keep.

Initial Disclosure Requirements
The terms and conditions of Electronic Fund Transfers for a member's account must be disclosed before the EFT service has been initiated. The disclosure must be substantially in the form provided by the Federal Reserve Board's Regulation E.

Subsequent Disclosure Requirements
Family First Credit Union will mail or deliver a written notice at least 21 days before the effective date of any change in a term or condition required to be disclosed by Regulation E if the change results in:

- Increased fees for the member;
- Increased liability for the member;
- A decrease in the available types of electronic funds transfers; or
- Stricter limitation on the frequency or dollar amount of transfers.

Conditions for liability

A member may be held liable for an unauthorized electronic fund transfer or a series of related unauthorized transfers involving the member's account only if Family First Credit Union has provided the disclosures required by Regulation E.

- Timely notice given – If the member notifies the credit union within two business days after learning of the loss or theft of the access device, the member's liability shall not exceed the lesser of $50.00 or a number of unauthorized transfers that occur before notice to the credit union.
- Timely notice not given – If the member fails to notify the credit union within two business days after learning of the loss or theft of the access device, the member's liability shall not exceed the lesser of $500.00 or the sum of:
    - $50.00 or the amount of unauthorized transfers that occur within the two business days, whichever is less; and
    - A number of unauthorized transfers that occur after the close of two business days and before notice to the credit union provided the credit union establishes that these transfers would not have occurred had the member notified the institution within that two-day period.
- Periodic statement; timely notice not given - A member must report an unauthorized electronic fund transfer that appears on a periodic statement within 60 days of the credit union's transmittal of the statement to avoid liability for subsequent transfers. If the member fails to do so, the member's liability shall not exceed the number of the unauthorized transfers that occur after the close of the 60 days and before notice to the credit union, and the credit union establishes would not have occurred had the member notified the credit union within the 60-day period. When an access device is involved in the unauthorized transfer, the member may be liable for other amounts set forth timely and untimely notices given.
- Extension of time limits – If the member's delay in notifying the credit union was due to extenuating circumstances, the credit union shall extend the times specified above to a reasonable period.
- Notice to Family First Credit Union
    - Notice to the credit union is given when a member takes steps reasonably necessary to provide the credit union with the pertinent information, whether or not a particular employee of the credit union actually receives the information
    - The member may notify the credit union in person, by telephone, or in writing
    - Written notice is considered given at the time the member mails the notice or delivers it for transmission to the credit union by any other usual means.
- Liability under state law or agreement – If state law or an agreement between the member and Family First Credit Union imposes less liability than is provided by this section, the member's liability shall not exceed the amount imposed under the state law or agreement.

Error Resolution Process
All errors will be resolved, and necessary adjustments made to the members' account within ten business days from the date of receipt of the member's notice. The results of the investigation will be provided to the member within three business days after the investigation is concluded. Family First Credit Union may extend the ten-business daytime limit to 45 calendar days from receipt of the notice if more time is needed to conduct the investigation. In these situations, the member's account will be credited within ten (10) business days for the amount in error.

Record Retention Policy
Family First Credit Union will retain all documentation relating to EFTs for at least two years. The credit union will also retain, until final disposition, records relating to any action filed under the Electronic Fund Transfer Act.

In General, to assure the credit union's compliance with the Electronic Fund Transfer Act, all of the officers of the Board and all members of the credit union staff will review the procedures for disclosing electronic funds transfers annually. The compliance officer will ensure proper training is provided to the credit union staff annually.