# SECTION XIV

# BANK SECRECY ACT

**Reviewed:** ***December 2018***
**Revised:** ***December 20, 2018***

# Table of Contents

**Page**

## I. Bank Secrecy Act

### Policy Statement

In general, it is the responsibility of Red Crown Federal Credit Union to report certain currency transactions to the Internal Revenue Service (IRS) and to maintain records relating to all currency and financial transactions for a specific period of time. Specifically, this law requires that the Credit Union report each deposit, withdrawal, and exchange of currency or other transaction involving in excess of $10,000 cash. It is the policy of Red Crown Federal Credit Union to report all cash transactions in excess of $10,000 by filing a Currency Transaction Report (CTR). It is the policy of Red Crown Federal Credit Union to report any activity over $5,000 deemed suspicious by the responsible officer or any insider activity deemed suspicious by filing a Suspicious Activity Report (SAR). It is the policy of Red Crown Federal Credit Union to have procedures in place to prevent and detect money laundering (Refer to Anti-Money Laundering Policy), and to verify the identity of its members (Refer to Member Identification Program). It is also the policy of Red Crown Federal Credit Union to retain all necessary financial records for the prescribed periods of time. In addition, this policy will provide guidance for employees and officers of the Credit Union in complying with the Bank Secrecy Act (BSA).

The Board designates the Internal Auditor(s), as the BSA Officer(s). The COO will serve as the backup BSA Officer. The Board has delegated responsibility for reviewing CTR's and SAR's to the Supervisory Committee. The Supervisory Committee will document their review in the monthly report to the Board.

A transaction in currency involves the physical transfer of currency. Transactions that are subject to the law include:

Currency transactions over $10,000, such as:

a. Deposits or withdrawals from any account,

b. Purchase or redemption of:
   Money Orders
   Travelers Checks
   Cashier Checks
   Investment Securities (i.e., CD's)
   Gift Cards

c. Domestic or foreign checks that are presented for cash,

d. Exchange of currency over $10,000 such as:
   Small to large bills,
   Foreign to U.S. currency, or vice versa

e. Payment on accounts (i.e., loans)

f. Multiple transactions aggregating more than $10,000,

g. Wire transfers (involving cash).

Transactions that are not subject to this law include the transfer of funds by means of a credit union check, credit union draft, wire transfer or other written order, which does not include the physical transfer of currency.

**Bank Secrecy Act Procedures**

A. For each cash transaction involving more than $10,000, or multiple transactions that aggregate more than $10,000, for one account or individual or on behalf of one individual, a currency transaction report (CTR) will be completed.

1. The teller may inform the member that this form is required by law and is not subject to waiver by an officer.
2. The form will be completed by the teller, downloaded into the system and retrieved by the BSA officer(s). The originals with supporting documentation will be retained in the RCFCU's BSA file for a period of five years. The CTR will be filed via BSA E-Filing, within 15 days of the date of the transaction, to:

FinCen-BSA E-Filing

B. The types of identification that will be allowed include:
1. Drivers license
2. United States passport
3. Military ID
4. Social Security card (under special circumstances)
5. State ID
6. Oklahoma carry and conceal license
7. Federally recognized Oklahoma Tribal Identification Card

C. Aliens or non-residents must present the following:
1. Permanent Resident Alien ID (issued by the United States government)
2. Passport
3. Tax identification number

D. All forms of identification must be valid and current.

E. Multiple transactions occurring on the same business day, involving the same account or individual or on behalf of the same individual, will be combined and a CTR completed, if they exceed $10,000. Large currency transaction reports will be reviewed daily by the BSA Officer(s) to ensure all CTRs are filed.

F. All cash transactions involving the transportation or receipt of currency to or from a foreign country will be reported to the BSA Officer(s) for review.

G. Exemptions:
Exemptions for CTR reporting will be granted to members who qualify.

Exemptions under Phase I are correspondent banks, government agencies and publicly traded companies. Members eligible for Phase II exemption are non-listed companies. Currently Red Crown does not have any exempt members.

1. Once an exemption has been granted the BSA Officer(s) will file a Designation of Exempt Person with the U.S. Department of Treasury, via BSA E-Filing Designation of Exempt Person.

2. The BSA Officer(s) will maintain a list of all exempted members.

3. All Phase II members will be monitored on an on-going basis for any unusual or suspicious activity or transactions. Any unusual or suspicious activity will be reported to the BSA Officer(s), and they will determine if a Suspicious Activity Report will be filed.

H. The tellers will record all sales of cashier checks or gift cards for $3000 or more in currency on a Monetary Instrument Transaction Log.

1. If the purchaser is a member, the following information will be obtained for the sale and entered on the Monetary Instrument Transaction Log. Transactions will reflect on the BSA Monetary Instruments report.
   a. Purchaser's name and account number,
   b. Date, Where, How the purchase was made,
   c. Type of instrument purchased,
   d. Serial number of instrument,
   e. Dollar amount of each instrument purchased.
   f. Method of identification.
   g. Copy of valid ID.

2. If the purchaser is not a member, the same information as in #1 above will be obtained for the sale and entered on the Monetary Instrument Transaction Log. Additionally, the following information will be gathered:

   a. Purchaser's address
   b. Purchaser's social security number (or alien identification number),
   c. Purchaser's date of birth

I. All filed CTRs, SAR***s*** and Monetary Instrument Transaction Log***s*** from each location will be maintained by the BSA Officer(s).

J. Records will be maintained for incoming and out-going wire transfers of $3000 or more for members and non-member recipients. The following records will be maintained and will be retrievable by name or account number.

1. Member name and address
2. Amount of wire order
3. Date of wire
4. Payment instructions
5. Identification of beneficiary and their financial institution

6. And any of the following items received: name and address of beneficiary, account number of beneficiary, and any other specific identifier of the beneficiary, in accordance with the Travel Rule.

RCFCU does not receive wire transfers for non-members. Receipt of Payable Upon Proper Identification (PUPID) transfers are prohibited. Origination of PUPID transfers require the approval of an officer and are monitored for unusual activity.

K. RCFCU will follow applicable retention guidelines, including:

1. Extensions of credit over $10,000 including:
    a. Borrower's name and address
    b. Loan amount
    c. Purpose of the loan
    d. Loan date

2. Each advice, request or instruction received regarding a transaction which results in the transfer of funds or of currency or other monetary instruments of more than $10,000 to a person, account or place outside the United States.

3. Each advice, request or instruction, given to another financial institution or other persons located within or outside of the United States, regarding transactions intended to result in the transfer of funds, or of currency or other monetary instruments over $10,000 to a person, account or place outside the United States.

4. Taxpayer identification numbers for each account holder (individuals or corporate) of the credit union.

5. A list of individuals and corporations for which a taxpayer identification number has not been obtained.

6. Record of the name, address and ID number of purchases and presenters of certificates of deposit.

7. Additional record keeping requirements detailed in 31CFR 103.34(b) (i.e. signature cards, statements for each account, checks over $100, etc.).

L. The BSA Officer(***s)*** will be responsible for ensuring that necessary records are maintained and that they are secure and protected to the extent possible from theft, damage or destruction.

M. BSA records and supporting documentation will be maintained for a period of 5 years.

N. All requests for any of this information will be directed to the President/CEO or his/her designee. Procedures included in the Rights to Financial Privacy Act will be followed.

O. Information regarding all suspected violations of the law will be forwarded to the NCUA regulatory agency and the appropriate federal law enforcement officials.

P. It is possible that an employee may become aware of or suspect criminal activity by a member or another employee(s). Any such suspicions are to be reported promptly to the President/CEO or BSA Officer(s), and will not be discussed with anyone else.

Q. The BSA Officer(s) will file a Suspicious Activity Report (Attachment C) for any activity over $5000 deemed suspicious. All accounts involved will be added to the high-risk account list. Ongoing monitoring of account(s) will be performed by the BSA Officer(s). If activity continues after a review of 90 days, the member relationship will be re-evaluated to determine if the credit union should terminate the relationship.

R. The BSA Officer(s) will file a Suspicious Activity Report for transactions involving criminal violations as follows: Insider abuse of any amount; transactions aggregating $5,000 or more when the suspect can be identified; transactions aggregating $25,000 or more regardless of a potential suspect. SARs reports are sent via FinCen BSA E-Filing

S. All SARs will be reported to the Supervisory Committee. The Supervisory Committee will report SAR activity to the Board on a regular basis.

T. The large currency transaction reports will be reviewed daily by the BSA Officer(s) for any unusual or suspicious activity including: transactions at or just under $10,000 for possible structuring; unusual wire activity; or other transactions not consistent with normal practices. The BSA Officer will file a Suspicious Activity Report when deemed necessary.

U. The BSA Officer(s) will maintain documentation regarding suspicious activities where a SAR was not deemed necessary.

V. All employees will be trained annually for compliance relating to BSA. Employees will be trained regarding record keeping requirements, anti-money laundering procedures, member identification procedures and suspicious activities.

W. The Board of Directors will appoint a BSA officer***(s)*** annually to oversee the BSA program. The BSA Officer***(s)*** will be responsible for ensuring that employees comply with the procedures set forth in this policy.

X. The Board of Directors will annually review and approve the BSA policy as per BSA requirements.

Y. An independent BSA review will be conducted annually. The review does not have to be performed by an outside source, however, if it is performed internally, the person conducting the review must be completely independent of day-to-day involvement in the BSA function. The person must be knowledgeable of BSA regulations. The review will include, at a minimum:

1. Annual Board approval of BSA and related policies
2. Annual appointment of BSA officer(s) by the Board
3. Annual training

4. Accuracy and filing of Currency Transaction Reports
5. Integrity of aggregation system
6. Designation of Exempt Persons Form
7. Biennial review of Phase II members
8. Documentation to support exemptions
9. Monetary instrument sales records
10. Wire transfer recordkeeping
11. Suspicious activity reporting
12. Member Identification Procedures
13. Anti-money Laundering Procedures
14. Correction of prior weaknesses

Z. Violations of the credit union's reporting requirements may subject the credit union, its employees and members involved to both civil and criminal liability. Under no circumstances will employees discuss these procedures with members or provide members with any advice as to how reporting requirements can be avoided. Employee violations of these procedures will be treated as a serious breach of credit union security and will be grounds of disciplinary action, including dismissal. Any violation of law or policy will be reported immediately to the President/CEO and/or BSA Officer(s).

## II. Anti-Money Laundering

### Policy Statement

It is the policy of Red Crown Federal Credit Union to identify and report to appropriate agencies any suspected money laundering conducted through the credit union. RCFCU will establish internal controls for money laundering detection and reporting to cover all operational areas of the credit union. These controls will focus on members, transactions, and geographic locations that lend themselves more readily to potential money laundering situations.

RCFCU will have an audit program to independently assess the effectiveness of the money laundering procedures. The audit will include reviewing transactions to insure proper suspicious activity reporting, employee training effectiveness, and the accuracy of present procedures.

All credit union employees, including new employees, will be part of an on-going training program covering money laundering detection procedures.

The BSA officer is responsible for managing and monitoring the compliance of this policy and for the filing of suspicious activity reports with appropriate agencies. All credit union employees will be instructed to report suspected money laundering situations to the BSA officer***(s)***, who will in turn report such situations to the Supervisory Committee of the credit union.

### Anti-Money Laundering Procedures

A. RCFCU will have procedures in place to identify and report potential money laundering. Money laundering usually includes one or more of the following areas:

1. **Placement,** the placing of unlawful cash proceeds into the credit union by deposits, wire transfers or other means.
2. **Layering**, the separating of the proceeds of illegal activities from their origins through the use of financial transactions such as converting cash into traveler's checks, money orders, letters of credit, securities, or valuable assets such as art, jewelry or precious metals.
3. **Integration**, using apparently legitimate transactions such as loans or forged or false documents to disguise illicit proceeds to allow laundered funds to be disbursed back to the laundering party.

B. Member account transaction reports will be monitored for any unusual activity. Monitoring will consist of, but will not be limited to:

1. Daily review of large currency transactions reports.
2. Weekly review of kiting suspect report;
3. Reviewing and investigating all insufficient or suspicious information from members;
4. Reviewing employee transactions and bank-to-bank transactions for unusual activity;
5. Reviewing unusual safe deposit box activity;
6. Reviewing loans paid off early;
7. Reviewing transaction activity of any member who is the subject of a law enforcement request.

C. RCFCU will review all member accounts to determine the accounts or members that could be considered "high-risk" members. These include, but are not limited to:

1. Members exempt from CTR filing;
2. Members with a high volume of cash transactions that do not meet the requirements for exempt members;
3. Nonbank financial institutions that are depositors of the institution (check cashing businesses);
4. Any other accounts for members or transactions that lend themselves more readily to potential money laundering situations.

D. All high-risk members will be added to a high-risk list and reviewed on a monthly basis by the BSA officer***(s)***. Monitoring will include:

1. Reviewing account transaction histories for any inconsistent activity;
2. Reviewing all payable-through accounts;
3. Reviewing all funds transfers for unusual transfers.

On an annual basis high-risk members and accounts will be re-evaluated to determine if the member and/or account activity continues to warrant designation as high-risk. If no suspicious activity or unusual transactions have occurred in the previous twelve-month period, the member will be removed from the high-risk list.

E. All credit union personnel will adhere to Red Crown's Member Information Program (MIP) for all transactions.

F. Any unusual activity will be reported to the President/CEO or BSA officer(s) immediately. The BSA officer***(s)*** will further investigate and monitor any reported transactions or activities. The BSA officer(s) will report all suspected money laundering situations to the Supervisory Committee and will file a Suspicious Activity Report with the appropriate agencies.

G. A credit union wide risk assessment to identify potential money laundering and terrorist financing risks will be conducted on an annual basis.

**Money Service Business Accounts**

A. A Money Service Business (MSB) is a commercial account involving a large volume of exchanges of currency for negotiable instruments. Defined by FinCen to include five distinct, types of financial services providers and the U.S. Postal Service: (1) currency dealers or exchangers; (2) check cashers; (3) issuers of money orders, or stored value card; (4) sellers or redeemers of money orders or stored value; and (5) money transmitters. There is a threshold requirement for businesses in the first four categories – a business that engages in such transactions will not be considered a money services business if it does not engage in such transactions in an amount greater than $1,000 for any person on any day in one or more transactions.

Currently RCFCU does not have any MSB accounts, however should we have any in the future, the following will be obtained before the account is opened.

1. Proof of registration with FINCEN and applicable state licensing;
2. Written anti-money laundering procedures of the MSB;
3. Written compliance program, including procedures for the following:
   a. Filing Currency Transactions Reports when necessary
   b. Record-keeping requirements for the sale of monetary instruments
   c. Record-keeping requirements for funds transfers
   d. Record-keeping requirements for currency exchanges
   e. Written OFAC program.

In addition, the credit union will also interview appropriate personnel to determine the MSB's targeted customer base, anticipated activity, list of services offered, if international wire transfers are conducted, and any limits or restrictions on services offered.

All MSB accounts will be monitored and reviewed by the BSA Officer***(s)*** for any unusual or suspicious activity and SAR will be filed when necessary. In the event RCFCU should feel the MSB is not complying with regulatory requirements, the account will be closed.

## Comparison with Governments Lists

1. Membership Accounts

RCFCU will screen new accounts as they are opened and use a third party system to compare established members with the Office of Foreign Assets Control (OFAC). FinCen files are downloaded whenever available and imported into ChoicePoint's Bridger System for checking OFAC compliance. The entire RCFCU membership data files are checked against the OFAC list each time the list is updated or at least once a month through core processor.

2. Loans

A credit bureau report is required for all new members seeking a loan. All credit bureau reports are compared against the most recent OFAC list. All makers, co-makers, dealerships, sellers of collateral and guarantors will be compared with the OFAC list before the loan is funded. Any suspicious situation, particularly share loans secured by certificates purchased with cash, will be reported to the BSA Officer***(s)***.

3. Wire Transfers

All nonmember originators and beneficiaries of wire transfers will be compared with the most current list of known or suspected terrorists or terrorist organizations provided by OFAC before a wire transfer is sent or before funds are disbursed.

4. International ACH Transactions (IAT)

All parties involved in an IAT transaction will be checked against OFAC prior to processing. This will be the responsibility of the CFO/Controller and/or person processing the IAT transaction. If any party to the IAT transaction is located on the Specially Designated Nationals (SDN) list, the transaction must be rejected and properly coded as a blocked transaction in the ACH system until further investigated. The BSA Officer***(s)*** and/or CFO/Controller should be notified.

**Procedures When a Name Appears on the List Provided by OFAC**

1. Verify the validity of the match.
   If a name being compared to the list provided by OFAC appears to be a match, RCFCU will verify the validity of the match by the following:
   a. Does the entire name match, or only a portion of the name;
   b. Is the address the same; and/or
   c. Is the date of birth or SSN/EIN the same?

2. If there are discrepancies in the validity of the match, RCFCU will record how the discrepancies were determined, maintain the records, and disregard the notification. If RCFCU cannot determine that the match is inaccurate, the OFAC Compliance Hotline will be notified. RCFCU will follow all instructions provided by the OFAC Compliance Hotline and will record and maintain all documentation.

**Blocking Funds**

If the OFAC Compliance Hotline instructs RCFCU to block the funds, the following will be done:

1. Place the funds in a membership account which earns dividends.

2. The name on the account should be titled the way it appears on the OFAC list and the account should be flagged with a permanent hold.

3. Within ten (10) days of blocking the account, a report will be filed with OFAC. The report will be sent electronically to the OFAC Compliance Programs Division and will contain the following, as applicable:

   a. Identity of the owner or account party
   b. The property and the location of the property;
   c. The account number of the property
   d. Actual or estimated value
   e. The date of the blocking; and
   f. A copy of the transfer or payment instructions and the name and address of the blocking institution;
   g. Name and telephone number of contact person.

An "Annual Report of Blocked Property" will be submitted to OFAC by September 30th of each year, effective as of June 30th. These reports will also be sent electronically to the OFAC Compliance Programs Division.

**Rejected Transactions**

If the OFAC Compliance Hotline instructs RCFCU to reject the transaction, within ten (10) days from rejecting the transaction, RCFCU will file a report with OFAC, containing the following:

1. Name and address of the transferee bank, the date and amount of the transfer;
2. Copy of the payment or transfer instructions received; and
3. The basis for rejection.

### Financial Crimes Enforcement Network (FinCEN) Requests

FinCEN's Section 314(a) requests are communications sent to financial institutions requesting acknowledgement of accounts with individuals and entities who are suspected of engaging in money laundering or terrorist financing activities.

The BSA officer***(s)*** will be responsible for ensuring that all 314(a) requests received are researched accurately and in a timely manner. After the requests have been researched, the 314(a) form will be shredded. The BSA officer(s) will keep a record of the tracking number, the date searched, the number of names searched and the findings for a period of five years. All names appearing on the 314(a) requests will be verified against the following:

1. The credit union's database for any active accounts
2. Paid accounts for the previous twelve months
3. Wire transfers of $3,000 or greater for the last six months
4. Currency Transaction Reports for the last six months
5. Monetary instruments purchased with cash of $3000 or greater during the last six months.
6. If a "hit" or "match" is received, contact FinCen to report the "match".

RCFCU has elected to file FinCEN form 314(b), which allows sharing of account information with other banking institutions. The BSA officer is responsible for receiving and providing information. Information received will be kept confidential and protected in accordance with the credit union's Information Security Program. RCFCU will establish a process for sending and responding to requests, and will ensure that the requesting party has filed the proper notice. The BSA officer***(s)*** will determine if information received or provided warrants the filing of a Suspicious Activity Report.

### Audit Program

An independent audit will be conducted annually of RCFCU's anti-money laundering program. The audit will include, at a minimum, the accuracy of present procedures, the effectiveness of employee training and reviewing transactions to ensure Suspicious Activity Reports are filed when required.

All audit findings will be reported to the Board of Directors. The BSA officer(s) will be responsible for correcting any deficiencies identified during the audit.

## III. Member Identification Program (MIP)

The Member Identification Program is designed to, at the time of account opening, provide reasonable assurance of the member's true identity and thereby assist in the prevention and detection of money laundering and/or financing terrorism. It also serves to deter those who would attempt to defraud the credit union. "Account" contemplates both deposit and lending relationships as well as other on-going service relationships.

## Definitions

### Member
For the purposes of this program, a member is an individual or legal entity that is opening a new membership account with Red Crown. It also means an individual who is opening a new account for another individual who lacks legal capacity (such as a minor or an incompetent) or for a group that has not formed a legal entity (such as a civic club). In the case of a joint account, it means each of the member/signer who does not already have a membership here.

### Account
For purposes of this program, an account is a formal banking relationship established to provide services or engage in financial dealings or services. It includes deposit accounts; loans and other forms of credit, safe deposit box rentals, safekeeping services, cash management, and custodian and trust services. It does not include such relationships if they are acquired through merger, acquisition, or purchase and assumption. It also excludes check cashing, wire transfer, and sale of a cashier check or money order, if no formal banking relationship, as described earlier in this paragraph, is established.

### U.S. Persons.
For purposes of this program, a "U.S. Person" is an individual who is a United States citizen, by birth or naturalization, or a person (other than an individual) that is established or organized under the laws of the United States of one of its states.

### Exceptions
This program needs not be applied to members who are federal, state, or local government entities, nor to companies whose common stock is listed on the New York or American stock exchange or on the NASDAQ National Market System (other than the small-capitalization segment of the NASDAQ NMS). It also need not be applied to a financial institution that is subject to regulation by a federal functional regulator, or to a bank regulated by a state bank regulator.

### Existing Members
RCFCU has a reasonable belief that it knows the true identity of each individual or entity that has had an account since October 1, 2003 and will not apply this program to such members. Exceptions to this provision may be made and identifying data may be collected and verified, at-any time on a customer, by the discretion of the staff handling a transaction or by the Bank Secrecy Act Officer***(s)*.**

### Member Information Required
RCFCU will obtain, at a minimum the following information for the member prior to opening an account:

1. Name
2. Date of Birth, for an individual
3. Address which shall be:
   a. For an individual, a residential or business street address:
   b. For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number or the residential or business street

address of next of kin or of another contact individual. A PO Box as a statement mailing address is acceptable, only if a residence address is given also.

4. SSN, or tax payer identification number
5. RCFCU will follow BSA identification requirements.

Acceptable forms of identification are:

1. Driver's License, with current residence address.
2. United States Passport
3. State issued ID card
4. Military ID
5. Oklahoma carry and conceal license
6. Federally recognized Oklahoma Tribal Identification Card

RCFCU will obtain, at a minimum the following information for a non-US citizen, in addition to the above:

A photo ID and three of the following valid and current documents:

1. Social Security card.
2. Passport Number and the country that issued it
3. Permanent Resident Alien ID card.
4. Government-issued document that provides evidence of nationality or residence, document # and country should be included.

**Exceptions for persons applying for a taxpayer identification number:**
Instead of obtaining the taxpayer identification number from a member prior to opening a membership, RCFCU will obtain a copy of the application before it opens or adds a signatory to the account and obtain the taxpayer identification number within sixty days after the account is established or a signatory is added to the account. In the event the member has not received the identification number within the sixty day period, the time period may be extended until such time the number is received if the credit union (1) sends a request, in writing, to the member and (2) the member provides evidence that the application for the identification number has been filed.

***Member Business Accounts/Beneficial Ownership***

RCFCU will obtain, at a minimum the following information for non-individual accounts in addition to the above ***member information required*****:**

1. The address of the principal place of business.
2. Photocopy of Articles of Incorporation, Partnership Agreement, Trust Instrument, or other operating agreement.
3. Employer Identification Number
4. If the entity is considered a high-risk account (see pg. 8 C), member information will be obtained on each individual with control of the account.
5. If documentary evidence of an entity's existence is not available, (e.g. sole proprietorships and informal partnerships) member information will be obtained on each individual with authority or control over such account.

6. ***RCFCU will identify and verify the identity of beneficial owners of legal entity members, subject to certain exclusions and exemptions, each time a new account is established. For this purpose, a new account includes the renewal of an existing account.***

   ***A legal entity member is defined as a corporation, limited liability company, other entity created by the filing of a public document with a Secretary of State or similar office, a general partnership, or similar entity that opens an account.***

   ***A legal entity member does not include sole proprietorships, unincorporated associates, or natural persons opening accounts on their own behalf.***

   ***A Beneficial Owner is defined as:***
   - ***Each individual who, directly or indirectly, owns 25% or more of the equity interest of a legal entity member (ownership prong)***
   - ***A single individual with significant responsibility to control, manage or direct a legal entity member, including an executive officer or senior manager, such as the CEO, CFO, COO, Managing Member, General Partner, President, Vice President, or Treasurer, or any other individual who regularly performs similar functions (control prong)***

   ***Prior to account opening, RCFCU will obtain, from the individual seeking to open a new account on behalf of the legal entity, identifying information for all beneficial owners, including name, physical address, date of birth, and an identifying number (SSN, passport, etc.***

   ***RCFCU will verify identifying information for each beneficial owner by following RCFCU's MIP requirements. In the event RCFCU cannot form a reasonable belief that it knows the true identity of each beneficial owner, the account will not be opened or renewed. The BSA Officer will be notified in the event of possible identity theft or intentional misrepresentation, who will determine if a Suspicious Activity Report is needed.***

   ***In the event of a renewal of an existing account, or in the instances where beneficial ownership has been previously obtained and verified, RCFCU may allow the individual opening the account to certify that the original information regarding the beneficial owners is still accurate, in which case RCFCU may rely on previously maintained documentation as long as all documentation on file is current.***

   ***Record Keeping/Retention***

   ***RCFCU will obtain and retain Certification of Beneficial Ownership/Recertification of Information forms and information pertaining to the individual opening the account on behalf of the legal entity, beneficial owners and any documentation utilized in verifying the beneficial owner's identity. Any discrepancies and accompanying resolutions will also be documented on the form.***

***All indentifying information, certification forms or equivalent will be maintained for a period of five years after the legal entity's account is closed. Verification records will be retained for a period of five years after the record is made.***

**Field of Membership**:
Any individual or legal entity is eligible for membership if they live, work, worship, volunteer or attend school in the eight (8) counties RCFCU serves. Membership eligibility will be noted at account opening.

**Online Account Opening and Non Face-to-Face Transactions**
When an account is opened or a signatory added where the member is not physically present, RCFCU will follow BSA requirements**.**

**Indirect Lending**
New account applications received through indirect lending must include all documents required to positively identify the potential member. Indirect loans will not be funded until the required documentation is received. The designee of the President/CEO is responsible for internal controls to ensure compliance with this policy.

**Member/Customer Identification Checklist**
Immediately following the account opening process, the risk of each individual on the account will be evaluated using the CIP checklist. The ratings of risk for the type, size, deposit method and source of funds should be noted based upon a predetermined table listed in the new account opening procedure.

**Discrepancies**
During the account opening and member identification process, any substantive discrepancies must be resolved and documented. If discrepancies cannot be resolved within thirty (30) days, the relationship will be terminated. If phony ID or ID theft is suspected, the BSA officer must be informed immediately to determine if a SAR should be filed.

**Record Keeping / Retention**
A Member Identification Form will be completed for all members opening a new account or adding a signatory to an account RCFCU will retain documents as set forth in BSA guidelines.

**Member Notification**
The Credit Union will provide adequate notice to its members that the Credit Union is requesting information to verify their identities in accordance with federal law. Written notice will be displayed at each Credit Union location.

**Government Lists**
At the time of account opening, all new members will be compared to any government list of suspected or known terrorists as required under Section 326 of the USA Patriot Act. Any possible positive response is handled in accordance with any federal directives regarding the particular list involved.

The Bank Secrecy Act Officer(s) is responsible for monitoring the Member Identification Program and adherence to required internal procedures.

## BSA/AML RISK ASSESSMENT

### OBJECTIVE

To identify the Credit Union's BSA/AML risk of being used to launder money or finance terrorist activity. Through an analysis of the Credit Union's size, location, products and services offered, methods of opening accounts, the Field of Membership (FOM) and operational issues, management has determined the credit union is at a low to moderate risk of being used to launder money or finance terrorism.

Size – Assets as of 03/31/2018 $200,643,160 with a membership of 23,562

### LOCATION/GEOGRAPHY

Red Crown Federal Credit Union's main office is located in Tulsa County, OK and the membership is open to eight (8) counties, which are: Creek, Mayes, Okmulgee, Osage, Pawnee, Rogers, Tulsa, and Wagoner. These counties are included in the North Texas High Intensity Drug Trafficking Area (HIDTA).

Red Crown FCU has four (4) branches and they are located:

| | |
|---|---|
| 5001 E 91st St<br>Tulsa, OK 74137<br>(Main) | 5321 E. 41st Street<br>Tulsa, OK 74135<br>(Midtown) |
| 3101 W Kenosha<br>Broken Arrow, OK 74012<br>(Broken Arrow) | 19 N Rowe<br>Pryor, OK 74361<br>(Mayes County) |

**Overall Risk: Moderate**

### ACCOUNTS/SERVICES OFFERED

The credit union's products and services are conventional in nature. In addition to regular share/share draft and business accounts and basic services, the credit union offers the following:
Term Share Certificates and IRA accounts
Electronic banking
Mobile Banking
Online Account Opening
Electronic payment Automated Clearing House (ACH), Bill Payer
Monetary Instruments - Cashiers checks, and gift cards
Wire transfers (Domestic and Foreign)
Credit Union Service Centers
Merchant Capture
Loans (Secured and Personal)
Indirect Loans
Credit Cards/Debit Cards
Gifts Cards
Safe Deposit Boxes
Third Party Insurance Credit Life and Disability
NO international trade
NO Foreign accounts
NO trust or asset management accounts for members
NO Money Service Businesses (MSB's)
See attached matrix for detailed assessment of areas of service

**Overall Risk: Low**

**MEMBERS**

Field of Membership (FOM) is open to anyone that lives, works, worships, attends school or volunteers in Creek, Mayes, Okmulgee, Osage, Pawnee, Rogers, Tulsa, and Wagoner County Oklahoma. Immediate family members of existing Red Crown members are also eligible to join. The credit union has no overseas branches or correspondent accounts outside the US.

**Overall Risk: Moderate**

SUBPOENAS

RCFCU will comply with criminal subpoenas when presented, and will verify authenticity of authorities before any information is given.
BSA Officer(s) will handle and maintain all information pertaining to subpoenas.

**Customer Identification Program (CIP)**

A CIP program has been established and is outlined in the Bank Secrecy Act Policy.

**OFAC/FinCen 314(a)**

RCFCU's member base is conservative in nature. OFAC policy and procedures are in place. The FinCen 314(a) alerts are directed to the BSA Officer(s) and CFO/Controller for purpose of identifying persons of interest. RCFCU uses the core processing system to run the membership and FinCen 314(a) alerts. RCFCU has not had any positive queries.

**Overall Risk: Low**

**Personnel Turnover**

RCFCU has low turnover of key personnel, but frontline personnel in branches change periodically.

## Compliance

Authority and accountability for compliance is clearly defined and enforced, including the designation of a BSA Officer(s). Independent testing is in place and effective. The Board of Directors has approved a BSA compliance program that includes policies, procedures, controls, and information systems that are adequate.

## Training

Training is scheduled at least annually (new employees upon hire), is appropriate, effective, covers applicable personnel, and necessary resources have been provided to ensure compliance.

# BSA RISK ASSESSMENT

May 2018

| Area / Service | Credit Union Risk | Regulatory Risk | Mitigation | Rating |
|---|---|---|---|---|
| Cash Transactions | Potential money laundering, potential structuring | Failure to maintain proper records (CTR, Monetary Instrument Log, etc), failure to file required records | Large currency reports are reviewed daily, BSA Officer files CTRs, based on reports, tellers are trained regarding requirements, procedures are in place to identify possible structuring, high risk customers identified, reviewed for possible laundering. SARs filed when deemed necessary | (1) High |
| Suspicious Activity Monitoring | Potential money laundering, structuring, fraud, kiting | Potential inadequate anti-money laundering program | Employees are trained periodically regarding monitoring procedures. All employees have possible suspicious activity forms that are completed and forwarded to BSA Officer. High risk members are identified and monitored. Reports are reviewed and monitored for suspicious activity, including early loan payoffs, cash transactions, kiting suspects, overdrafts, etc | (1) High |
| Monetary Instruments | Potential money laundering, potential structuring, fraud | Fail to maintain proper records | ***It is the Credit Union's policy not to sell cashier's checks to non-members. Cashier's checks can be sold to members and shared branch members. Gift cards are sold to members, shared service branch and non-members per VISA agreement.*** BSA Officer reviews currency report for cash purchases of cashier's checks and gift cards. Tellers are trained regarding logs, procedures in place to monitor for possible structuring. | (2) Medium |
| Wire transfers | Potential ***money*** laundering, potential structuring, fraud | Failure to maintain proper records, failure to comply with the requirements of OFAC | Policy not to perform transfers for non-members. High risk members identified and monitoring for potential money laundering. Required records are maintained, procedures in place to monitor for possible structuring. International wires are performed through Fedline. All non-member beneficiaries and originators for all wires, domestic and international, are verified against OFAC. | (2) Medium |

# BSA RISK ASSESSMENT

May 2018

| Area / Service | Credit Union Risk | Regulatory Risk | Mitigation | Rating |
|---|---|---|---|---|
| Merchant Capture Process | Potential money laundering, fraud | Failure to comply with requirements of the USA Patriot Act. Failure to comply with requirements of OFAC. | Information Security policy and annual review on members account in addition to onsite review. | (3) Low |
| Mobile Banking | Potential money laundering, fraud | Failure to comply with requirements of MIP/CIP and OFAC, inadequate antimoney laundering procedures | Mobile banking is restricted to transactions within the member account. There is no direct access to the RCFCU database. Usage agreements are required from members who have access to A2A transfers. Daily limits and delayed controls are in place. Third party site is password protected behind a firewall. Multifactor authentication is required. | (3) Low |
| Money Service Businesses | Potential money laundering, potential structuring | Failure to perform proper due diligence, potential failure regarding CTR filing due to large cash volume. | Credit union does not have Money Service Businesses | (3) Low |
| Deposit Accounts | Potential money laundering, fraud | Failure to comply with requirements of the USA Patriot Act. Failure to comply with requirements of OFAC. | The credit union does not offer potential high-risk accounts, like trust management, pay-through accounts, etc. Employees are trained annually regarding MIP/CIP requirements, MIP/CIP sheets are completed for all new ***members*** . Accounts are not opened over the phone. Chexsystems is performed on all new account holders, OFAC is verified on all account holders, signors, PODs, and beneficiaries. High risk customers have been identified and monitored. | (3) Low |

# BSA RISK ASSESSMENT

May 2018

| Area / Service | Credit Union Risk | Regulatory Risk | Mitigation | Rating |
|---|---|---|---|---|
| Time Deposits | Potential money laundering, fraud | Failure to comply with requirements of the USA Patriot ACT, failure to comply with requirements of OFAC. | Employees are trained annually regarding MIP/CIP requirements. MIP/CIP sheets are completed for all new members. OFAC is verified on all account holders and signors. Beneficiaries may be verified when warranted. Employees are trained regarding potential, money laundering procedures are in place to monitor CD's purchased with cash. | (3) Low |
| Safe Deposit Boxes | Potential money laundering, fraud | Failure to comply with requirements of the USA Patriot Act. Failure to comply with requirements of OFAC. | Employees are trained annually regarding MIP/CIP requirements. MIP/CIP sheets are completed for all new members. OFAC is verified on all account holders, | (3) Low |
| | | | signors, and beneficiaries. Employees are trained regarding potential money laundering. | |
| Exempt Members | Potential money laundering, fraud | Failure to properly maintain records, potential to exempt ineligible businesses | The credit union does not have exempt members. | (3) Low |
| Lending Services | Fraud, possible money laundering | Failure to comply with requirement of the USA Patriot Act, failure to comply with the requirements of OFAC. | Employees are trained annually regarding MIP/CIP requirements. MIP/CIP sheets are completed for all new members. OFAC is verified on all account holders, co-signers, guarantors, and sellers of collateral and dealerships. Loan officers are trained regarding potential structuring using time deposits as collateral. | (3) Low |
| OFAC | Penalties due to OFAC violations | Failure to comply with requirements of OFAC | All members are verified prior to accounts being opened. Wire transfers are verified. Data base is verified periodically. At this time, the risk is considered low regarding monetary instruments. Possible limits may be established regarding payees. | (3) Low |
| Co-banks Investments | Potential money laundering | Potential inadequate anti-money laundering program | The bank does not have foreign correspondent banks. Investment portfolio is managed conservatively | (3) Low |

# BSA RISK ASSESSMENT

May 2018

| Area / Service | Credit Union Risk | Regulatory Risk | Mitigation | Rating |
|---|---|---|---|---|
| Internet Banking | Fraud | Failure to comply with requirements of MIP/CIP and OFAC, inadequate anti-money laundering procedures. | Internet banking is restricted to transactions within the member account or with designated accounts within the CU that the member is a signer on. Internet Banking includes Billpayer, which is managed by the member via a secure site. There is no direct access to the RCFCU database. Usage agreements are required from members who have access to A2A transfers. Daily limits and delayed transfer controls are in place. 3rd party site is password protected behind a firewall. Multifactor authentication is required. Member controls password. Wire origination is not offered. | (3) Low |
| ***Online Account Opening*** | ***Fraud Identity Theft*** | ***Failure to comply with requirements of MIP / CIP and OFAC.*** ***Failure to perform proper due diligence before account opening.*** | ***Potential members have to pass requirements based on criteria outlined in procedures.*** ***Account is not opened if potential member does not pass verification requirements.*** | |
| Employees | Fraud, Failure to comply with program | Potential inadequate BSA program | Employees are trained annually, and as needed. New employees are screened, with credit checks and reference checks. Historically low turn over in personnel. | (3) Low |

# OFAC RISK ASSESSMENT

December 2018

| Area / Service | Mitigation | Residual Risk |
|---|---|---|
| Deposit/Time Accounts | All owners of accounts are verified against OFAC prior to account opening. Signers on accounts are also verified against the OFAC list. We may verify beneficiaries when warranted. | Low |
| Loan Accounts/Indirect Lending | All borrowers are verified against OFAC prior to loan funding. Co-signers and guarantors, dealerships and sellers of collateral are also verified. Same procedures apply to loan applications received through indirect lending. | Low |
| Safe Deposit Boxes | Safe Deposit Boxes are opened only for members. OFAC is verified on each member at the time of account opening. | Low |
| Monetary Instruments | It is the credit union's policy not to sell monetary instruments (cashier's checks) to non-members. Red Crown sells cashier's checks to members and shared branch members. Gift cards are sold to members and non-members per VISA agreement. | Low |
| International ACH Transactions (IAT) | All parties involved in an IAT transaction will be checked against OFAC prior to processing. If any party to the IAT transaction is included on the Specially Designated Nationalists (SDN) list, the transaction is rejected and properly coded as a blocked transaction in the ACH System until further investigated. | Low |
| Wire Transfers | It is the credit union's policy not to perform wire transfers for non-members. All non-member originators and beneficiaries, both incoming and outgoing, are verified against OFAC. Outgoing wires are verified prior to submission; incoming wires are verified prior to funding. The credit union has not performed wire transfers to financial secrecy havens. | Low |
| Cashed Checks | Checks are not cashed for non-members unless the check is drawn on the credit union. | Low |
| Electronic Banking | ACH sources are verified against OFAC list monthly. International ACH are compared to the OFAC list as they come in. | Low |
| Internet Banking | Usage agreements are required from members who have access to A2A transfers. Daily limits and delayed transfer controls are in place. | Low |
| MSB's | The credit union does not have any registered Money Service Businesses | Low |

# OFAC RISK ASSESSMENT

December 2018

| Area / Service | Mitigation | Residual Risk |
|---|---|---|
| Merchant Capture /<br>Remote Deposit Capture | All account owners are verified against OFAC prior to opening and periodically for existing members | Low |
| Mobile Banking | All account owners are verified against OFAC prior to opening and periodically for existing members | Low |
| **Member Business Accounts / Beneficial Ownership** | **All account owners are verified against OFAC prior to opening and periodically for existing members** | **Low** |