# TABLE OF CONTENTS

## Introduction

## BSA Compliance Program & Risk Assessment

## Member Identification Program

## Member Due Diligence

## Currency Transaction Reports

## Monetary Instruments

## Funds Transfers

## Suspicious Activity Reports

## Office of Foreign Asset Control

## 314(a) and 314(b) Information Sharing

## Responding to Law Enforcement Requests

## Money Services Businesses

## Recordkeeping Requirements

---

*CUNA’s Bank Secrecy Act Compliance Guide is intended to provide useful information to assist credit unions in complying with the Bank Secrecy Act and Office of Foreign Assets Control requirements. CUNA is not engaged in rendering legal or other professional advice in presenting this information. This online manual contains CUNA copyrighted information and public information published by government agencies. While CUNA makes every effort to present reliable and accurate information, CUNA does not guarantee the accuracy of such information. In addition, CUNA does not endorse, approve, certify or control any of the “live” links to other Internet addresses which are provided for members’ convenience in accessing information not maintained on CUNA’s Web site.*
What is the Bank Secrecy Act?

Congress enacted the Bank Secrecy Act (BSA) in 1970, to assist law enforcement in the investigation and thwarting of money laundering, terrorist financing, tax evasion and other criminal activity. The “Act” is actually made up of several statutes, including the Money Laundering Control Act, the Anti-Drug Abuse Act, the Currency and Foreign Transactions Reporting Act, and most recently, the USA Patriot Act. These statutes work together toward the goal of detecting and curtailing criminal activity. In 1990, the Secretary of the United States Treasury Department created the Financial Crimes Enforcement Network (FinCEN) to administer the BSA, with the assistance of the federal regulatory agencies (including NCUA). FinCEN’s BSA regulations are codified at 31 CFR Chapter X.

[On March 1, 2011, FinCEN transferred its regulations from 31 CFR Part 103 to 31 CFR Chapter X as part of an ongoing effort to increase the efficiency and effectiveness of its regulatory oversight. 31 CFR Chapter X is organized by generally applicable regulations and by industry-specific regulations. Please note that documents published prior to March 1, 2011 will continue to contain citations to 31 CFR Part 103. Documents published on or after March 1, 2011 will contain citations to 31 CFR Chapter X.]

BSA “rigorous scrutiny” by examiners

 Examiner's scrutiny of BSA compliance programs has grown significantly over the years. FinCEN has adopted a “take no prisoners” attitude to money laundering and penalties are 10 times what they used to be. FinCEN and NCUA have an agreement in which NCUA examiners will give credit unions a “high risk” designation for all significant BSA violations, as well as a DOR and a 90 day return visit from the examiners to make sure all BSA violations have been addressed. Additionally, with a cease and desist order issued against a small credit union in 2014 due to BSA violations in connection with money service business (MSB) accounts, NCUA has directed its field staff to closely scrutinize all MSB accounts for BSA compliance.

And finally, credit unions are being called on to play a major role in the war on terrorism. The information from BSA Suspicious Activity Report (SARs) allows our military and our law enforcement to connect the dots between seemingly unrelated individuals. The FBI reported that approximately 18% of the Bureau’s international terrorism cases in 2014 had related BSA reports. You can expect your examiners to continue to scrutinize your BSA programs.

What must credit unions do to comply with the Bank Secrecy Act?

The BSA requires financial institutions (such as credit unions, banks, thrifts, money service businesses, some insurance carriers, etc.) to comply with certain reporting, recordkeeping and identity verification requirements. The BSA regulations establish four regulatory requirements for compliance. A credit union’s BSA program must incorporate policies/procedures that:

- Implement proper internal controls (such as internal procedures, checks/balances, etc.) to ensure that your BSA program is functioning as intended;
• Provide training for appropriate personnel, at least annually;

• Provide adequate annual independent audit procedures;

• Require the participation of a qualified and knowledgeable BSA officer; and

• Effective May 11, 2018, appropriate risk-based procedures for conducting ongoing legal-entity member due diligence.

The recordkeeping and reporting requirements under the BSA require a credit union to:

• Complete currency transaction reports (CTRs) which must be filed for currency transactions exceeding $10,000 (For more information go to CTR chapter);

• Complete suspicious activity reports (SARs) which must be filed in instances where there is suspected or known suspicious activity (such as the structuring of cash deposits and withdrawals to avoid currency transaction reporting, check fraud, loan fraud, credit card or debit card fraud, wire transfer fraud, embezzlement, etc.) (For more information go to SARs chapter);

• Capture certain information (such as name of purchaser, date of purchase, type of instrument, serial numbers, transaction amount and verification method) when monetary instruments are purchased within $3000 and $10,000 thresholds (For more information go to Monetary Instruments chapter); and

• Capture certain information (such as member’s name/address, amount, date, payment instructions, and beneficiary information—if available) when processing wire transfers in excess of $3000. (For more information go to Funds Transfer chapter)

Suspicious Activity: The BSA also requires institutions to put processes in place (manual or automated) to assist in the identification of suspicious or terrorist activity. This task will require the credit union to monitor the activity within its institution and the level of monitoring required should be dictated by the credit union’s assessment of risk---taking into account its high-risk products, services, members and geographic locations. This is not to say that a credit union is not expected to monitor activity in accounts considered low risk. However, the amount and complexity of activity monitoring for low risk accounts will differ substantially from that required for high-risk accounts. Credit unions have a great deal of flexibility to determine the appropriate monitoring system for the particular complexities of their businesses.

Customer (Member) Identification: In 2001, Congress enacted the USA Patriot Act in response to the September 11th terrorist attacks on New York City and the Pentagon. Title III of the Act amended the BSA. The resulting regulations required institutions to set minimum standards for the identification and verification of potential members. Section 326 of the Patriot Act required credit unions to implement member identification programs (MIPs). Under the
MIP/CIP, each institution is required to put procedures in place that will enable it to identify and verify the identity of potential members. A credit union’s MIP must be risk-based (i.e. designed to address the risks inherent in that institution’s membership) and must collect (at a minimum) four vital pieces of information during the account opening process: name, address, date of birth and identification number. *Note that Member Identification Program (MIPs) are the same as Customer Identification Programs (CIPs) for purposes of the BSA regulations and guidance.* (For more information go to [MIP chapter](#))

**Customer (Member) Due Diligence:** In addition to these provisions, a credit union is expected to implement member due diligence procedures that are designed to assist the credit union in developing an accurate picture of the normal and expected activity of its members. The revised Federal Financial Institutions Examinations Council’s (FFIEC) BSA/AML Examination Manual refers to this as “customer due diligence” or “CCD”. Effective May 11, 2018, credit unions are now required to identify and verify the beneficial owners of legal entity accounts.

According to FinCEN, the BSA/AML manual is designed to provide comprehensive guidance to examiners (including NCUA examiners). Due diligence procedures should be designed to help the credit union obtain sufficient information (beyond the four pieces of CIP information) to develop a level of comfort with its member’s expected account activity, as well as aid in the identification and thwarting of suspicious and potentially criminal activity. (For more information go to [MDD chapter](#))

**Information Sharing:** The USA Patriot Act also contains information sharing provisions. Section 314(a) of the Act requires credit unions to respond to requests for information regarding suspected terrorists or money launderers. Credit unions are required to search their records for any possible matches on FinCEN’s list of suspects. Section 314(b) of the Act permits financial institutions to share information with one another in order to better identify and report activities that may involve money laundering or terrorist activities. (For more information go to [Information Sharing chapter](#))

**Foreign Asset Control:** Although not a part of the BSA, a credit union’s responsibilities under Office of Foreign Assets Control (OFAC) regulations are a necessary component in the fight against money laundering and terrorist financing. OFAC issues lists of people, organizations, and countries that are prohibited from “doing business” (i.e. receiving/sending funds or opening accounts) within the United States. All credit unions must check the names of people who want to open accounts, take out loans, wire money, purchase money orders, and conduct other transactions against the OFAC list. In the event of a match, the credit union must block or freeze property and/or fund payments and report the match to OFAC. The OFAC list can be accessed via the Department of Treasury’s website. (For more information go to [OFAC chapter](#))

**Risk Assessment:** According to NCUA, credit unions must use a risk-based approach when developing their programs. The revised Federal Financial Institutions Examinations Council’s (FFIEC) BSA/AML Examination Manual states that a financial institution’s risk assessment...
Introduction

process should involve two steps: (i) the identification of specific risk categories (“risk profile”) through a review of the products, services, members, and geographic locations of a particular credit union, and (ii) the completion of a detailed analysis of the data identified in the risk profile which is used to develop processes/procedures to manage identified risks.

Such an approach requires the credit union to examine its business (across the institution), rank the business categories according to their inherent risks, and create a BSA/AML program designed to manage those risks.

The risk assessment should be considered the foundation of a BSA/AML compliance program. Without completing a comprehensive and thoughtful risk analysis of its business, it is highly unlikely that a credit union can design an effective program well suited to manage the risks of that particular institution.

Credit unions should perform a thorough risk analysis prior to the development of a BSA/AML program, especially larger credit unions with complex business operations. There is no “one-size fits all” approach to developing this assessment and a standard credit union template is unlikely to work. NCUA acknowledges that there is potentially more than one-way to manage a particular risk and has encouraged its examiners to be flexible during their review of BSA/AML programs. There is no universal “right answer”, only the answer that best addresses the uniqueness of each credit union and its particular risks.

A credit union’s risk assessment should be updated (when appropriate) in conjunction with any changes to the credit union’s risk profile. For example, the risk assessment should be updated (where appropriate) when new products and/or services are introduced, existing products or services are changed, the credit union expands through mergers and acquisitions, etc. At a minimum, best practices suggest that financial institutions review their risk assessments periodically, at least every 12 to 18 months.

In addition, management is expected to: (i) understand the credit union’s BSA/AML risk exposure as identified by the risk assessment, (ii) develop appropriate policies, procedures and processes to monitor and manage the institution’s risks, and (iii) develop a compliance program designed to mitigate the credit union’s BSA/AML risks.
Compliance Program & Risk Assessment

Federally insured credit unions are required to comply with Section 748 of NCUA’s regulations, which addresses BSA compliance, as well as security programs, reporting suspected crimes and catastrophic acts.

**Privately insured credit unions:** Although not subject to NCUA’s regulations, privately insured credit unions are subject to all the requirements of the Bank Secrecy Act, as well as the USA PATRIOT Act’s Customer Identification Program. NCUA works closely with NASCUS on BSA compliance. CUNA recommends that privately insured credit unions follow NCUA’s Part 748 rules addressing BSA to ensure sufficient compliance.

NCUA’s rules require federally insured credit unions to at a minimum:
1. Designate a BSA compliance officer who has been appointed by the board;
2. Provide for a system of internal controls to ensure ongoing compliance;
3. Provide for independent testing to be conducted by credit union personnel or outside parties; and
4. Provide training for appropriate personnel.

In May of 2018, new due diligence requirements went into effect that require these four provisions, as well as an additional one:

1. Appropriate risk-based procedures for conducting ongoing member due diligence, to include, but not be limited to:
   - Understanding the nature and purpose of member relationships for the purpose of developing a member risk profile; and
   - Conducting ongoing monitoring to identify and report suspicious transactions, and
   - On a risk basis, maintain and update member information – including information regarding the beneficial owners of legal entity members.

For detailed information on identifying and verifying the beneficial owners of legal entity members see Chapter 3 – Member Due Diligence in this manual.

NCUA requires credit unions’ compliance programs to be:
- in writing,
- approved by the credit union’s board of directors, and
- reflected in the minutes of the credit union.

NCUA examiner expectations include adequate BSA policies, procedures and controls for each of the following:
- verifying member identity;
Designation of the BSA Compliance officer

According to the FFIEC’s Examination Manual, the credit union’s board of directors must designate a qualified BSA officer. The BSA officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA officer is also charged with managing all aspects of the BSA compliance program and with managing the credit union’s adherence to the implementing regulations. NOTE: The board of directors is ultimately responsible for the credit union’s compliance. See FinCEN's “Culture of Compliance” Advisory.

The BSA officer’s level of authority and responsibility within the credit union is critical. The board of directors is responsible for ensuring that the BSA compliance officer has sufficient authority and resources (monetary, physical, and personnel) to effectively administer the compliance program.

The BSA officer is expected to be fully knowledgeable of the Bank Secrecy Act and all related regulations, as well as understand the credit union’s products, services, members, geographic locations and the money laundering and terrorist financing risks associated with those activities. The BSA compliance officer should be in a position to regularly apprise the senior management staff and the board of directors of ongoing compliance with the BSA.

The FFIEC’s BSA Examination Manual notes that simply the board’s appointment of a BSA compliance officer is not sufficient to meet the regulatory requirements if that person does not have the expertise, authority, or time to satisfactorily complete the job.

A System of Internal Controls

The second requirement refers to the policies and procedures the credit union puts in place to limit and control risks associated with BSA. The level of sophistication of your internal controls will be commensurate with the size, structure, risks and complexity of your credit union. A large, complex credit union is more likely to have departmental internal controls that will uniquely address the risks to a particular department or line of business.

The following are examples of some of the items that may be included in your internal control procedures (more details on these items is provided throughout the manual):
• Identify credit union products, services, members, and/or branches that you consider more vulnerable to abuse by money launderers or other criminals, and provide a program to manage the higher risk;
• Inform the board of directors and senior management of compliance initiatives, identify compliance deficiencies, corrective actions taken, and notify the board and the senior management of Suspicious Activity Reports (SARs) that have been filed;
• Provide for program continuity despite changes in management or employees;
• Meet all of the recordkeeping and reporting requirements;
• Implement risk-based Customer Due Diligence (CDD) policies & procedures;
• Identify reportable transactions and accurately file all required reports, such as SARs, CTRs, etc.;
• Provide for the segregation of duties where you can, so that it isn’t the same person determining who is exempt from filing, as the person who determines when a report should be filed, and who actually completes the reports, etc.;
• Provide for sufficient controls and monitoring systems for timely detection and reporting of suspicious activity;
• Include adequate supervision of employees who handle currency, complete reports, grant exemptions, etc.; and
• Train all employees to be aware of their responsibilities under BSA.

Independent Testing

NCUA’s third minimum Bank Secrecy Act requirement is periodic independent testing of the credit union’s BSA program. It is recommended that an audit of the BSA compliance program be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. Credit unions that do not have any of these options available to them, may comply with this requirement by using qualified persons who are not involved in the function being tested, or audited. The persons conducting the test should report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.

The frequency of the required independent testing is not specifically defined in the regulation, however, the regulators recommend that it be done every 12 to 18 months, depending on the credit union’s risk profile.

According to the FFIEC’s BSA/AML Examination Manual, a credit union’s independent auditing program should include the following:

• An attestation to the effectiveness and integrity of the BSA/AML compliance program, including policies, procedures and processes;
• A review of the credit union’s risk assessment for reasonableness given the credit union’s risk profile (based on products, services, members, and geographic locations);
• Appropriate transaction testing to verify the credit union’s adherence to the BSA record-keeping and reporting requirements (Customer Identification Program (CIP), Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), CTR exemptions, and 314(a) and (b) Information Sharing);
• An evaluation of management’s efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable;
• A review of staff training for adequacy, accuracy, and completeness;
• A review of the effectiveness of the suspicious activity monitoring systems (manual, automated or a combination) used for BSA/AML compliance. Reports reviewed may include, but are not limited to:
  o Suspicious activity monitoring reports;
  o Large currency aggregation reports;
  o Monetary instrument records;
  o Funds transfer records;
  o Nonsufficient funds (NSF) reports;
  o Large balance fluctuation reports;
  o Account relationship reports; and
• An assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness and effectiveness of the credit union’s policy.

Examiners Expectations

Additionally, the FFIEC BSA/AML Examination Guide encourages examiners to evaluate the following factors/items when determining the reasonableness of an institution’s independent audit:

• The independence of the individual(s) performing the audit and whether that person(s) reports directly to the board of directors or a designated board committee;
• The qualifications of the person(s) performing the audit;
• Auditor’s reports/work papers to determine if the audit was comprehensive and timely. A comprehensive audit should focus on the following:
  o BSA/AML risk assessment
  o Overall BSA/AML compliance program
  o BSA reporting and record keeping requirements
  o Customer Identification Program (CIP) implementation
  o Adequacy of customer due diligence (CDD) policies, procedures and processes
  o Credit union staffs’ adherence to BSA/AML policies, procedures and processes
  o Transaction testing that places an emphasis on high-risk operations
  o Adequacy of training (i.e. comprehensiveness, accuracy of materials, training schedule and attendance tracking);

Compliance Program & Risk Assessment
The ability of the suspicious activity monitoring systems to track unusual activity. In order to make this determination, the examiner may:

- Review the credit union’s policies, procedures, and processes for suspicious activity monitoring
- Evaluate the system’s ability to establish and apply expected activity or filtering criteria
- Determine whether the filtering criteria are reasonably based on the credit union’s risk assessment
- Evaluate the system’s ability to generate suspicious activity monitoring reports;

Audit tracking of previously identified deficiencies and management’s correction strategies; and

The audit’s scope, procedures, and work papers (where applicable) to determine the adequacy based on the following:

- Overall audit coverage and frequency in relation to the risk profile of the credit union;
- Board reporting and supervision of, and its responsiveness to, audit findings;
- Adequacy of transaction testing, especially for high-risk operations and suspicious activity monitoring systems;
- Competency of the auditors or independent reviewers regarding BSA/AML requirements.

Training

All appropriate personnel: At a minimum, the credit union’s BSA training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person’s specific responsibilities. For example, training for tellers should focus on examples involving large currency transactions or other suspicious activities, while training for the loan department should provide examples involving money laundering through lending arrangements.

New staff: In addition, an overview of the BSA/AML requirements typically should be given to new staff during employee orientation.

BSA Compliance officer: The BSA compliance officer should receive periodic training that is relevant and appropriate to the activities and overall BSA risk of the credit union.

Board of Directors: While the board of directors may not require the same degree of training as financial services operations personnel, they need to understand the importance of BSA regulatory requirements, the ramifications of noncompliance, and the risks posed to the credit union. Without a general understanding of the BSA, the board of directors cannot adequately provide BSA oversight, approve policies, or provide necessary resources. Remember, the ultimate compliance responsibility lies with the board of directors.

Frequency: NCUA recommends that BSA training be done every 12 to 18 months. It should also be ongoing and incorporate current developments and changes.
Record Keeping: Credit unions should document their training programs. Keep records of training and testing materials, the dates of training sessions and attendance records. Have these materials available for examiners.

Examiner Expectations: The FFIEC BSA/AML examination manual advises examiners to look for certain elements within a credit union's training program such as:

- The board of directors’ and senior managements’ commitment to ongoing education/training and compliance;
- Employee accountability for ensuring BSA compliance;
- Comprehensiveness of training – taking into account the specific risk of individual business lines;
- Training of personnel from all applicable areas of the credit union;
- Frequency of training;
- Coverage of credit union policies, procedures processes and new rules/regulations in training program;
- Coverage of different forms of money laundering and terrorist financing (placement, layering and integration) and examples of suspicious activity in training program; and
- Penalties for noncompliance with internal policies and regulatory requirements.

Finally, examiners have been directed to perform random knowledge testing of employees (such as tellers, funds transfer personnel, internal auditors, etc.) to assess their knowledge of BSA/AML policies and regulatory requirements.

RISK ASSESSMENT

Your BSA compliance program should be structured to your credit union’s specific level of risk. Determining your level of risk, or risk assessment generally involves two steps:

**Step One:** Identify the specific risk categories unique to your credit union, and
**Step Two:** Prepare a more detailed analysis of the data you gathered in Step One.

**Step One:** Although attempts to launder money or conduct other illegal activities through a credit union can emanate from many different sources, certain products, services, members and geographic locations may be more vulnerable or have historically been known to be abused by money launderers and criminals. For example, some products and services may allow a higher degree of anonymity (such as electronic funds payments), or involve the handling of high volumes of currency (such as monetary instruments like cashier’s checks, money orders, and traveler’s checks).

In addition to products and services, you may have some members that could be considered higher risk, such as nonresident aliens, cash intensive businesses like restaurants, even certain occupations like attorneys or accountants, who can at times be paid in large sums of cash.
Step Two: Once you have identified risk categories, the second step of the risk assessment process requires that you do a more detailed analysis of the data you gathered in the first step. Specifically, some of the factors you may consider include:

- Purpose of the account;
- Actual or anticipated activity in the account;
- Nature of the member's business or occupation;
- Member's location; and
- Type of products and services used by the member.

Using the risk assessment from this analysis, the credit union management should develop appropriate policies, procedures and processes to monitor and control the credit union’s BSA risks, with more emphasis on higher-risk products, services, members and branches.

An effective risk assessment should be an ongoing process, not a one-time exercise. The credit union should continually reassess its BSA risk exposures and communicate across departments and product lines. The identification of a BSA risk or deficiency in one area of business may indicate concerns elsewhere in the credit union. The federal regulators recommend reassessing the BSA risk at least every 12 to 18 months.

For guidance on preparing your risk assessment you should refer to Appendices I & J of the FFIEC’s BSA/AML Examination Manual.

Also important to note: Make sure that your risk assessment is comprehensive, so your examiner does not feel that it is necessary to complete his or her own risk assessment of your credit union. This would likely submit your credit union to more scrutiny during your exam, and you don’t want that! Your BSA compliance program must be adequately risk-based.
1. Has the board of directors established an appropriate written program to assure the credit union meets BSA reporting and recordkeeping requirements?

2. Does the written BSA compliance program address:
   a. Internal controls?
   b. Independent testing?
   c. Responsible individual?
   d. Training?
   e. Customer Identification?

3. Is the credit union’s independent testing adequate for the size and complexity of the institution?

4. Does the BSA officer have appropriate knowledge, resources, and authority – commensurate with the complexity of the credit union’s operations?

5. Is the credit union’s training adequate for the size and complexity of the institution?
TEST YOUR KNOWLEDGE

Question 1:

True or False: The credit union’s board of directors is ultimately responsible for the credit union’s BSA compliance?

Question 2:

The BSA officer must be knowledgeable of:
   a. BSA, and related regulations;
   b. The credit union’s products and services;
   c. The credit union’s members;
   d. The credit union’s neighborhoods;
   e. a & b
   f. All of the above.

Question 3:

True or False: If you are a small credit union it is acceptable to have the BSA officer determine when a CTR is necessary, fill out the CTRs, and determine who is eligible for a CTR exemption.

Question 4:

Regulators recommend that independent testing of your BSA program should be done:
   a. Annually
   b. Every 12 to 18 months
   c. Whenever necessary
   d. Before each exam

Question 5:

Which of the following products and services could possibly pose a higher risk for illegal activities?
   a. Wire transfers
   b. Monetary instruments
   c. Traveler’s checks
   d. All of the above
Quiz Answers:

Answer 1:
True! Although the BSA officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance and managing all aspects of the BSA compliance program, the credit union’s board of directors is ultimately responsible for the credit union’s compliance. This is why it is critical that the board of directors designate a qualified BSA officer.

Answer 2:
The answer is f. All of the above. The BSA officer is expected to be fully knowledgeable of the Bank Secrecy Act and all related regulations, as well as understand the credit union’s products, services, members, geographic locations and the money laundering and terrorist financing risks associated with those activities. The BSA compliance officer should be in a position to regularly apprise the senior management staff and the board of directors of ongoing compliance with the BSA.

Answer 3:
False: As part of the credit union’s internal controls, you must have policies and procedures in place to limit and control risks associated with BSA. This includes the segregation of duties where you can, so that it isn’t the same person determining who is exempt from filing, as the person who determines when a report should be filed, and who actually completes the reports, etc. Also include adequate supervision of employees who handle currency, complete reports, grant exemptions, etc.

Answer 4:
The answer is b. every 12 to 18 months. The frequency of the required independent testing is not specifically defined in the regulation, however, the regulators recommend that it be done every 12 to 18 months, depending on the credit union’s risk profile.

Answer 5:
The answer is d. All of the above. Although attempts to launder money or conduct other illegal activities through a credit union can emanate from many different sources, certain products, services, members and geographic locations may be more vulnerable or have historically been known to be abused by money launderers and criminals. For example, some products and services may allow a higher degree of anonymity (such as electronic funds payments), or involve the handling of high volumes of currency (such as monetary instruments like cashier’s checks, money orders, and traveler’s checks).
**Member Identification Program (MIP)**

*Note: FinCEN and the FFIEC refer to these requirements as Customer Identification Program (CIP)*

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) required the U.S. Department of Treasury to issue regulations setting forth minimum standards for financial institutions to identify and verify any person who opens an account. Section 326 of the USA PATRIOT Act requires financial institutions to:

- Implement reasonable procedures to verify the identity of any person seeking to open an account, to the extent reasonable and practicable;
- Maintain records of the information used to verify the person’s identity;
- Determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency; and
- Provide the member opening a new account with notice of the information collection requirement.

The Department of Treasury, the National Credit Union Administration, and other federal agencies issued final regulations implementing Section 326 of the USA PATRIOT Act, which became effective on October 1, 2003. The aim of the final rule was to protect the U.S. financial system from money laundering and terrorist financing. According to the regulators, this rule would have the added benefit of helping to protect consumers against various forms of fraud, including the growing incidence of identity theft involving new accounts.

The regulation requires all financial institutions, including credit unions, to implement a Customer Identification Program, or CIP. A credit union’s CIP (MIP) must contain procedures that assist in:

- obtaining identifying information from anyone opening an account,
- verifying that information, and
- enabling the credit union to form a reasonable belief that it knows the true identity of the accountholder.

**MIP Must Be Risk-Based**

The regulations are intended to be risk based, which means that Treasury’s regulations provide minimum standards. A financial institution’s MIP/CIP should be tailored to:

- its size,
- location,
- types of accounts offered,
- methods of opening accounts, and
- any other risk factors the financial institution believes affects its CIP procedures.

Credit unions are expected to be vigilant in their efforts to recognize members who might try to use the credit union for financing terrorism or conducting money-laundering activities.
A credit union does not have to verify each of the four required pieces of information, but must verify the person’s identity to the extent necessary to form a reasonable belief that it knows the true identity of each member.

**Obtaining Identifying Information**

A credit union must apply its MIP to each person that establishes a new account. This includes not only members, but joint account holders, and co-borrowers.

The regulation requires credit unions to get at least four pieces of information for each new member/customer:

- Name,
- Date of birth,
- Address, and
- Identification number.

Although the MIP regulation currently does not require you to update this identifying information, other standards do, and soon a new customer identification regulation is expected to as well.

**Address:** Credit unions must get a residential or business street address so that there is a physical location at which someone could be contacted by a government investigator. If the prospective individual member is unable to provide a residential or business street address, the credit union may accept an address of a friend or relative, or an Army Post Office (APO) or Fleet Post Office (FPO) box number.

The address for a business can be either the principal place of business, local office, or other physical location of the business. The credit union can get additional addresses, such as a mailing address, to meet its own or the member’s needs.

**Identification Number:** Credit unions will get a social security number (SSN) for U.S. citizens, or an employer identification number (EIN) for a business. For non-U.S. citizens, the rule allows some flexibility. You can obtain:

- A SSN from a resident alien,
- An individual taxpayer identification number (ITIN),
- A passport number and the country of issuance,
- An alien identification card number, or
- A number and country of issuance on any other foreign government-issued document evidencing nationality or residence with a photo or similar safeguard.

Again, these are the minimum requirements, and each credit union must determine whether additional information is necessary for purposes of verifying the identity of your members.
Verify Identifying Information

Verification of identity must be done before or within a reasonable time after the account is opened. Although you are not required to verify every element of the identifying information you receive from the member, you must verify enough information to form a reasonable belief that you know the member, the joint owner, or the co-borrower. The credit union does not have to verify the identity of any guarantors and others involved in the consumer loan process who will not be receiving the loan proceeds. Authorized users of credit cards are not subject to MIP/CIP verification because they aren’t responsible for repayment. Also, if the authorized user is not a member of the credit union and there is no enforceable agreement for the credit union to provide services to the authorized user, the MIP/CIP is not required.

Credit unions have the flexibility to determine when verification will be done and what methods it will use. The credit union should assess the membership base it serves (citizens, foreign nationals, businesses), the methods it uses to open accounts (in-person, by mail, via Internet), and the types of accounts opened when shaping its MIP verification procedures.

There are two methods that credit unions can use to verify identity—documentary or non-documentary methods.

Documentary methods: Using the documentary method generally requires the use of unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver’s license, passport, military ID, or a Matricula Consular issued by Mexico. [NOTE: NCUA neither endorses nor prohibits a credit union’s acceptance of specific documents issued by foreign governments such as the Matricula Consular. Ultimately, the credit union will have to decide, based on appropriate risk factors, whether or not a certain form of ID is acceptable].

This verification method is useful when the person is present when opening the account or being added as a joint account holder, since the photo provides visual verification. However, reviewing a photocopy of a driver’s license mailed in with an application would be insufficient on its own, but could be used in conjunction with additional documents or non-documentary methods.

Non-documentary methods: Using non-documentary methods generally will include such items as:

- Comparing the information provided by the person with information obtained from a credit bureau, or against fraud and bad check databases, such as Telecheck or ChexSystems. Obtaining references from other financial institutions;
- Contacting the member after the account is opened to confirm information such as telephone number and address;
- Obtaining a tax return or a financial statement;
- Using any type of online verification system;
• Checking the information with information available from any other trusted third-party source;
• Checking public databases.

Non-documentary methods become particularly helpful when you are verifying the identity of a new member applying for a credit union account through the mail, Internet, or fax.

These terms, documentary and non-documentary can be confusing because non-documentary methods can include things that would typically be called documents, like a financial statement. A general rule seems to be that for individuals, a documentary method of verification is relying on government-issued documents, while non-documentary method is relying on something that is not a government issued document.

A credit union is not required to verify the validity of a document. However, if the document is obviously fraudulent on its face, the credit union must consider that factor in determining whether it can form a reasonable belief that it knows the true identity of the member. The credit union may want to have as part of its MIP policy that it will file a suspicious activity report (SAR) if fraudulent identification is presented.

Verification Procedures

Your MIP procedures must describe:
• How the identity will be verified;
• When documentary methods, non-documentary methods, or a combination of both methods will be used; and
• What documents and non-documentary information the credit union will accept.

The regulation specifically recommends that, at a minimum, you address the following four situations in your verification procedures:

• When should the credit union not open an account at all? For example, credit unions may adopt procedures that state that a person must supply all of the required information and documents for in-person applications and/or pass an online verification or a credit report review before the account is opened. The procedures may state that other situations will be referred to management to consider what additional steps are appropriate.

NOTE: The Fair Credit Reporting Act requires credit unions to provide an adverse action notice if the refusal to open the account is based on a consumer report.

• When will the credit union open an account while it attempts to verify identification and under what terms will the account be authorized? For example, the credit union may allow certain accounts to be opened prior to verification for member convenience, but the credit union should specify limitations on transactions, or only allow a share account in order to limit risk.
If a credit union feels there is a low-risk justification in opening an account before identity verification, CUNA suggests that the credit union notify the person that membership is granted conditionally, based on being able to verify the identity of the person and any nonmember joint account owner in accordance with federal law. The credit union should also notify the person that if their identity cannot be verified as required in its procedures, it will close the account in a specific number of days and return the funds to the person with/without the payment of any dividends.

It is also important that credit union evaluate under what, if any, circumstances it would extend credit in any form until it has verified the person’s identity.

- **When should the credit union close an account after attempts to verify the identity of the person fails?** The credit union’s MIP should state a specific time period during which verification has to be completed.

It’s the credit union’s choice whether it will close the account if it can’t verify the person’s identity. There may be complications in simply closing the account. Treasury and the Agencies have determined that there is no statutory basis to create a safe harbor that would shield financial institutions from state regulatory or borrower liability if a financial institution should choose to close an account. Any such closure should be consistent with the credit union’s existing procedures for closing accounts in accordance with its risk management practices.

- **When should the credit union file a suspicious activity report (SAR)?** A credit union must file a SAR when it suspect any violation of laws or regulations, such as:
  - When it suspects funds were derived from illegal activities,
  - Where there is suspicious activity regarding money laundering or structuring transactions to evade currency transaction reporting,
  - Insider abuse, or
  - Identity theft.

Although every failure to verify individuals’ identities should not trigger a SAR, every instance when the credit union is presented with fraudulent, or seemingly fraudulent, documents for purposes of identification should be reviewed by management as a possible reason to file a SAR.

[See Chapter 7 for more information about the SAR reporting requirements.]

**Account opening procedures**

Your MIP procedures must also include:
• What will the credit union do if an individual cannot present a government-issued document with a photograph to verify his or her identity?

• What will the credit union do if it is not familiar with the document presented?

• How will the credit union verify member identity for applications that are mailed in or received over the Internet?

Verifying Business Accounts

Credit unions should pay particular attention to its’ MIP procedures when opening business accounts. Business accounts can pose a higher risk for money laundering and examiners will expect to see appropriate steps taken to verify the actual existence of the business. Oftentimes, businesses and other legal entities are verified using a combination of documentary and non-documentary methods.

For corporations, partnerships, other businesses, trusts, and other legal entities, the MIP regulations suggest the use of the following documents as evidence of the existence of the entity:

- Certified articles of incorporation,
- A government –issued business license,
- A partnership agreement,
- A trust agreement.

The credit union must include in its Member Identification Program, situations where the credit union believes the level of risk with a particular business member will warrant the obtaining of names and verifying the identities of the officers of the business or those authorized to make deposits and withdrawals and apply for loans with the credit union.

Additionally, the Treasury and Justice Departments have designated certain parts of the United States as High Intensity Money Laundering and Related Financial Crimes Areas (HIFCAs). A HIFCA map is available on FinCEN’s website. A credit union can consult the map for each business account it opens. If the business is located in one of these areas, the credit union should consider verifying the identities of one or more signatories with authority and control over the account.

Record Retention

The credit union must have specific MIP procedures on making and maintaining all MIP records required by the regulation. At a minimum, the MIP records must include:

Identifying Information: Credit unions are required to maintain a record of all the information they receive from their members. This includes the name, address, date of birth, and identification number. The credit union must develop its own record keeping system, including how best to retrieve this information in the event that the government requests the information. Keep in
mind, the purpose of the MIP regulation is to help provide the federal government with an audit trail to track down the flow of funds of money launderers and terrorists.

These records must be retained for five years after the date the account is closed. The records maintained can be either a copy of the actual document or a description of the document.

NOTE: Some state laws prohibit photocopying of driver’s licenses – you will want to check with your state credit union league to see if your state is one of them. There are also military regulations that prohibit the copying of military IDs. Remember, the BSA regulation does not require that you photocopy documents – it requires that you maintain a description of the document.

If the credit union chooses to maintain a description of the documents used, that description must include:

- A description of any document that was relied on to verify its member’s identity;
- Any identification number in the document;
- The place the document was issued;
- The date of issuance and expiration date, if any.

Verification methods: Additional records that must be maintained include a description of the verification methods used, results of verification, and if substantive discrepancies occur, steps that the credit union has taken to resolve the discrepancies and the resolution of the situation. These records must be kept for 5 years after the record is made.

Electronic records: The credit union can use electronic records to comply with the record retention requirements, as long as the records are accurate and are filed or stored in a manner that is accessible within a reasonable period of time.

Lists of Known Terrorists or Terrorist Organizations

Your MIP must include procedures for determining whether your member appears on any federal government list of known or suspected terrorists or terrorist organizations. To date, there have been no designated government lists to verify specifically for MIP purposes. It is important to note that these lists are separate and distinct from the terrorist list required by the Office of Foreign Assets Control (OFAC). OFAC is a division of the U.S. Treasury Department, which administers and enforces economic and trade sanctions against targeted foreign countries. Credit unions are responsible for checking OFAC’s Specially Designated Nationals and Blocked Persons List (SDN list) and blocking the accounts of any person, country, or entity appearing on that list. [For more information on OFAC’s list see Chapter 8]
When (if) Treasury does issue a MIP/CIP terrorist list, it will work in consultation with NCUA and you will be contacted. At that time, you will be required to compare your members’ names against the list and follow the directions from Treasury that will accompany the list you receive.

**Notice to Members**

To meet the notice requirement you must provide your members and your potential members, with a notice that describes the information collection requirements of the rule. While you are not required to provide individual copies of the notice to each potential member, you must provide it in a manner that ensures every member will see it before opening an account. You can accomplish this for most account openings by posting the notice in your lobby, on your website, or including it on your account application. Make sure you consider how you are distributing the notice to members who mail in their applications. If you aren’t including the notice on the application, you may want to include a separate notice with the account applications that you mail out.

Every credit union will need to determine how to provide notice to best meet its needs. Posting a lobby notice alone will not comply with the MIP notice requirement, unless opening accounts face to face in the office is the only way the credit union adds members, joint account holders, and co-borrowers. The notice is considered adequate if it “generally describes the identification requirements.” The notice can be very simple as shown by the sample notice below, which is included in the MIP regulations:

§1020.220(a)(5)(iii):

**Sample notice.** If appropriate, a bank may use the following sample language to provide notice to its customers:

**IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT**

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver’s license or other identifying documents.

**Services Not Subject to the MIP Rule**

There are some services that are not subject to this rule, such as:

- check-cashing,
- wire transfers,
- sale of checks or money orders, or
• accounts opened for the purpose of participating in an employee benefits plan.

Additionally you will not have to verify the identity of any existing member, or existing joint account holders or co-borrowers, as long as you have a reasonable belief that you know the identity of those persons.

And finally, this MIP rule does not apply to another credit union that is opening an account at your credit union, or any account opened by federal, state or local governments.

Employee Retirement Accounts

According to Treasury’s regulation, an account for MIP purposes does not include an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 (ERISA). Treasury states that if the only account a person opens at the financial institution is an employee benefit plan, such as a simplified employee plan (SEP) or a 401(k) employee savings account, then the financial institution doesn’t have to comply with CIP verification for that person. Treasury provided this exclusion for ERISA-type accounts because it was persuaded that retirement savings accounts are not the type to be used for money laundering or terrorism financing purposes.

Due to their membership requirements, credit unions may require the person to open a separate membership account or will conduct some type of verification on the person opening the retirement account as a good business practice. If the credit union doesn’t do the MIP verification for an employee benefit account and the person later opens another type of account, the credit union at that time must comply with the MIP requirements for this new account. Keep in mind, OFAC requirements apply to the opening of any type of account as well as numerous other transactions at the credit union.

Reliance on Another Financial Institution

A credit union is permitted to rely on another financial institution to perform some or all of the elements of the MIP, if reliance is addressed in the credit union’s MIP procedures and the following criteria are met:

• The relied-upon financial institution is subject to the BSA/AML program requirements and is federally regulated;
• The member has an account or is opening an account at the credit union, as well as at the other federally regulated institution;
• Reliance is reasonable,
• The other financial institution enters into a contract requiring it to certify annually to the credit union that it has implemented its BSA/AML program, and that it will perform (or its agent will perform) the specified requirements of the credit union’s MIP.

Use of Third Parties

The MIP regulation allows a credit union to arrange for a third party, such as a car dealer, to verify the identity of the member. The credit union can also arrange for a third party to maintain
its records. However, the credit union is ultimately responsible for that third party’s compliance with MIP requirements. As a result, credit unions should establish adequate controls and review procedures for such relationships.
MEMBER IDENTIFICATION PROGRAM CHECK LIST
[Source: NCUA]

1. Has the credit union established a written MIP that provides for:
   - Obtaining basic identifying data for each person opening an account?
   - Verification of the identity of any person opening an account?
   - Maintenance of records of the information used to verify the person’s identity?
   - Determination whether the person appears on any federal government list of suspected terrorists?
   - Adequate notice that the credit union will request information to verify identity?

2. Is the MIP board-approved?

3. Does the MIP require the following minimum information prior to opening an account:
   - Name,
   - Date of birth,
   - Address,
   - Identification number
     (taxpayer identification number for U.S. person; for a non-U.S. person a taxpayer identification number, passport number and country of issuance; alien identification card number, or number and country of issuance, of any other government-issued document bearing a photo or similar safeguard?)

4. Does the credit union maintain the identifying data for 5 years after the account is closed?

5. Does the Credit union maintain a descriptive record of any document used to verify identity for 5 years after the account is opened?

6. Does the credit union maintain a record of the resolution of any discrepancies in basic identifying data for 5 years?

7. Does the credit union maintain a descriptive record of any non-documentary method used to verify identity for 5 years after the account is opened?

8. Does the credit union have a process for handling exceptions to the standard MIP policy?
TEST YOUR KNOWLEDGE

Question 1:
The identification and verification rules do NOT apply to which of the following?

A. Joint owners
B. Beneficiaries
C. Co-borrowers
D. Non-resident aliens

Question 2:
In which of the following situations would a credit union need to verify an existing member’s identity?

A. Opening a VISA credit card or adding a Money Market account
B. Adding Home Banking or Voice Response service
C. Adding ACH or Bill Payment services
D. None of the above – credit unions do not have to verify existing member’s identity

Question 3:
Must the credit union verify identity before the member opens an account or can this be done when the member comes in to conduct his first transaction?

Question 4:
Does the MIP rule prohibit a minor from opening an account?

Question 5:
Must a credit union verify the accuracy of all of the identifying information it collects during the MIP process?

Question 6:
Does the original information obtained during account opening have to be retained or can the credit union satisfy the recordkeeping requirement by just keeping updated information about the member (such as the member’s current address)?

Question 7:
If the credit union obtains more than the required identifying information during the account opening process, does it have to keep this additional information for five years too?
Answers to Test

Answer 1:
The correct answer is “b.” The MIP regulations apply to anyone applying to open an account, which includes any accountholder on the account. This would include all members, joint owners, and trustees as well as both resident and non-resident aliens. However, beneficiaries are not signers on an account and therefore, would not be included in this list. Additionally, the definition of “account” means any “formal banking or business relationship established to provide an ongoing service, dealing, or other financial transaction.” This definition is broad enough to include loans, and therefore co-borrowers would also fall under the requirements.

Answer 2:
The answer depends on a couple of things. First, let’s start with answer “d” and determine whether the credit union needs to verify the identity of an existing member at all.

The regulations apply to all “customers” which is defined as any person applying to open an account. This definition excludes those individuals who already have an account, but does not exclude existing members seeking to open another account. Therefore, an existing member would only have to be verified if he or she goes through the process of opening a new account.

However, answer “d” isn’t necessarily a wrong answer. When a member opens an account and the credit union correctly verifies his information, the credit union would not need to re-verify his identity again (when he opens a second account) if it has a reasonable belief that it still knows the identity of the member. However, at the time the second account is opened, if the credit union is not comfortable with the member’s identity, it would need to re-verify his information.

Now let’s look at the other answers to determine if they are considered “new accounts.” The regulation defines account as a “formal banking or business relationship established to provide ongoing services, dealings, or other financial transactions.” This would include a deposit account, transaction account, credit account or other extension of credit. Therefore, answer “a” would be correct because adding a VISA credit card or Money Market account would be considered a new account. The credit union would have to follow its MIP procedures for opening new accounts for existing members.

Adding services such as home banking, ACH or bill payment to an existing account may not be considered a new account. Services such as these all seem to require an underlying deposit or transaction account already in place to be activated. If these services have been available as a benefit for the type of account that was already opened, it would not be considered a new account relationship, which would make answers “b” and “c” wrong, and the credit union would not need to re-verify its member’s identity.

Answer 3:
The regulations do not require that the credit union verify a member’s identity before opening the account. Requiring the credit union to do that would be unduly burdensome for both the credit union and the member. However, the credit union must verify its member’s information within a reasonable period of time after the account is opened.
The rule does not specify what it means by “reasonable” but gives the credit union flexibility to use a risk-based approach to determine how soon identity must be verified. The amount of time it will take the credit union to verify identity may depend upon the type of account opened, whether the member is physically present when the account is opened, and the type of identifying information available.

Given the flexibility of the regulations, waiting until the member conducts his first transaction may be sufficient. However, be careful that some members don’t fall through the cracks. The credit union runs the risk that the member may never conduct a transaction or conduct a transaction several months later. Therefore, procedures should be in place that would follow up with those members that rarely conduct transactions. For example, if the credit union is unable to verify the member’s identity within a reasonable time, it may want to follow up with a letter (even though this may be expensive) or a phone call. If the identity is still not verified, procedures should be in place to address what actions the credit union will take, including when an account should not be opened or when a joint owner should not be added.

Keep in mind, however, that it may be possible to violate other laws by permitting a member to transact business before verifying his or her identity. For example, OFAC prohibits transactions involving individuals, entities or countries on the agency’s SDN/Blocked Persons List. The credit union should verify a person’s identity to make sure it is not engaging in prohibited transactions.

Answer 4:

No. The MIP rule states that the credit union’s “member” is the individual who opens the account for an individual who lack legal capacity, such as a minor. In other words, if a parent opens an account for a child, the member for purposes of the MIP rule is the parent. If, however, a minor opens the account, then the minor is the member. According to NCUA, when a minor opens the account, he/she can be verified through documentary methods such as a driver’s license or work permit. If these are not available, the minor could be identified through non-documentary methods such as verification by an existing member, using public databases, verification of identity by parent/teacher. A credit union’s MIP policy will need to specify what types of documentary and/or non-documentary evidence it will accept and the circumstances under which such documentation will be acceptable.

Treasury explains that where a credit union send its employees to elementary schools so that students may open savings accounts as part of a program to promote financial literacy, a student opening the account is the member and the credit union must get the name, address, date of birth, and taxpayer identification number of the student. Since verification procedures are risked-based, credit union can use any reasonable documentary or non-documentary method to verify a student’s identification.

Answer 5:

No, the final rule provides that a credit union’s MIP must contain procedures for verifying the identity of the member using the information obtained during the credit union’s MIP process. A credit union need not establish the accuracy of every element of identifying information obtained and is only required to obtain sufficient information to form a reasonable belief that it knows the true identity of the member.
Answer 6:

Yes, the original information must be retained. Under MIP, credit unions are required to maintain the identifying information obtained from a member (during the account opening process) 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. Obtaining and maintaining updated member information serves valuable, but different, purposes.

Answer 7:

The credit union must keep all identifying member information gathered during the account opening process for five years after the account is closed, or in the case of credit card accounts, five years after the account is closed or becomes dormant. This would include any identifying information the credit union will use to establish a reasonable belief it knows the true identity of the member. So, for example, if the credit union obtains other identifying information at account opening in addition to the minimal information required, such as the customer's phone number, then the credit union must keep a record of that information also.
Member Due Diligence (MDD)

NOTE: FinCEN and the FFIEC refer to these requirements as Customer Due Diligence (CDD), CDD and MDD are the same regulation.

FinCEN states that this due diligence requirement is a critical part of any effective BSA compliance program because it assists financial institutions in performing risk assessments of their customers, or in our case, our members. This additional information is to be collected for ALL of your members to help you better determine whether a member is or isn’t “higher risk”.

FinCEN issued a new Customer Due Diligence (CDD) rule that went into effect May 11, 2018.

MDD/ CDD General Guidance

You will note that some requirements of the MDD are similar to the Member Identification Program (MIP), which requires credit unions to know the true identity of its members. Going well beyond the MIP requirement, the MDD also requires credit unions to:

- gain an understanding of the nature and purpose of member relationships and understand your member’s normal and expected transaction activity, based on their occupation or business operations, so that you can better determine if something is suspicious, and whether a SAR needs to be filed;

- keep an eye out for indicators of potential changes in the member’s risk profile, for example a change in employment, a change in business operations, or unexpected account activity;

- include procedures to periodically monitor your member’s information.

- On a risk basis, maintain and update member information – including information regarding the beneficial owners of legal entity members.

Additionally, according to the Examination Manual, a credit union’s BSA/AML program should include due diligence guidelines that:

- are commensurate with the credit union’s BSA/AML risk profile, with particular attention paid to high-risk members;

- contain a clear statement of management’s overall expectations, as well as management’s expectations regarding staff responsibilities (such as those responsible for reviewing/approving changes to a member’s risk rating or profile);

- ensure that the credit union possesses sufficient member information to implement an effective suspicious activity monitoring system;
• provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained; and

• as a best practice, ensure the credit union maintains current member information.

Beneficial Ownership of Legal Entities

The 2018 CDD/MDD rule includes new requirements for “beneficial owners” of “legal entity” accounts.

**Beneficial owners**: The definition of beneficial owners has two prongs:

**Ownership criteria**: Each individual, if any, who directly or indirectly, through any contract arrangement, understanding, or otherwise, owns 25% or more equity interest in the legal entity (this is a baseline threshold – credit unions are permitted to have a lower threshold);

AND

**Control criteria**: A single individual with significant responsibility to control, manage, or direct the legal entity, such as CEO, CFO, VP or other member of the senior management team or a person that regularly performs similar functions.

The number of individuals that satisfy the definition of “beneficial owner”, and must be identified and verified will vary. Depending on the factual circumstances, up to four individuals may need to be identified for the ownership prong, and only one individual must be identified for the control prong.

The certification form can be filled out without a beneficial owner that meets the ownership criteria, as long as there is at least one beneficial owner who meets the control criteria.

Additionally, the credit union is permitted (encouraged if the entity is considered higher-risk) to require a lower ownership threshold, thus making it more likely for an owner to meet the beneficial ownership criteria.

**Legal entities**: The rule defines a “legal entity” as a: corporation, LLC, or other entity that is created by the filing of a public document with a Secretary of State or similar office; a general partnership or similar entity.

The following are NOT legal entities: Sole proprietorships, unincorporated associations (such as, Scout Troops and youth sports leagues), or natural persons opening accounts on their own behalf.
Additionally, the rule considers the following exempt from the definition of legal entity because the information is generally available from other credible sources:

- department or agency of the federal, state, or local government;
- any entity established under the federal, state or local laws of the U.S., or any interstate compact, that exercise governmental authority on behalf of the government;
- any entity whose common stock is listed on one of the stock exchanges;
- any subsidiary of an entity listed on one of the stock exchanges and whose common stock is owned (at least 51 percent) by the listed entity;
- an issuer of securities;
- an investment company;
- an investment advisor,
- an exchange or clearing agency;
- an entity registered with the SEC;
- an entity registered with the Commodity Futures Trading Commission;
- A bank holding company;
- A pooled investment vehicle;
- An insurance company regulated by a State;
- A financial market utility;
- A foreign financial institution, where its regulator maintains beneficial ownership information;
- A non-U.S. governmental department, agency or political subdivision that engages only in governmental activities.

The following entities are only subject to the control criteria prong in the definition of “beneficial owner”:

- Any legal entity that is established as a non-profit corporation or similar entity and has filed its organizational documents with the appropriate State authority.
- Any legal entity only to the extent that it opens a private banking account subject to BSA requirements.
- Any pooled investment vehicle that is not exempt.

**Identification of Beneficial Owners:** A credit union can identify the beneficial owners of business accounts in one of three ways:

1. by obtaining a “Certification Regarding Beneficial Owners of Legal Entity Customers” provided in the rule (it will also be available in electronic form);

2. by using the credit union’s own forms, as long as they meet the requirement in the rule; or

3. by obtaining the required information by any other means – provided the person opening the account and providing the information certifies that it is accurate.

**NOTE:** Using FinCEN's form DOES NOT provide you with a safe harbor in regard to compliance.
Verification of Beneficial Owners: Credit unions must verify each identified beneficial owner of legal entity accounts according to risk-based procedures to the extent reasonable and practicable. At a minimum, these procedures must include all of the elements of the credit union’s Member Identification Program (MIP).

In regard to documentary verification, FinCEN has clarified that you may use photocopies or other reproductions of the documents. However, given the vulnerabilities inherent in the reproduction process, you are encouraged to conduct your own risk-based analyses of the types of photocopies and reproductions that you will accept, for example optical resolution threshold or digital reproductions transmitted in certain file formats.

Exemptions: The following legal entities are exempt from the identification and verification requirements:
- Private label retail credit cards established at point-of-sale, up to a limit of $50,000 (co-branded major credit cards are not exempt);
- Entities that finance the purchase of postage, where payments are remitted by the credit union **;
- Entities that finance insurance premiums, where payments are remitted by the credit union **;
- Entities that finance the purchase or leasing of equipment, where payments are remitted by credit union **.

** Except where the legal entity account member can make or receive payments from a 3rd party, or where a cash refund is possible.

Written Procedures: Credit unions are required to develop written procedures to identify and verify “beneficial owners” of “legal entity” members and include these procedures in their Anti-Money Laundering (AML) compliance programs.

Additionally, credit union must establish procedures for making and maintaining a record of all of the identification and verification information collected.

Credit unions are also expected to add appropriate risk-based procedures for conducting ongoing member due diligence to their anti-money laundering compliance programs.

Recordkeeping Requirements: At a minimum your record must include:
- Any identification information obtained, including the Certification Form, if applicable;
- A description (type, identification number, place of issuance and dates of issuance and expiration, if any) of any document relied upon;
- Any non-documentary methods used; and
- Any measures taken in response to any substantive discrepancies, and the results those actions.

Member Due Diligence
Record Retention: Identification related records must be retained for 5 years after the date the account is closed. Verification related records must be retained for 5 years after the record is made.

Beneficial Owner Certification Form: If your credit union chooses to use FinCEN’s certification form, it must be completed by the person opening the new account (on or after May 11, 2018) on behalf of a legal entity. It must be a natural person authorized to open the account – it cannot be the entity itself.

This form requires the person opening the account to provide their name and title, as well as the name, address, date of birth and identification number for the "beneficial owners" of the entity. The number of individuals that satisfy this definition of “beneficial owner” may vary from one to five depending on the factual circumstances, and the same person may meet the criteria for both ownership and control.

The certification form can be filled out without a beneficial owner that meets the ownership criteria, but there must be at least one beneficial owner who meets the control criteria - CEO, CFO, VP or other member of the senior management team or a person that regularly performs similar functions. Additionally, the credit union is permitted (encouraged if the entity is considered higher-risk) to require a lower ownership threshold.

IOLTA Accounts: For purposes of the MDD/CDD rule, credit unions should treat the attorney opening the IOLTA account as the beneficial owner of the legal entity account. Similar to other guidance for IOLTA and escrow accounts, the attorney or escrow agent is considered the member and the credit union has no CIP obligations with respect to the underlying clients whose funds are being held in the IOLTA or escrow accounts.

Legal entity accounts existing before May 11, 2018: The requirement to identify and verify beneficial owner information for your legal entity accounts will be implemented prospectively – only for new accounts opened on or after May 11, 2018. FinCEN recognized that to implement these requirements retroactively would be “too unduly burdensome.” That said, FinCEN does expect you to obtain beneficial ownership information for accounts already in existence on May 11, 2018 when, in the course of normal monitoring, you detect information relevant to reevaluating the account’s risk.

OFAC Implications: FinCEN generally expects beneficial ownership information to be treated like MIP and related information, and accordingly used to ensure that you are complying with other BSA-related requirements, such as OFAC. Credit unions should use beneficial ownership information to help ensure that you do not open or maintain an account, or otherwise engage in prohibited transactions or dealings involving individuals or entities subject to OFAC-administered sanctions.

Reliance on another financial institution: A credit union may rely on the performance by another financial institution (including an affiliate) with regard to these due diligence requirements with respect to any legal entity member that is opening, or has opened, an
account or has established a similar business relationship with the other financial institution to provide or engage in services, dealing or other financial transactions, provided that:

- The reliance is reasonable under the circumstances;
- The other financial institution is subject to anti-money laundering regulations and is regulated by a Federal agency; and
- The other financial institution enters into a contract requiring it to certify annually that it has implemented its anti-money laundering program, and that it will perform the specified requirements of the credit union’s procedures to comply with this rule.

**High Risk Member Procedures**

Your procedures should include the enhanced and ongoing due diligence procedures you will follow once you have identified any high-risk members.

For example, when you have identified a potentially high risk member, you should consider obtaining the following information, if applicable, at account opening and throughout the relationship:

- purpose of the account;
- source of funds and wealth;
- individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors;
- Occupation or type of business;
- Financial statements;
- Financial institution references;
- Where the business is organized;
- Member’s place of employment;
- Description of member’s primary trade area and whether international transactions are expected to be routine;
• Description of the business operations, the anticipated volume of currency and total sales, as well as a list of major customers and suppliers;

• Explanation of changes in account activity.

Similar to the MIP, in many instances, member information can be confirmed through information reporting agencies, financial institution references, correspondence and telephone conversations with the member, on-site visits, third-party references and public research (such as the Internet or commercial databases).

Due Diligence for Marijuana-Related Businesses

For credit unions making the business decision to provide financial services to marijuana-related businesses, FinCEN issued guidelines in February 2014 which include three new types of SARs (“Marijuana Limited” SAR, “Marijuana Priority” SAR and “Marijuana Termination” SAR). Additionally, there are seven new customer due diligence requirements:

1. Verifying with the appropriate state authorities whether the business is duly licensed and registered;

2. Reviewing the license application (and related documentation) submitted by the business for obtaining a state license to operate its marijuana-related business;

3. Requesting from state licensing and enforcement authorities available information about the business and related parties;

4. Developing an understanding of the normal and expected activity for the business, including the types of products to be sold and the type of customers to be served (i.e.: medical versus recreational customers);

5. Ongoing monitoring of publicly available sources for adverse information about the business and related parties;

6. Ongoing monitoring for suspicious activity, including for any of the red flags describe in the guidance;

7. Refreshing information obtained as part of customer due diligence on a periodic basis and commensurate with the risk.

But the real challenge is the due diligence requirement to determine whether any of the “priorities” listed in the guidance could be “implicated” by the marijuana-related business. The “priorities” include:

• Preventing the distribution of marijuana to minors;
• Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels;
• Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
• Preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
• Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
• Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
• Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on public lands; and
• Preventing marijuana possession or use on federal property.

FinCEN also notes in these guidelines that “marijuana is a dangerous drug and that the illegal distribution and sale of marijuana is a serious crime that provides a significant source of revenue to large-scale criminal enterprises, gangs, and cartels. The Department of Justice is committed to enforcement of the Controlled Substance Act consistent with those determinations.”
MEMEBER DUE DILIGENCE CHECK LIST

Does the credit union have an adequate Member Due Diligence (MDD) process in place:

- that is commensurate with the credit union’s BSA/AML risk profile?
- that contains a clear statement of management’s overall expectations?
- that contains a clear statement of management’s expectations regarding staff responsibilities?
- that ensures the credit union possesses sufficient member information to implement an effective suspicious activity monitoring system?
- that provides guidance for documenting analysis associated with the due diligence process?
- that ensures that credit unions maintain current member information?
- to gain an understanding of each member’s normal and expected transaction activity?
- to look for indicators of potential changes in the members’ risk profiles?
- that include enhanced and ongoing due diligence procedures for higher-risk members?
Currency Transaction Reports (CTR)

The BSA requires all financial institutions to file a currency transactions report (CTR) for each:

- deposit, withdrawal, payment, transfer or other transaction (i.e.: denomination exchanges, purchase of monetary instruments);
- involving currency of more than $10,000;
- unless an exemption applies.

A CTR is filed only on currency transactions. Currency includes cash from any country - coin or paper.

Structuring

Multiple transactions, totaling more than $10,000, made during the course of one business day, by or on behalf of any member, should be consolidated and reported as one transaction. It is the credit union’s responsibility to watch out for anyone trying to structure their transaction in an effort to avoid CTR reporting.

For example, member Jim makes:

- a $4,000 deposit at Branch #1,
- a $4,000 deposit at Branch #2, and
- a $3,000 deposit through an ATM machine – all on the same day.

If the credit union is aware of all of these transactions, it must file a CTR reporting the $11,000 in currency deposits made by Member Jim.

Aggregating Transactions

Keep in mind that you only consolidate all of the deposits or all of the withdrawals. You do not add deposits and withdrawals together or off-set them.

For example, Member Jan:

- deposits $6,000 in currency to her savings account (Cash In).
- withdraws $4,000 in cash from her checking account (Cash Out).
- presents $5,000 in currency to be exchanged for Euros ($5,000 Cash In and $5,000 in Euros Cash Out).

Aggregating her Cash In ($6,000 deposit and $5,000 to be exchanged) – the credit union must report the $11,000 Cash In. Aggregating her Cash Out ($4,000 withdrawal and receiving $5,000 in foreign currency - Euros) – the credit union is not required to report the $9,000 Cash Out.

Also, credit unions should be on alert for members who enter the credit union planning to deposit or withdraw over $10,000 in currency and change their minds when learning that a CTR will be filed. For example, the member might instead deposit or withdraw only $9,000.

A CTR should not be filed for suspicious transactions involving $10,000 or less in currency or to note that a transaction of more than $10,000 is suspicious. Any suspicious or unusual activity
should be reported using FinCEN’s Suspicious Activity Report (SAR). (For more information go to SARs chapter)

**Deposits made at night or over the weekend or holiday**, must be aggregated and treated as if they were made on the next business day. For credit unions that are open on Saturday, whether Saturday is considered a “business day” or “the weekend” is addressed in the CTR instructions: “For a bank, a business day is the day on which transactions are routinely posted to customers’ accounts, as normally communicated to depository customers.”

NCUA’s Examples:

- A member places one deposit bag into the night depository at a credit union on Friday night, two bags on Saturday (the credit union isn’t open on Saturday) and two on Sunday. Then on Monday morning, a teller processes all five deposit bags and deposit slips at the same time, but posts each individual deposit separately.

  Because these deposits occurred at night and over the weekend they should be treated as a single transaction for reporting purposes, having been received on Monday, the following business day.

- Two employees representing the same small business in their town each make a $7,000 currency deposit to the company’s account during the same business day. The deposits are made at different branches of the credit union. Because both deposits are on behalf of the same company and made at the same credit union, they are subject to aggregation. A CTR must be filed if the credit union is aware of both transactions.

**Aggregation for Businesses with Common Ownership**

FinCEN issued a ruling in 2012 that stated that although multiple businesses may share a common owner, the presumption is that separately incorporated entities are independent persons. Therefore, the currency transactions of separately incorporated businesses should not automatically be aggregated as being on behalf of any one person simply because those businesses are owned by the same person.

The presumption that the entities are separate, however, is rebuttable. It is ultimately up to a credit union to determine, based on information obtained in the ordinary course of business, whether multiple businesses that share a common owner are, in fact, being operated independently depending on all the facts and circumstances. The results of this determination affect whether the businesses’ currency transactions should be aggregated for purposes of complying with currency transaction reporting obligations.

If a credit union determines that these businesses (or one or more of the businesses and the private accounts of the owner) are not operating separately or independently of one another or their common owner - e.g., the businesses are staffed by the same employees and are located at the same address, the credit union accounts of one business are repeatedly used to pay the expenses of another business, or the business accounts are repeatedly used to pay the personal expenses of the owner - the credit union may determine that aggregating the
businesses’ transactions is appropriate because the transactions were made on behalf of a single person.

When determining whether to aggregate transactions as being on behalf of the same person, a credit union must use its knowledge of relevant facts and circumstances. There are no universal rules applicable to any situation. Once a credit union determines that the businesses are independent, then it should not aggregate the separate transactions of these businesses. Alternatively, once a credit union determines that the businesses are not independent of each other or their common owner, then the transactions of these businesses should be aggregated going forward.

CTR Filing Requirements

CTRs must be filed within 15 calendar days after the day of the transaction. If a credit union has failed to file CTRs on reportable transactions within the required time frame, it should begin the process of completing the forms and contact the BSA Helpline at 1-800-949-2732 or e-mail FRC@fincen.gov.

NOTE: The 25 day specifications compliance allowance has expired. In the 1980s, FinCEN issued an electronic specification referencing a 25 day period for filing on magnetic media between 1987 and 2008. This additional time allowance was to account for physically shipping the magnetic media to the processing center in Detroit, Michigan. After 2008, some businesses continued to ship their batch e-filing to Detroit, so FinCEN allowed the 25-day compliance period referenced in its earlier specifications to stand until March 31, 2013. This was to allow them to update their systems in order to be in compliance with the established regulatory 15 day requirements. After March 31, 2013, all CTRs must be filed within 15 days – no exceptions.

When filling out the CTR you will be providing information that identifies:
- the people involved in the transaction,
- the amount of currency involved,
- the type of transaction, and
- identifying information about your credit union.

There is a “multiple persons” section that must be completed if more than one person is involved in the transaction.

Joint Accounts: For deposits into joint accounts, a CTR must list all joint owners on the account, because they all have access to the funds at the moment they are deposited. In the case of account withdrawals, list only the individual who is making the withdrawal, unless you have facts to suggest that all or additional joint owners will benefit from the transaction.

NOTE: FinCEN has a 1995 Guidance that requires all financial institutions to list all joint owners on both joint account deposits and withdrawals – unless there was a reason to believe that only the individual making the transaction would benefit from the transaction. In 2009, CUNA was advised by FinCEN that its interpretation has changed and an updated guidance would be
issued “sometime in the near future”. The guidance finally appeared in FAQs issued in April 2013 to assist with the new electronic CTR. Questions 23 & 24 confirm FinCEN’s revised position for joint accounts.

This form is now electronic. For your CTR form questions, please contact FinCEN’s helpline at: 1-800-949-2732 or e-mail FRC@fincen.gov.

Record Retention

You must maintain copies of CTRs for 5 years from the date of the report.

CTR Exemptions

There are certain transactions that are so unlikely to aid in the prevention of criminal activity, that the BSA regulations have exempted them from CTR reporting.

There are two categories of exempt persons - Phase I and Phase II.

The Phase I designation exempts:
- credit unions and banks, to the extent of their domestic operations;
- government agencies, or departments;
- any entity exercising government authority on behalf of the United States, any state or political subdivisions;
- entities whose common stock is listed on the New York, American or Nasdaq stock exchanges (with some exceptions);
- any subsidiary of one of the stock exchange listed entities, where at least 51% of its stock is owned by the listed entity.

The Phase II designation includes two categories:
- non-listed businesses (which refers to those not listed on the stock exchange or their subsidiaries), and
- payroll members.

The “non-listed businesses” must meet the following 4 criteria:

- Must have maintained a transaction account with the credit union for at least 2 months, or, a member may be eligible in less than 2 months, if the credit union chooses to conduct a risk-based analysis to form a reasonable belief that the member has a legitimate business purpose for conducting frequent or regular large currency transactions. NOTE: Credit unions are not required to use the risk-based approach – the option is available to allow financial institutions to choose between the flexibility of a risk-based approach or the simplicity of the two-month threshold.
• Must frequently engage in transactions in currency with the credit union in excess of $10,000 (“frequently” means the member has conducted 5 or more reportable transactions in currency within a year);

• Must be organized or incorporated under the federal or a state law of the U.S.; and

• Must not derive more than 50% of its gross revenues from any “ineligible” business activity.

**Ineligible business activity:** There are certain types of businesses that the FFIEC considers “ineligible” to qualify as exempt from CTR filing, such as car dealers, pawnshops, race tracks, real estate brokers and several others.

31 CFR Chapter X
1020.315(e)(8)

**Ineligible businesses.** A business engaged primarily in one or more of the following activities may not be treated as a non-listed business for purposes of this section: Serving as financial institutions or agents of financial institutions of any type; purchase or sale to customers of **motor vehicles of any kind**, vessels, aircraft, farm equipment or mobile homes; the practice of law, accountancy, or medicine; auctioning of goods; chartering or operation of ships, buses, or aircraft; gaming of any kind (other than licensed parimutuel betting at race tracks); investment advisory services or investment banking services; real estate brokerage; pawn brokerage; title insurance and real estate closing; trade union activities; and any other activities that may be specified by FinCEN. A business that engages in multiple business activities may be treated as a non-listed business so long as no more than 50% of its gross revenues are derived from one or more of the ineligible business activities listed in this paragraph (e)(8).

NOTE: Phase I members may be treated as exempt regardless of their involvement in “ineligible” activities.

**Payroll Customers/ Members**

Payroll customers in Phase II include persons or businesses that meet the following 3 criteria:

• Maintain a transaction account with the credit union for at least 2 months or, a member may be eligible in less than 2 months, if the credit union chooses to conduct a risk-based analysis to form a reasonable belief that the member has a legitimate business purpose for conducting frequent or regular large currency transactions;

• Operate a firm that regularly **withdraws** more than $10,000 in order to pay its employees in currency (“regularly” means five or more reportable transactions in currency within the year); and

• Incorporated or organized under the federal or a state law of the U.S.
This exemption only applies to payroll withdrawals.

**Summary of Phases I Requirements:**

Source: FIN-2012-G003

<table>
<thead>
<tr>
<th>Type of Customer</th>
<th>Trans Freq.</th>
<th>Waiting Period</th>
<th>Ineligible Activity</th>
<th>File DOEP Report</th>
<th>Annual Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit unions &amp; banks</td>
<td>N/A</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Govt. departmts., agencies, or authorities</td>
<td>N/A</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Entities listed on stock exchange</td>
<td>N/A</td>
<td>None</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Subsidiaries of those listed on stock exchange</td>
<td>N/A</td>
<td>None</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Summary of Phase II Requirements:

<table>
<thead>
<tr>
<th>Type of Customer</th>
<th>Trans. Freq.</th>
<th>Waiting Period</th>
<th>Ineligible Activity</th>
<th>File DOEP Report</th>
<th>Annual Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-listed businesses</td>
<td>5 or more transaction/year</td>
<td>2 months, or less after risk based analysis</td>
<td>No more than 50% of gross revenues from ineligible activity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Payroll Customer</td>
<td>5 or more transaction/year</td>
<td>2 months, or less after risk based analysis</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Source: FIN-2012-G003

Designation of Exempt Person Form (DOEP)

In order for a credit union member to get a CTR exemption, the credit union must file a one-time Designation of Exempt Person (DOEP) form with FinCEN within 30 days after the first transaction in currency that the credit union member wants to exempt.

NOTE: The Designation of Exempt Person form is not required for credit unions, banks, government agencies or entities exercising government authority - they are automatically exempt. This means that operating cash transfers between a credit union and its corporate, the 12 Federal Reserve banks or another credit union or bank do not require a DOEP form to be filed. (Effective January 5, 2009)

The exemption applies only to transactions involving the exempt person’s own funds. If an exempt person conducts a transaction on behalf of someone else, that transaction does not fall under the exemption and the credit union must file a CTR for that transaction.
Annual Review

The credit union must maintain appropriate documentation of all CTR exemptions that are granted and it must review the granted exemptions on an annual basis for both Phase I and Phase II exemptions to make sure that they are still appropriate. Credit unions do not have to perform this annual review for credit unions, banks, or government agencies/departments.

If during a review it is determined that something has changed over the past year and the member is no longer eligible for the exemption – the member’s exemption status must be changed and the credit union must file CTRs going forward. Credit unions are not required to back file CTRs for the preceding year to the time when their member’s status actually changed.

[NOTE: Effective January 5, 2009, the previously required biennial renewal requirement for Phase II exemptions (non-listed businesses and payroll customers) has been removed from the rule and credit unions are no longer required to record and report a change of control over a Phase II exempt person.]

Suspicious Activity

The CTR exemption rules do not relieve you of your separate obligations to conduct an investigation of potential suspicious activity and, if appropriate, report such activity for both Phase I and Phase II exempt members. (For more information go to SARs chapter)

Safe Harbor for Exemptions

The credit union is not liable for the failure to file a CTR for a transaction in currency by an exempt person, unless the credit union knowingly provides false or incomplete information or has reason to believe that the member does not qualify as an exempt member.

Exceptional Relief for Armored Car Services

FinCEN issued guidance in 2013 to address situations where large currency transactions are conducted by an armored car service to debit or credit the account of the member. For example, where a member is a large cash business, such as a restaurant, and the business member contracts with an armored car service to pick up the cash from the restaurant and transport it to the credit union for deposit into the business account.
CURRENCY TRANSACTION REPORTING CHECKLIST
[Source: NCUA]

Does the credit union have an adequate process to identify transactions? ☐

Does the credit union file CTRs for all transactions and multiple transactions in currency in one day greater than $10,000, unless there is an exemption? ☐

Are CTRs filed within 15 days after the transaction occurs? ☐

Does the credit union properly exempt permitted persons from CTR filing by filing a “Designation of Exempt Person” form? ☐

For exempt persons, does the credit union perform an annual review of the account to ensure the exemption remains appropriate? ☐

Is the annual review of CTR exemptions documented? ☐

Are CTRs retained for 5 years? ☐
TEST YOUR KNOWLEDGE

Question 1:
True or False: A credit union must file a Currency Transaction Report (CTR) if a member purchases $15,000 worth of traveler’s checks with money from her checking account.

Question 2:
True or False: A member writes three checks (one check each) to three different people. The total amount of the three checks exceeds $10,000. Each payee cashes his check at the credit union on the same day. The total amount of cash that is withdrawn from the member’s account in one day is more than $10,000. The Bank Secrecy Act (BSA) Regulations require a credit union to file a Currency Transaction Report (CTR).

Question 3:
The compliance officer at Raven’s Federal Credit Union learned during an audit that a member made a $15,000 cash deposit at the teller lane but no Currency Transaction Report (CTR) was filed. The transaction occurred over two months ago. Should the form be filed?

Question 4:
Our member deposited $9,000 in cash at the credit union in the morning, and later that day withdrew $3,000 in cash from an ATM. Do we need to fill out a CTR?

Question 5:
A member goes to a grocery store and buys groceries in the amount of $50. The member swipes their debit card, enters a PIN and is asked if they would like cash back. They respond "yes" and ask for $50 cash making the total transaction $100. Earlier in the day the member withdrew $9,970 in cash from the credit union. Does the $50 in cash received from the debit card transaction get added to the $9,970 thereby requiring a CTR?

Question 6:
Does a CTR need to be filed when you know a member is placing more than $10,000 in a Safe Deposit Box?

Question 7:
Is a CTR required when a person presents a check, in excess of $10,000, for payment in cash at a financial institution and receives less than $10,000 after fees, or other deductions, are charged against the amount of the check?
Test Answers:

Answer 1:

False. A Currency Transaction Report (CTR) is filed for every deposit, withdrawal, payment, transfer or other transaction involving CASH (currency) of more than $10,000.00. This means that cash of any country, including any coin or paper money of the United States or of any other country, is included in the definition of currency. The purchase of cash equivalents or negotiable instruments like traveler’s checks don’t trigger a filing of a CTR unless made with cash and exceeds $10,000. This answer is false because the travelers’ checks were paid for merely by a transfer from the member’s account. By the way, the Bank Secrecy Act also requires a credit union to maintain certain information when the member purchases a “monetary instrument” – such as travelers’ checks, cashier checks, and money orders -- **with cash** in amounts from $3,000.00 to $10,000.00.

Answer 2:

False. The general rule is if a deposit, withdrawal, payment, transfer or other transaction involving cash of more than $10,000 is done in one day **by or on behalf of any person** a CTR must be filed. The BSA regulations require a credit union to treat multiple currency transactions as a single transaction and file a CTR only if the credit union has knowledge that the multiple transactions are by or on behalf of any person and the transactions result in either cash in or cash out totaling more than $10,000 during any single business day.

In this case, one person is not cashing the checks and, unless the credit union has knowledge otherwise, it has to assume the three individuals cashing the checks are not acting on behalf of the check-writer. This situation is similar to the situation where checks are written to pay bills. The creditors are not cashing the checks on the check-writer’s behalf - they are cashing the checks on their own behalf. The same is true in this case. The three individuals are presumably cashing the checks on their own behalf.

Of course, if the credit union has knowledge that the three individuals are acting on behalf of the check-writer, the credit union must file a CTR. Another thing to evaluate is if the check-writer has "structured" the transaction to avoid having a CTR filed. Structuring is when someone tries to divide a transaction into several different transactions to avoid the CTR filing. A good example of structuring is as follows: A credit union member comes in and tries to cash a $12,000 check. When he finds out that a CTR will be filed, he leaves and shortly thereafter three separate people come in to cash three $4,000 checks written on the member’s account. Not only should the credit union file a CTR in this example, but the credit union should also file a Suspicious Activity Report (SAR). Remember, if the credit union has any suspicions about the transaction or transactions, it should always file an SAR.

Answer 3:

Yes. According to the Bank Secrecy Act (BSA), a credit union has 15 days after a transaction to file a currency transaction report. In cases where this deadline has been missed, the CTR should be prepared and the reason(s) for delinquency documented.
If a credit union has doubts as to whether CTR backfilling of unreported transactions is necessary, it should contact FinCEN’s Regulatory Hotline at: 1-800-949-2732 or e-mail BSA_Resource_Center@fincen.gov.

**Answer 4:**

No. When aggregating cash transactions for the purpose of filling out a currency transaction report (CTR), you must consolidate deposits (Cash In) and withdrawals (Cash Out) separately. You do not add deposits and withdrawals together, or off-set them.

**Answer 5:**

No, this transaction does not trigger a CTR. According to FinCEN, since the transaction was POS and the merchant is effectively an intermediary between the credit union and the member, it doesn't meet the requirement that the transaction be "by, through or to the [credit union]." If the member had taken out the $50 from an ATM, it would trigger a CTR.

**Answer 6:**

No. You do not need to file a CTR in this situation because no "transaction" has occurred. A transaction is defined as "deposit, withdrawal, exchange or other payment or transfer". However, if the situation feels suspicious to you, you should consider filling out a suspicious activity report (SAR).

**Answer 7:**

The BSA only requires a CTR for a transaction in currency, such as a deposit, withdrawal, exchange or transfer of currency, in excess of $10,000. A transaction in currency involves the physical transfer of currency from one person to another. Accordingly, the transfer of currency below $10,000 would not trigger the CTR requirement, despite the amount of the check. For example, if a person cashed a check for $10,100 and received $9,990 after a service fee was charged against the amount of the check, the financial institution would not be required to file a CTR. On the other hand, if a person purchased a cashier’s check for $9,990 and paid a service fee of $20 for a total of $10,010 in cash, the financial institution would be required to file a CTR. The key lies in the amount of the physical deposit, withdrawal, exchange or transfer of currency.
Monetary Instruments

Credit unions sell a variety of monetary instruments (e.g., checks or share drafts, money orders, cashier's checks, traveler's checks, etc.) in exchange for currency. Purchasing these instruments in amounts of less than $10,000 is a common method used by money launderers to evade large currency transaction reporting requirements. That’s why the Bank Secrecy Act requires credit unions to keep records regarding the issuance or sale of monetary instruments for currency in amounts between $3,000 and $10,000, inclusive.

Purchaser Verification

The credit union’s records of sales must contain the following information.

If the purchaser has an account with the credit union:

- Name of the purchaser.
- Date of purchase.
- Types of instruments purchased.
- Serial numbers of each of the instruments purchased.
- Dollar amounts of each of the instruments purchased in currency.
- Specific identifying information, if applicable.

If the purchaser does not have an account with the credit union*:

- Name and address of the purchaser.
- Social Security or alien identification number of the purchaser.
- Date of birth of the purchaser.
- Date of purchase.
- Types of instruments purchased.
- Serial numbers of each of the instruments purchased.
- Dollar amounts of each of the instruments purchased.
- Specific identifying information for verifying the purchaser’s identity (e.g., state of issuance and number on driver’s license).

If the purchaser cannot provide the required information at the time of the transaction or through the credit union’s own previously verified records, the transaction should be refused.

*Federal credit unions (FCUs) are permitted to sell negotiable checks and money orders to non-members within their fields of membership (12 CFR 701.30). If the purchaser does not have an account with the credit union and is not in the FCU’s field of membership, the transaction cannot be conducted. The FCU should have policies and procedures in place to address providing services to non-members.
Contemporaneous Purchases

For purposes of recordkeeping, multiple purchases during one business day totaling $3,000 or more are treated as one purchase. Similarly, purchases of different types of instruments totaling $3,000 or more are treated as one purchase.

Recordkeeping Requirements

Records of monetary instrument sales of $3,000-$10,000 must be retained for five years, and can be maintained in either a manual or electronic format. Some readers may recall that when this recordkeeping requirement was first established, it mandated that financial institutions retain a centralized log of these sales of monetary instruments. However, the physical log requirement was eliminated in the mid-1990s.

If the credit union’s data processing system has the ability to generate a report that contains the required information, the credit union will not need to maintain a separate record of these transactions. However, the credit union must be able to generate this report for any currency transaction for the purchase of a credit union check, cashier’s check, money order, or traveler’s check. The credit union must also be able to aggregate these currency transactions to determine if a member or account made more than $10,000 in transactions during a day.

Monetary Instrument Recordkeeping Checklist

Is a record of required information maintained for the issuance or sale of each monetary instrument (i.e., credit union check, cashier’s check, traveler’s check, and/or money order) for currency in amounts between $3000 and $10,000?

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of purchaser</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of purchase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type(s) of instruments purchased</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial numbers(s) of each instrument(s) purchased</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amount in dollars of each instrument purchased</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Method used to identify the identity of the purchaser</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Frequently Asked Questions on Monetary Instruments

Q: Can the credit union require a member to deposit currency in their share account before purchasing monetary instruments?

A: Credit unions are permitted to implement a policy that requires members who want to purchase monetary instruments in amounts between $3,000 and $10,000 with currency to first deposit the currency into their deposit accounts. Nothing within the BSA, or its implementing regulations prohibits financial institutions from instituting such a policy. However, according to FinCEN, the transaction is still subject to the BSA recordkeeping requirements discussed in this chapter. Credit unions generally maintain most of this information in the normal course of business.

Q: Do credit unions need to maintain a hand written monetary instrument log if the computer system does not maintain this information?

A: Credit unions no longer have to maintain a chronological monetary instrument log, however, they do still need to maintain a record to document the purchase in currency and issuance of a credit union check, cashier’s check, money order, or traveler’s check in amounts of $3,000 to $10,000 inclusive.

The record of these transactions can be in either a manual or electronic format. The record must be kept for five years. If the credit union’s computer system has the ability to generate a report that contains the required information, it does not need to maintain a separate log. However, the credit union must be able to generate this report for any currency transaction for the purchase of a credit union check, cashier’s check, money order, or traveler’s check. And, the credit union must be able to aggregate these currency transactions to determine if a member or account made more than $10,000 in transactions during a day.

Q: Are credit unions required to collect monetary instrument data for the sales of stored value cards?

A: No. According to FinCEN and NCUA, doing so is not currently required by statute or regulation. Stored value or prepaid cards technically fall outside of the definition of a “monetary instrument.” However, some institutions voluntarily collect the information for BSA recordkeeping purposes as a best practice.

Note: FinCEN issued a rule in 2011 to require providers of prepaid access to file SARs, collect and retain customer transactional information, and maintain an anti-money laundering program – similar to what financial institutions and other categories of money services businesses (MSBs) are required to do. This rule falls under FinCEN’s MSB regulations and does not apply to credit unions.
Q: Are credit unions required to file Form 4790, Report of International Currency or Monetary Instruments (CMIR)?

A: While the BSA regulations provide exceptions from filing, the exceptions generally do not apply to member transactions. However, the credit union is not required to file a CMIR (FinCEN Form 105) for transfers of funds through normal credit union operations, which do not involve the physical transportation of currency or monetary instruments.

A person (member) must file whenever he or she: physically transports, mails, or ships; causes to be physically transported, mailed, or shipped; attempts to physically transport, mail or ship; or attempts to cause to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside the United States, or into the United States from any place outside the United States. A person is deemed to have caused such transportation, mailing or shipping when he aids, abets, counsels, commands, procures, or requests it to be done by a financial institution or any other person.
Funds Transfers

The Bank Secrecy Act requires credit unions to collect and retain certain information in connection with “funds transfers” of $3,000.00 or more. The funds transfer rules are intended to help law enforcement agencies detect, investigate and prosecute money laundering and other financial crimes by preserving an information trail about persons sending and receiving funds through funds transfer systems.

The term “funds transfer” generally refers to wire transfers. A “funds transfer” is a “series of transactions, beginning with the originator’s payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by the originator’s bank or an intermediary bank intended to carry out the originator's payment order. A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order.” Fund transfers “as defined by the Electronic Fund Transfer Act,” as well as any other funds transfers that are made through an automated clearinghouse, an automated teller machine, or a point-of-sale system, are excluded from this definition.

❖ Please note that wire transfers that are “remittance transfers” under the EFTA and Regulation E are subject to the BSA funds transfer rule.

Other Key Terms

Here are some key terms used throughout this chapter:

Beneficiary financial institution: financial institution receiving a payment or transmittal order for payment to its member’s account.

Intermediary financial institution: a receiving financial institution, other than the transmittor’s financial institution or the recipient’s financial institution.

Originator: the sender of the first payment order in a funds transfer.

Originator's financial institution: the financial institution that issues the payment or transmittal order for the originator, unless the originator is the financial institution itself.

Payment or transmittal order: an instruction to a financial institution to effect payment.

Receiving financial institution: the financial institution to which the sender’s instruction is addressed.

Transmittor's financial institution: the financial institution that issues the transmittal order for the transmittor, unless transmittor is the financial institution itself. The term transmittor's financial institution generally includes an originator’s financial institution.
Travel Rule

The Bank Secrecy Act’s (BSA) “Travel Rule” requires the credit union to include certain information in payment orders relating to transmittals of funds (mostly wires) of $3,000 or more, whether or not currency is involved. In other words, certain information must “travel” with the wire. Again, funds transfers governed by Regulation E or the Automated Clearinghouse rules are not covered by the Travel Rule.

All “transmittor’s financial institutions” (generally speaking, the originating financial institution) must include and send the following in the transmittal order:

- The transmittor’s name, account number, and address;
- The identity of the transmittor’s financial institution;
- The amount of the transmittal order;
- The execution date of the transmittal order; and
- The identity of the recipient’s financial institution.

If received, the transmittor’s financial institution must also include the name, address, account number and any other specific identifier of the recipient. In addition, an intermediary financial institution must pass on all of the information it receives from a transmittor’s financial institution or the preceding intermediary financial institution.

The “customer information files” (CIF) exception to the rule, which expired on July 1, 2004, permitted financial institutions under certain conditions to exclude a transmitter’s true name and street address from transmittal orders and substitute coded information instead. Many financial institutions had operational difficulties complying with the rule because many transmittals were automated, and in some cases, the CIF records did not accurately reflect the true name and a street address of the transmittor. Credit unions that wire funds will violate the Travel Rule if their transmittals do not accurately reflect the “true” name and address of the transmittor of funds.

Exceptions to the Funds Transfer Rule

The following transfers are excluded from the BSA funds transfer rules:

- Transfers of less than $3,000;
- Debit transfers;
- “Electronic fund transfers” as defined by the Electronic Fund Transfer Act, as well as any other funds transfers made through ATM, ACH, and POS systems;
• Transfers where both the originator and the beneficiary are any of the following:
  
  o a domestic bank (definition of “bank” includes credit union);
  o a wholly-owned domestic subsidiary of a domestic bank;
  o a domestic broker or dealer in securities;
  o a wholly-owned domestic subsidiary of a domestic broker or dealer in securities;
  o the United States;
  o a state or local government; or
  o a federal, state or local government agency or instrumentality; and

• Transfers where both 1) the originator and the beneficiary are the same person, and 2) the originator’s and beneficiary’s financial institution are the same “domestic bank.”

Responsibilities of an Originating Financial Institution

Recordkeeping Requirements

For each payment order in the amount of $3,000 or more that a credit union accepts as an originating financial institution (“originator’s bank”), the credit union must obtain and retain the following records:

  • Name and address of the originator;
  • Amount of the payment order;
  • Date of the payment order;
  • Any payment instructions;
  • Identity of the beneficiary’s institution;
  • As many of the following items as are received with the payment order:
    o Name and address of the beneficiary;
    o Account number of the beneficiary;
    o Any other specific identifier of the beneficiary.

If the originator is not an established member¹, the credit union should collect and retain the information listed above. In addition, the originator’s financial institution must collect and retain other information, depending on whether the payment order is made in person.

Payment Orders Made in Person

If the payment order is made in person, the credit union must verify the identity of the person placing the payment order before it accepts the order. If it accepts the payment order, the credit union must obtain and retain the following records:

¹ Federal credit unions (FCUs) may offer wire transfer services to non-members within their fields of membership (12 CFR 701.30).
• Name and address of the person placing the order.

• Type of identification reviewed.

• Number of the identification document (e.g., driver’s license).

• The person’s taxpayer identification number (TIN) (e.g., Social Security number (SSN) or employer identification number (EIN)) or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. If the originator’s financial institution has knowledge that the person placing the payment order is not the originator, the institution must obtain and record the originator’s TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.

Payment Orders Not Made in Person

If a payment order is not made in person, the credit union must obtain and retain the following records:

• Name and address of the person placing the payment order; and

• The person’s TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof, and a copy or record of the method of payment (e.g., check or credit card transaction) for the funds transfer. If the originator’s financial institution has knowledge that the person placing the payment order is not the originator, the institution must obtain and record the originator’s TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.

Retrievability Requirements

Information retained must be retrievable by reference to the name of the originator. When the originator is a member whose account is used for funds transfers, information retained must also be retrievable by account number. Records must be maintained for five years.

Travel Rule Requirement

For funds transmittals of $3,000 or more, the credit union must include the following information in the transmittal order at the time that the order is sent to a receiving financial institution:

• Name of the transmittor, and, if the payment is ordered from an account, the account number of the transmittor;

• Address of the transmittor;
• Amount of the transmittal order;

• Date of the transmittal order;

• Identity of the recipient's financial institution;

• As many of the following items as are received with the transmittal order:
  o Name and address of the recipient;
  o Account number of the recipient;
  o Any other specific identifier of the recipient.

• Either the name and address or the numerical identifier of the transmittor's financial institution.

There are no recordkeeping requirements in the Travel Rule.

Responsibilities of an Intermediary Financial Institution

Recordkeeping Requirements

The credit union must retain a record of each payment order of $3,000 or more that it accepts as an intermediary financial institution.

Travel Rule Requirements

For funds transmittals of $3,000 or more, an intermediary financial institution must include the following information, if received from the sender in the original transmittal order:

• Name and account number of the transmittor;

• Address of the transmittor;

• Amount of the transmittal order;

• Date of the transmittal order;

• Identity of the recipient's financial institution;

• As many of the following items as are received with the transmittal order:
  o Name and address of the recipient;
  o Account number of the recipient;
  o Any other specific identifier of the recipient.
• Either the name and address or the numerical identifier of the transmittor's financial institution.

The credit union as an intermediary financial institution must pass on all of the information received from the preceding institution. However, the credit union has no duty to obtain any additional information.

Responsibilities of a Beneficiary's Financial Institution

Recordkeeping Requirements

The credit union must retain a record of each payment order of $3,000 or more that it accepts as a beneficiary's financial institution. If the beneficiary is not an established member (*see note on page 7), the credit union must retain the following information.

Proceeds Delivered in Person

If proceeds are delivered in person to the beneficiary or its representative or agent, the institution must verify the identity of the person receiving the proceeds and retain a record of the following:

• Name and address;
• The type of document reviewed;
• The number of the identification document;
• The person's TIN, or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof;
• If the institution has knowledge that the person receiving the proceeds is not the beneficiary, the institution must obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's identification;

Proceeds Not Delivered in Person

If proceeds are not delivered in person, the credit union must retain a copy of the check or other instrument used to effect the payment, or it must record the information on the instrument. The institution must also record the name and address of the person to which it was sent.

Retrievability Requirements

Information retained must be retrievable by reference to the name of the beneficiary. When the beneficiary is an established member of the credit union and has an account used for funds transfers, information retained must also be retrievable by account number.
There are no Travel Rule requirements for beneficiary financial institutions.

Recordkeeping requirements for originators, intermediaries and beneficiary financial institutions excerpted from the “Core Overview - Funds Transfers” in the FFIEC BSA/AML Examination Manual.
Funds Transfer Recordkeeping Checklist

For funds transfers of $3,000 or more, does the credit union retain a record of the following information?

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and address of originator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amount of the payment order</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution date of the payment order</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment instructions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity of the beneficiary’s bank</td>
<td></td>
<td></td>
</tr>
<tr>
<td>As many of the following as are received with the order:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name and address of beneficiary;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account number of beneficiary; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other specific identifier of the beneficiary?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Frequently Asked Questions on Funds Transfers

Q: Are all funds transfers subject to the recordkeeping requirements, regardless of the size of the transaction?

A: No, only covered funds transfers equal to or greater than $3,000 are subject to the rule. Remember that a number of funds transfers are excluded from the rule, including funds transfers governed by the Electronic Fund Transfer Act (Regulation E) and Automated Clearinghouse (ACH) rules. Therefore, funds transfers that are made through an automated clearinghouse, an automated teller machine, or a point-of-sale system, are excluded from coverage. See “Exceptions” on page 3.

Q: Since ATM, ACH and POS transactions are exempt from coverage, what is an example of a funds transfer that does not involve a wire that would still be covered by the BSA funds transmittal rules?

A: A check can be the transmittal order within a transmittal of funds. For example, a member orders a transmittal of funds at the credit union to be sent to a customer at another financial institution. The credit union, as the originating institution sends its own check payable to the other financial institution rather than the institution’s customer. The check contains accompanying instructions to have the financial institution subsequently credit customer’s account. In such a case, the check and its instructions are the transmittal order effecting a transmittal of funds.

Q: Do the funds transfer rules apply to transfers from a member’s individual credit union account to his or her joint account at the same credit union?

A: No. The originator and beneficiary are the same person, and the originator’s and beneficiary’s financial institution are the same “domestic bank.” These transfers are excepted from the rule.

Q: How long must information collected be kept under the Travel Rule?

A: All collected information is required to be maintained for at least five years.

Q: Does the rule require the credit union to report the collected information to the government?

A: No, however, the information related to a funds transfer may be subject to the BSA’s suspicious activity reporting requirements detailed in Chapter 5.
Q: When a credit union requires the assistance of its corporate credit union to wire funds, which party has responsibility for recordkeeping?

A: Both the credit union, as the originator of the wire transfer, and the corporate credit union, as an intermediary financial institution, have record keeping responsibilities under the BSA regulations.

The credit union as originator must maintain records of all wire transfers in the amount of $3,000 or more with the following exceptions:

(a) Funds transfers where the originator and the beneficiary are any of the following:
   
   (1) a bank, thrift, or credit union;
   (2) a wholly-owned domestic subsidiary of a bank, thrift, or credit union chartered in the United States;
   (3) a broker or dealer in securities;
   (4) a wholly-owned domestic subsidiary of a broker or dealer in securities;
   (5) a futures commission merchant or an introducing broker in commodities;
   (6) a wholly-owned domestic subsidiary of a futures commission merchant or introducing broker in commodities;
   (7) the United States;
   (8) a state or local government; or
   (9) a federal, state or local government agency or instrumentality; and

(b) Funds transfers where both the originator and beneficiary are the same person and the originator’s bank, thrift, or credit union, and the beneficiary’s bank, thrift, or credit union are the same.

The credit union originating the wire transfer must retain the original, a microfilm copy, or some other copy or electronic record of the following information:

- Name and address of the originator of the payment order;
- Amount of the payment order;
- Execution date of the payment order;
- Any payment instructions received from the originator;
- Identity of the beneficiary’s financial institution; and
- As many of the following items as are received:
  - Name and address of the beneficiary
  - Account number of the beneficiary
  - Any other specific identifier of the beneficiary

The corporate credit union, when acting as an intermediary financial institution, must retain the original or a microfilm, other copy, or electronic record of the payment order for each payment order it accepts.

In addition, before completing the transaction and transmitting funds, each credit union has a responsibility to check the OFAC SDN list and to ensure there is no match. Source: NCUA Letter to Credit Unions No. 05-CU-09
Suspicious Activity Reports

Credit unions are required to file a Suspicious Activity Report (FinCEN SAR Form 111) via FinCEN’s E-Filing System with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
  - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
  - Is designed to evade the BSA or its implementing regulations.
  - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a financial institution.

SARs & Marijuana-Related Activities

A financial institution’s obligation to file a SAR is unaffected by state laws legalizing marijuana-related activities. The FinCEN provides specific guidelines for SAR filings related to serving these businesses. A financial institution would file a:

- “Marijuana Limited” SAR if the institution reasonably believes (based on CDD) that the marijuana-related business does not violate state law or implicate one of the DOJ’s enforcement priorities.
- “Marijuana Priority” SAR if the institution reasonably believes (based on CDD) the business being conducted implicates one of the DOJ enforcement priorities or violated state law.
• “Marijuana Termination” SAR if the institution terminates a member/customer for reasons related to its anti-money laundering compliance program.

FIN-2014-G001: BSA Expectations Regarding Marijuana-Related Businesses (fincen.gov)

What is “suspicious activity”?

So, what exactly is “suspicious activity”? Suspicious activity covers anything from unusual behavior to obvious efforts to avoid BSA recordkeeping requirements. There are a number of activities that should raise a “red flag” in the minds of credit union personnel as possibly facilitating money laundering or terrorist financing. When encountered, these types of activities warrant closer scrutiny, which will sometimes include filing a SAR. Some examples of suspicious activity include:

• A member uses unusual or suspicious identification documents that cannot be readily verified.

• A member makes frequent or large transactions and has no record of past or present employment experience.

• A member separates a cash transaction over $10,000 in to several transactions in an attempt to avoid the CTR reporting threshold (see “Structuring” below).

• A member is reluctant, when establishing a new account, to provide complete information about the nature and purpose of his business, anticipated account activity, prior relationships with financial institutions, information on the location of the business or the names of its officers and directors.

• A member tries to persuade a credit union employee not fill out a CTR or maintain required records.

• Many small, incoming wires are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the member’s transaction history.

• Wire or EFT activity is unexplained, repetitive, or shows unusual patterns.

The FFIEC BSA/AML Examination Manual provides a number of additional examples of red flags for both money laundering and suspicious activity.

Some characterizations of suspicious activity for purposes of completing the SAR include: BSA structuring/money laundering; bribery/gratuity; check fraud; check kiting; commercial loan fraud; unauthorized electronic intrusion; consumer loan fraud; counterfeit check, credit/debit card, or other instrument; credit card fraud; debit card fraud; defalcation/embezzlement; false statement;
Structuring

Structuring occurs when a person breaks up a transaction for the purpose of evading the BSA reporting and recordkeeping requirements. Credit unions are required to file a SAR whenever a transaction involves or aggregates at least $5,000, and the credit union knows or suspects that the transaction is designed to evade any requirements of the BSA. Therefore, to comply with the suspicious activity reporting requirements, the credit union must have systems in place to identify the kinds of transactions and accounts that may exhibit suspicious activity, such as structuring.

Unlawful structuring of transactions can take two basic forms:

- A member might deposit currency on multiple days in amounts under $10,000 (e.g., $9,900.00) for the intended purpose of circumventing the credit union’s obligation to report any cash deposit over $10,000 on a CTR. These deposits do not require aggregation for currency transaction reporting since they occur on different business days. However, they do meet the definition of structuring under the BSA.

- A member or members may engage in multiple transactions during one day or over a period of several days or more, in one or more of the credit union’s branches, in a manner intended to evade either the CTR or some other BSA requirement, such as the recordkeeping requirements for wire transfers of $3,000 or more.

The credit union’s anti-money laundering program should be designed to detect and report both categories of structuring to guard against use of the institution for money laundering, and ensure the institution is compliant with the suspicious activity reporting requirements of the BSA.

*FinCEN Ruling 2005-6: Suspicious Activity Reporting (Structuring)*

Timing of a SAR Filing

BSA regulations require that a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days.

Credit unions may need to review transaction or account activity for a member to determine whether to file a SAR. The need for a review of account activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the credit union, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.

According to the FFIEC BSA/AML Examination Manual, the phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review:
“There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an account holder’s normal account activity. For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The bank’s automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is “suspicious” within the meaning of the SAR regulation.”

SAR Filing on Continuing Activity

According to FinCEN guidance, financial institutions may file SARs for continuing activity after a 90-day review with the filing deadline being 120 days after the date of the previously related SAR filing. Institutions may also file SARs on continuing activity earlier than the 120-day deadline if the institution believes the activity warrants earlier review by law enforcement.”

So, for filings where a subject has been identified, the timeline is as follows:

- Identification of suspicious activity and subject: Day 0.
- Deadline for initial SAR filing: Day 30.
- End of 90 day review: Day 120.
- Deadline for continuing activity SAR with subject information: Day 150 (120 days from the date of the initial filing on Day 30).

If the activity continues, this timeframe will result in three SARs filed over a 12-month period. From FinCEN’s online BSA FAQs (fincen.gov).

FinCEN and the financial institution regulators recommend that institutions develop policies, procedures, and processes indicating when to escalate issues or problems identified as result of repeat SAR filings on accounts. The procedures should include:

- Review by senior management and legal staff (e.g., BSA compliance officer or SAR committee).
- Criteria for when analysis of the overall member relationship is necessary.
- Criteria for when to close the account.
- Criteria for when to notify law enforcement, if applicable.

The credit union should continue to file SARs if conduct continues, even if a law enforcement agency has declined to investigate or there is knowledge that an investigation has begun. The filing of SARs on continuing suspicious activity provides useful information to law enforcement, and the information contained in a SAR that one law enforcement agency has declined to investigate may be of interest to other law enforcement agencies, as well as supervisory agencies.
Board Notification of SAR Filings

NCUA regulations require credit unions to “promptly” notify their board of directors (or its designated committee) of SAR filings. The NCUA has defined “prompt” to mean at least monthly, unless the seriousness of an activity merits immediate reporting. The rule does not specify a particular method of reporting to provide credit unions flexibility in tailoring a format to their particular needs and circumstances.

Safe Harbor from Civil Liability and SAR Confidentiality

The BSA provides protection from civil liability for all reports of suspicious transactions made to “appropriate authorities,” including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the thresholds.

FinCEN recently updated the BSA regulations to further clarify its expectation with regard to SAR confidentiality. Under the previous regulation, a credit union and its officers, directors, employees, etc. were prohibited from notifying any person that was the subject of a SAR report. To further clarify the scope of confidentiality surrounding SAR reports, FinCEN issued a final rule and accompanying guidance clarifying SAR confidentiality. According to the final rule, credit unions are not to disclose the SAR or any information revealing the existence of a SAR to parties other than those authorized to receive this information such as appropriate law enforcement, regulators, etc. FinCEN notes that it was important to clarify the scope of the provision due to the potentially serious consequences of an unauthorized disclosure.

The credit union should contact FinCEN and NCUA if it receives a request for a copy of a SAR or information contained in the SAR from anyone other the entities mentioned above. In addition, the credit union should make sure that it has the proper internal controls in place to minimize the risks of SAR disclosure.

What about law enforcement inquiries and requests?

As mentioned above, credit unions are only permitted to disclose information related to the SAR filing to FinCEN, appropriate law enforcement authorities or to its federal regulator, NCUA. Right to Financial Privacy Act protections are not triggered by requests for supporting documentation, related to SAR filings, made by FinCEN, appropriate law enforcement or a supervisory agency. “Supporting documentation” has been defined to mean all documents and records that assisted the credit union in making the determination to file the SAR.

Credit unions need to have policies and procedures in place to respond to such requests (e.g., subpoenas, 314(a) requests, National Security Letters), monitoring the transaction activity of suspects, and identifying unusual or suspicious activity related to these individuals or entities. In some cases, the credit union will need to file a SAR related to the subjects of law enforcement inquiries. However, mere receipt of any law enforcement inquiry, does not, by itself, require the credit union to file a SAR.
Nevertheless, a law enforcement inquiry may be relevant to the credit union’s overall risk assessment of certain members and accounts. The credit union should assess all of the information it knows about a member, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program. The credit union should also determine whether a SAR should be filed based on all of the available information on a member.

Credit unions are not required to file a SAR for a robbery or burglary as long as it is reported to the local law enforcement authorities.

**Transaction Monitoring**

NCUA and the banking regulators expect financial institutions to have policies and procedures in place to monitor suspicious transactions. A transaction monitoring system can either be manual: consisting of a manual review of various reports generated by the credit union’s data processing system; or automated: a system designed to automatically detect and alert staff to unusual or atypical transactions. Upon identification of any unusual activity, the Compliance Officer or other assigned personnel should review the member’s account activity to determine whether the activity is “suspicious.”

**Manual Systems**

Examples of reports generated by manual systems include:

- Currency activity reports
- Wire transfer reports
- Monetary instrument sales reports
- Large item reports
- Significant balance change reports, and
- Non-sufficient funds (NSF) reports.

The process of transaction monitoring may involve the review of daily reports, reports that cover a period of time (e.g., weekly or monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the credit union’s BSA/AML risk profile and appropriately cover its high-risk products, services, members, and the geographic locations of its main and branch offices.

Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. In addition, the programming of the credit union’s monitoring systems should be independently reviewed as part of the credit union’s BSA audit.

**Automated Systems**

Automated account-monitoring systems typically use computer programs, developed in-house or purchased from vendors, to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, ACH transactions, and ATM transactions,
directly from the credit union’s core data processing system. Large financial institutions that operate in many locations or have a large volume of high-risk customers typically use automated account-monitoring systems.

Current types of automated systems include rule-based and intelligent systems:

- Rule-based systems detect unusual transactions that are outside of system-developed or management-established "rules." These rules are applied using a series of transaction filters or a rules engine. Rule-based automated monitoring systems can apply complex or multiple filters.

- Intelligent systems are adaptive systems that can change their analysis over time on the basis of activity patterns, recent trends, changes in the customer base, and other relevant data. Intelligent systems review transactions in context with other transactions and the member’s profile. In doing so, these systems increase their information database on the member, account type, etc. as more transactions and data are stored in the system.

As with the manual system, management should periodically review the filtering criteria and thresholds established to ensure that they are still effective and appropriate for the institution. The credit union’s programming methodology should also be independently validated.
Frequently Asked Questions on Suspicious Activity Reporting

Q: Is a credit union required to file both a CTR and a SAR for a suspicious transaction in excess of $10,000 in cash?

A: Yes. The BSA requires all financial institutions to file currency transaction reports (CTRs) whenever a currency transaction exceeds $10,000 unless an exemption applies. If a currency transaction exceeds $10,000 and is suspicious, the credit union must file both a CTR and a SAR reporting the suspicious or criminal aspects of the transaction. If a currency transaction equals or is below $10,000 and is suspicious, the institution should only file a suspicious activity report. This information is contained in the instructions to the SAR.

Q: A teller happens to notice that three individual depositors arrived together in the same automobile. They each got in line and proceeded to deposit $5000.00 in currency into different accounts at the credit union. Should the credit union complete a SAR if it suspects that these transactions are related?

A: Yes, the credit union should complete a SAR if it suspects that these three $5000.00 deposits are related. Suspicious activity often involves related transactions conducted by two or more people. For example, different individuals may structure cash deposits so that they fall below the CTR reporting threshold.

If the credit union wants to report suspicious activity involving multiple suspects, it should include as many copies of Page One of the SAR as there are suspects and complete a separate Part II for each suspect. The narrative should include a complete description of the transactions involved (time, place, type of transaction, type of instruments, amounts involved, circumstances that make the transactions suspicious, etc.) and a description of the relationship between or involvement of the suspects.

The credit union’s member attempts to cash a fraudulent cashier’s check that was provided to him by the person who just purchased his used car. How should the credit union complete the SAR when one of its members is the victim of a crime?

When the credit union’s member is the victim of a crime, the credit union should not provide “Suspect Information” about the member in Part II of the Suspicious Activity Report. The suspect that should be listed in Part II is the person, if known, who defrauded the member (i.e., the person who gave the member the fraudulent cashier’s check). The credit union may include information about the member/victim in the narrative portion of the SAR.

The credit union will have few details about the suspect. However, the member should be able to provide a description of the suspect, a name, or a phone number or an email address that was used to correspond with the suspect before the transaction. If suspect information is unknown or unavailable, the credit union should mark the box in Part II of the Suspicious Activity Report form entitled “Suspect Information Unavailable.” However, any partial or incomplete identifying information should be included in Part II, or in the narrative. Responses commonly used to clarify why data is not being provided include: none, not applicable and unknown.
Q: What should the credit union do if it determines that it has filed incorrect information on the SAR?

A: The credit union should file a corrected report. When correcting an error on a previously filed report, mark box 1 (“corrects prior report”) and follow the directions to make the necessary changes. Whenever a corrected report is filed, the credit union should explain the changes in the SAR narrative. The credit union may need to correct a clerical error, such as an incorrectly reported name or address. Or, it may discover previously undetected suspicious activity related to a previously filed SAR, in which case the date range, dollar amounts, summary characterization and narrative of the original Suspicious Activity Report may need to be amended.

Q: What is the filing timeframe for submitting a continuing activity SAR?

A: Credit unions may file SARs for continuing activity after a 90-day review with the filing deadline being 120 days after the date of the previously related SAR filing. Financial institutions may also file SARs on continuing activity earlier than the 120-day deadline if the institution believes the activity warrants earlier review by law enforcement.”

So, for filings where a subject has been identified, the timeline is as follows:

Day 0: Identification of suspicious activity and subject:
Day 30: Deadline for initial SAR filing:
Day 120: End of 90 day review:
Day 150 (120 days from the date of the initial filing on Day 30): Deadline for continuing activity SAR with subject information

If the activity continues, this timeframe will result in three SARs filed over a 12-month period.

-FinCEN SAR Frequently Asked Questions (fincen.gov)

Q: Are credit unions required to notify their boards of directors whenever a SAR is filed?

A: Yes, in October 2006 NCUA issued a final rule requiring credit unions to “promptly” notify their board of directors of SAR filings. “Promptly” has been defined as “at least monthly”, unless the seriousness of the activity merits immediate reporting.

Q: Should a credit union file a SAR when there is a data security breach that potentially exposes members’ confidential financial information to computer hackers?

A: Yes. The credit union is required to file a SAR in the case of a data security breach. For purposes of the SAR, “computer intrusion” is defined as gaining access to a computer system of a financial institution to:

- Remove, steal, procure, or otherwise affect funds of the credit union or its members;
- Remove, steal, procure or otherwise affect critical information of the credit union including member account information; or
- Damage, disable or otherwise affect critical systems of the credit union.
For purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other “non-critical information systems” of the credit union (or its data processor) that provide no access to credit union or member financial or other critical information.

Credit unions should also review Part 748, Appendix B of NCUA’s security regulation for the appropriate steps to take when a data security breach at the credit union has compromised sensitive member information.

Q: A member walks into the credit union to conduct a transaction, then changes or restructures the transaction after asking the teller whether a CTR was filed. Must the credit union report that on a SAR?

A: Yes, the credit union should file a SAR if the teller and the BSA compliance officer agree that the member is attempting to avoid currency transaction reporting requirements.

Q: Is the credit union required to file a SAR each time it files a blocking report with the Office of Foreign Assets Control (OFAC)?

A: No. According to FinCEN, blocking reports filed with the Office of Foreign Assets Control (OFAC) fulfill the BSA’s requirement to file SARs for such transactions.

OFAC requires credit unions to block (“freeze”) property and payment of any fund transfers or transactions involving blocked countries or individuals, and to report the "blocks" within 10 days of occurrence. These so-called blocked countries and individuals appear on OFAC’s “Specially Designated Nationals and Blocked Persons” List (SDN List). Failure to block and report an “illicit transfer” may subject the credit union to civil fines, and possibly criminal penalties.

There may still be instances where the credit union will have to file reports with both FinCEN and OFAC. For example, credit unions are required to file an SAR in addition to the OFAC report if a transaction triggers BSA reporting rules for reasons other than a match on OFAC’s list (e.g., suspected money laundering or ID theft); or if the credit union possesses information not included on the OFAC report that should be filed with FinCEN.

Q: Should the credit union file a copy of a SAR with a state law enforcement agency?

A: “Banks” (definition includes credit unions) are “encouraged” to file a copy of the SAR with state and local law enforcement agencies “where appropriate.”

Q: Can the credit union close a member’s share account after identifying suspicious activity and filing a SAR?

A: According to the NCUA Examiner’s Guide, the answer is “no.” The credit union cannot close an account or even restrict services based solely on a SAR filing:

“Since a credit union member has a fundamental right to maintain a share account and participate in elections, the credit union cannot deny someone credit union membership because it has identified suspicious activity. However, the credit union may wish to consider limiting access to certain services. To do so, the credit union must have established written
policies and have notified its members of the policies in advance. The credit union should not consider the mere filing of a SAR as the basis for limiting services.

Similarly, the credit union may find it necessary to consider reassigning or terminating the services of an employee who is the subject of a SAR. The credit union should seek advice from counsel in these situations.

The credit union may not, by law, notify any person involved in an activity being reported on a SAR that the credit union has reported the activity, or that it has filed a SAR. However, this prohibition does not preclude a disclosure in an appropriate manner of the facts that serve as the basis of the SAR, so long as the disclosure is not made in a way that indicates or implies that the credit union has filed a SAR, or that the SAR includes that information."

Office of Foreign Assets Control

The Office of Foreign Assets Control (OFAC) is a division of the U.S. Treasury Department that administers and enforces economic and trade sanctions under a number of federal statutes against targeted foreign countries and their agents, terrorism sponsoring agencies and organizations, and international narcotics traffickers based on U.S. foreign policy and national security objectives. Credit unions are required to block property and payment of any funds transfers or transactions involving any country, entity or individual appearing on OFAC’s “Specially Designated Nationals and Blocked Persons” list (or “SDN List”). All of the bank regulatory agencies and the National Credit Union Administration cooperate to ensure financial institution compliance with the OFAC regulations.

In addition to OFAC’s Specially Designated Nationals List, credit unions are responsible for responding to 314(a) information requests under the USA Patriot Act’s amendments to the BSA. Section 326 of the USA Patriot Act also requires credit unions to check “a 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 function regulators.” However, the list has not yet materialized. Lastly, there are a number of other “Watch Lists,” such as the Federal Bureau of Investigation’s “Most Wanted Terrorists List” and the Financial Action Task Force List that some institutions choose to monitor because of their high risk location, business line or customer base.

OFAC Compliance Program

Although not required by specific regulation, NCUA and the state regulators will expect a credit union to establish and maintain an effective, written OFAC compliance program that is commensurate with the institution’s OFAC “risk profile.” Much like the credit union’s BSA compliance program, the credit union’s OFAC program should:

- Identify high-risk areas (e.g., wires, cross-border ACH transactions);
- Provide for appropriate internal controls for screening and reporting;
- Establish independent testing (audit) for compliance;
- Designate an employee (or employees) as responsible for OFAC compliance; and
- Create training programs for appropriate personnel in all relevant areas of the credit union.

The credit union’s policies, procedures, and processes for reviewing transactions and transaction parties should reflect the institution’s OFAC risk assessment. When conducting a risk assessment, the credit union must take into consideration the institution’s products, services, membership base, transactions, and geographic location. OFAC sanctions can reach into virtually all areas of a credit union’s operations. Therefore, the credit union should consider all types of transactions and transaction parties when conducting its risk assessment (see “Covered Transactions”). Lastly, the credit union’s risk assessment should take into account the resources (staff, technology, etc.) it has available to implement its OFAC compliance program. -See the FFIEC BSA/AML Examination Manual for a discussion of what examiners look for when evaluating a credit union’s OFAC compliance program.
Specially Designated Nationals and Blocked Persons List

As mentioned above, OFAC administers a number of U.S. economic sanctions and embargoes that target geographic regions and governments (such as Cuba, Iran, North Korea), as well as other programs that target individuals or entities (such as narcotics traffickers, named terrorists, terrorist organizations). In addition to targeted countries, OFAC publishes a list of “Specially Designated Nationals and Blocked Persons” ("SDN List") that includes hundreds of names of targeted entities and individuals.

A number of the named individuals and entities are known to move from country to country and may turn up anywhere in the world. All “U.S. persons” are prohibited from dealing with SDNs wherever they are located and must block (“freeze”) all SDN assets. The OFAC SDN List is updated regularly, and is available on the OFAC Web site. Since OFAC’s programs change frequently, it is very important that credit unions check the OFAC website on a regular basis to ensure that they have the most current SDN list.

Other OFAC Lists

OFAC maintains other sanctions lists in addition to the SDN List. They include:

- Sectoral Sanctions Identifications (“SSI”) List
- Foreign Sanctions Evaders (“FSE”) List
- Non-SDN Palestinian Legislative Council List
- Non SDN Iranian Sanctions List
- List of Foreign Financial Institutions Subject to Part 561 (the "Part 561 List")
- List of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 (the 13599 List)

In October of 2014, OFAC began including all of its non-SDN sanctions in a consolidated set of data files called the “Consolidated Sanctions List.” The Consolidated Sanctions List is not part of OFAC’s SDN List, however, some of these files may also appear on the SDN List. Credit unions are responsible for checking the SDN List and non-SDN lists like the FSE and SSI List – the consolidated list helps to streamline this process for institutions and OFAC screening vendors.

Speaking of OFAC screening, there are several vendors that offer “interdiction software” which automates the process of sifting through all of the names on the OFAC list. The software contains every name on the SDN and other OFAC lists and screens for “hits” with each transaction. Using interdiction software doesn’t completely protect the credit union from liability for compliance violations. However, should a violation occur, OFAC will “favorably consider a [credit union’s] business decision to use interdict software as well as other good faith manual and electronic compliance efforts in determining mitigation.” (Source: Office of Foreign Assets Control Regulations for the Financial Community)
“Blocking” Assets & Rejecting Transactions

OFAC regulations require credit unions to block property and payment of any funds transfers or transactions involving any country, entity or individual appearing on OFAC’s SDN List. Blocking is just another word for freezing a target’s property.

When the credit union blocks a transaction, it accepts the funds and freezes them so that the individual or entity cannot obtain or recover possession of the funds. Once it has been determined that funds need to be blocked, they must be placed into an dividend or interest-bearing account on the credit union’s books from which only OFAC-authorized debits may be made.

Some OFAC-administered programs will require a credit union to reject the transaction altogether, rather accept and freeze funds. In these cases, the underlying transaction is prohibited, however there is no blockable interest involved so the transaction is simply rejected.

Both blocked and rejected transactions must be reported to OFAC within 10 business days of occurrence (see “Reporting Requirements”).

Covered Transactions

OFAC regulations are written quite broadly to cast a wide net over just about any transaction that might involve a Specially Designated National (SDN) or blocked person, or blocked country. Property subject to blocking includes “anything of value.” For example: money, checks, drafts, debts, obligations, notes, warehouse receipts, bills of sale, evidences of title, negotiable instruments, trade acceptance, contracts, and anything else real, personal, or mixed, tangible or intangible, “or interest or interests therein, present, future, or contingent.” Practically everything that credit unions do every day involves “property” within the meaning of the OFAC regulations. Likewise, “property interest” is defined as any interest whatsoever, direct or indirect.

Therefore, OFAC compliance impacts all types of transactions and account services, for example:

- Opening new accounts
- Wire transfers
- Automated Clearinghouse (ACH) transactions
- Electronic Fund Transfers (EFTs)
- Cashing or depositing share drafts/checks
- Purchase of money orders or cashiers’ checks
- Dispensing loan proceeds and accepting loan payments
- Safety deposit boxes
- Trust Accounts
Certain transactions are considered riskier than others and deserve careful scrutiny, including: cross-border ACH transactions, international wires, nonresident alien accounts, commercial letters of credit, transactional electronic banking, foreign correspondent accounts, and payable through accounts.

All the parties to the above transactions should be checked against OFAC’s SDN/Blocked Persons list for a possible match. This means scanning the names of:

- Primary members
- Joint account holders
- Co-signers
- Guarantors
- Collateral owners
- Beneficiaries
- Makers/payees of checks and share drafts
- Parties on the other end of a wire transfer
- Etc.

The initial OFAC screening of new members may be performed as part of the credit union’s CIP and CDD procedures. New accounts should be compared with the OFAC list prior to being opened or shortly thereafter. Remember that it is illegal to do business with an OFAC target. Therefore, the account opening process cannot be completed until the credit union conducts the OFAC screening.

As for other transaction parties, the FFIEC BSA/AML Examination Manual states that: “the extent to which the credit union includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, will depend on the credit union’s risk profile and available technology.” That being said, the credit union will violate OFAC regulations if one of these parties turns out to be an OFAC target and the credit union fails to block the transaction.

**When should you screen an account?**

OFAC suggests that accounts be screened at the following stages:

**Upon account opening:** prior to opening or allowing an account to be operated, an institution should screen account holders, beneficiaries, authorized signers, powers of attorney, and any other parties to the account against OFAC’s SDN List to ensure compliance with OFAC’s sanction programs.

**Upon updating information:** accounts should be screened when amending account holders, beneficiaries, authorized signers, or powers of attorney.
Periodic screening of existing accounts: upon SDN List updates for electronic records, and upon scheduled reviews of member files or due diligence documentation reviews for paper based records.

Distribution of funds: prior to distributing funds to beneficiaries upon the death of the primary account holder(s).

What about checking older records? Since many older records are paper-based, their screening should be addressed in the context of the institution’s risk assessment.

Screening ACH Transactions

All parties to an ACH transaction are subject to the requirements of OFAC. In 2006, OFAC clarified the application of its rules for domestic and cross-border ACH transactions. (FFIEC BSA/AML Examination Manual)

With respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying that the originator is not a blocked party and making a good faith effort to determine that the originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying that the receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC policies.

ODFIs are not responsible for un-batching transactions and ensuring that they do not process transactions in violation of OFAC’s regulations if they receive those transactions already batched from their members/customers. If the ODFI un-batches the transactions it received from its members/customers, then the ODFI is responsible for screening as though it had done the initial batching.

With respect to OFAC screening, these same obligations hold for cross-border ACH transactions. For outbound cross-border ACH transactions, however, the ODFI cannot rely on OFAC screening by the RDFI outside of the United States. In the case of inbound ACH transactions, the RDFI is responsible for compliance with OFAC requirements. Credit unions can expect additional guidance in the future as OFAC works with the financial services industry to provide more detailed information on cross-border ACH.

What to do when the credit union has a “hit” on the SDN List

So, what should the credit union do when it gets a “hit” or match on the OFAC SDN List? OFAC offers the following advice when calling its compliance hotline:

1. Is the “hit” or “match” against OFAC’s SDN list or targeted countries, or is it “hitting” for some other reason (i.e., various other lists maintained by the FBI, CIA, or other agencies), or can you not tell what the “hit” is? If it’s hitting against OFAC’s SDN list or targeted countries, continue to 2 below. If it’s hitting for some other reason, you should contact the “keeper” of whichever other list the match is hitting against, or call the
Financial Crimes Enforcement Network (FinCEN), 1-800-949-2732. If you are unsure whom to contact or can’t tell what the hit is, contact your interdiction software provider that told you there was a “hit.”

2. Now that you’ve established that the hit is against OFAC’s SDN list or targeted countries, you must evaluate the quality of the hit. Compare the name of your account holder/name in your transaction(s) with the name on the SDN list. Is the name in your transaction an individual while the name on the SDN list is a vessel, organization or company (or vice-versa)? If yes, you do not have a valid match.* If no, please continue to 3 below.

3. How much of the SDN’s name is matching against the name of your account holder/name in your transaction? Is just one of two or more names matching (i.e., just the last name)? If yes, you do not have a valid match.* If no, please continue to 4 below.

4. Compare the complete SDN entry with all of the information you have on the matching name of your account holder or person or entity involved a particular transaction. An SDN entry often will have, for example, a full name, address, nationality, passport, tax ID or Cedula number (personal ID number for some non-U.S. residents), place of birth, date of birth, former names and aliases. Are you missing a lot of this information for the name in your transaction? If yes, go back and get more information and then compare your complete information against the SDN entry. If no, please continue to 5 below.

5. Are there a number of similarities or exact matches? If yes, please call the hotline at 1-800-540-6322. If no, you do not have a valid match.

Adapted from “When should I call the OFAC Hotline?” available on the OFAC Website.

Licenses

Through a licensing process, OFAC may permit certain transactions that would otherwise be prohibited under its regulations. There are two types of licenses:

- **General licenses** authorize categories of transactions without the need for case-by-case authorization from OFAC. These licenses can be found on OFAC’s website and in the regulations for each sanctions program.

- **Specific licenses** are issued on a case-by-case basis. Any person having an interest in a transaction or proposed transaction (member or credit union on the member’s behalf) may file an application for a license authorizing the transaction.

Before processing a transaction, the credit union should verify that it conforms to the terms and conditions of the license; and retain a copy of the authorizing license for recordkeeping purposes.

Applications for the unblocking of funds transfers are available on the [OFAC web site](http://www.treasury.gov/).
Reporting Requirements

As previously mentioned, credit unions are required to block or "freeze" property and payment of any funds transfers or transactions involving blocked countries or individuals, and to report the "blocks" within 10 business days of occurrence.

Blocking reports must identify:

- The owner or account party;
- A description of the property;
- The property’s location;
- Any existing or new account number or similar reference necessary to identify the property, actual or estimated value;
- The date the transaction was blocked;
- A photocopy of the payment or transfer instructions;
- Documentation showing that the blocked funds have been deposited into a new or existing blocked account which is clearly identifying the interest of the individual or entity subject to blocking;
- The name and address of the credit union as the holder of the account; and
- The name and telephone number of a contact person at the credit union from whom compliance information can be obtained.

Reports are also required for rejected items. Reports on these items also must be filed within 10 business days and include:

- The name and address of the transferee financial institution;
- The date and amount of the transfer;
- A photocopy of the payment or transfer instructions received;
- The basis for rejection; and
- The name and telephone number of a contact person at the transferee financial institution from whom compliance information can be obtained.

Annual Report. In addition, all holders of blocked property are required to file a comprehensive annual report on blocked property held as of June 30 by September 30 each year. The report is filed using Form TDF 90-22.50, which is accessible on the OFAC Website.

Record Retention

All OFAC records must be retained for 5 years. For items that are rejected in accordance with OFAC regulations, credit unions must maintain records for five years from the date of the transaction. For blocked accounts, credit unions must maintain records for five years after the date that the account is unblocked. In addition, credit unions are required to maintain a full and accurate record of the blocked account for as long as the credit union is holding the blocked property.
Penalties for Violations

The fines for violations can be substantial. Depending on the program, criminal penalties can include fines ranging from $50,000 to $10,000,000 and imprisonment ranging from 10 to 30 years for willful violations. Depending on the program, civil penalties range from $11,000 to $1,000,000 for each violation.

Other Government Lists

“326” List

Section 326 of the USA Patriot Act also requires credit unions to check “a 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.” At the present time, nothing meets the definition of any such list.

The final CIP regulations stated that financial institutions would receive notification of the creation of any Section 326 list. None has been issued to date. Nevertheless, credit unions must have procedures in place for determining whether a member appears on any list of known or suspected terrorists or terrorist organizations. Credit unions must determine whether a member appears on the list “within a reasonable period of time” after the account is opened, or earlier if required by another federal law or regulation or by a federal directive issued in connection with the list. The credit union must also have procedures for when a member’s name is on the list.

If the 326 List is ever released, it must be issued by a federal government agency and designated as a “CIP list” by Treasury in consultation with the federal functional regulators. Credit unions do not have an affirmative duty to seek out all lists of known or suspected terrorists or terrorist organizations compiled by the federal government. Instead, credit unions will receive notification by way of separate guidance regarding these lists. However, as mentioned above, no guidance has been issued thus far.

Other “Watch Lists”

In addition to OFAC and FinCEN’s 314(a) lists, a number of “watch lists” are maintained by other government agencies, in the United States and abroad. For example:

- Interpol
- Federal Bureau of Investigation’s List of Most Wanted Terrorists
- Financial Action Task Force (FATF) List
- Politically Exposed Persons (PEP) List
- Non-Cooperative Countries and Territories (NCCT)
- Bank of England’s Consolidated List
- Canadian Consolidated List
Initially, there was confusion regarding Section 326 of the USA Patriot Act and checking all of these additional government lists. However, NCUA has made it clear that credit unions only need to check OFAC’s list and respond to FinCEN’s 314(a) requests for information. That is, until a Section 326 list is created.
Frequently Asked Questions on OFAC Compliance

Q: Is there a dollar limit on which transactions are subject to OFAC regulations?

A: No. There is no minimum or maximum amount subject to OFAC regulations. Any transaction with a SDN will violate these regulations.

How much interest does the credit union have to pay on blocked funds?

OFAC regulations require that funds earn interest at a commercially reasonable rate, i.e., at a rate currently offered to other depositors on deposits or instruments of comparable size and maturity.

Q: Can the credit union deduct service charges from the account?

A: Generally yes. In most cases, OFAC regulations contain provisions to allow a financial institution to debit blocked accounts for normal service charges, which are described in each set of program regulations. The charges must be in accordance with a published rate schedule for the type of account in which the funds are maintained. Credit unions should check with OFAC compliance staff before imposing charges since sanction program requirements vary.

Q: What should the credit union do if it has a blocked account that needs to be escheated to the state?

A: The credit union should discuss the matter with state authorities and with OFAC. The state may have a license to escheat blocked funds, pending OFAC approval of each transfer. The credit union should contact OFAC directly for instructions on how to proceed.

Q: Many credit unions contribute toward charities and other non-profits. To what extent does the credit union need to review the recipients of these gifts or the principals of the charities?

A: Although it’s highly unlikely that most charities that credit unions contribute to would be on the OFAC list, donations to charitable institutions must be handled as any other financial transaction. Credit unions must ensure that the donations are in compliance with OFAC sanctions programs as well.

Q: Are credit unions really required to check the maker and payee of every check or share draft that the credit union processes?

A: Since OFAC regulations require credit unions to check all parties to every transaction that flows through the credit union against the SDN List, credit unions are technically required to monitor all checks and share drafts for possible matches – including both the maker and payee of every check. Credit unions have often asked exactly how OFAC expected them to comply with this requirement with regard to share drafts.

OFAC offers some guidance on checks and share drafts in the FFIEC’s BSA/AML Examination Manual. According to the OFAC materials in the manual, a credit union will be exposed to liability for processing a check if it “knows or has reason to know” that a transaction party on a
check is an OFAC target, especially personally handled transactions in a high-risk area. For example, if the credit union knows or has a reason to know that a check transaction involves an OFAC-prohibited party or country, OFAC would expect timely identification and appropriate action.

Q: Is the credit union required to purchase “tracking software” in order to comply with OFAC regulations?

A: Credit unions are not required by regulation to purchase “tracking” or “interdiction” software (i.e., special software designed to interdict prohibited transactions). However, credit unions are required to check virtually every transaction that comes through against the OFAC list. Interdict software automates the process of sifting through all of the names on the OFAC list. The software contains every name on the SDN/Blocked Persons list and screens for “hits” with each transaction. Larger institutions will find it impossible to do this manually. Smaller institutions may be able to do so, but the question is, how efficiently can this task be accomplished manually?

Using interdiction software doesn’t completely protect the credit union from liability for compliance violations. However, should a violation occur, OFAC will “favorably consider a [credit union’s] business decision to use interdict software as well as other good faith manual and electronic compliance efforts in determining mitigation.” (Source: OFAC’s “Foreign Assets Control Regulations for the Financial Community”). In addition, use of the software helps generate an audit trail, which will be useful when the credit union conducts its annual audits. See next question.

Q: Does OFAC require credit unions to conduct annual audits?

A: OFAC’s “Foreign Assets Control Regulations for the Financial Community” states that “[a]n in-depth audit of each department in the [credit union] should probably be conducted at least once a year.” This language seems to indicate that the annual audit is a recommendation, rather than a requirement. Nevertheless, NCUA’s examiners will be checking to see if credit unions are performing annual OFAC audits. The audit may be conducted by the credit union’s internal audit staff or an outside auditor.

Q: Does the credit union need to file OFAC’s Annual Report of Blocked Property if it has had no “hits” on the SDN List in the last year?

A: OFAC requires all holders of blocked property to file a comprehensive annual report on blocked property held as of June 30th by September 30th each year. There is no need to file the report if the credit union has had no “hits” on the SDN List and is holding no blocked property. The report is filed using Form TDF 90-22.50.

Q: Are credit unions required to check beneficiaries against the OFAC list?

A: Property, as defined in OFAC’s regulations, includes most products that financial institutions offer their members and customers. Further, the definition of “interest” in OFAC’s regulations includes any interest whatsoever, direct, indirect, present, future, or contingent. Given these broad definitions, OFAC’s position is that an account beneficiary has a future and or contingent interest in funds in an account, and consistent with an institution’s risk profile, should be screened to ensure OFAC compliance. Beneficiaries should be screened upon account
opening, when amending beneficiaries, and prior to distributing funds upon the death of the primary account holder(s). They will also be screened as the credit union conducts periodic reviews subject to changes in OFAC's SDN List. See OFAC's “Frequently Asked Questions,” Q#95 on OFAC’s website.

Q: Must the credit union block the primary member’s account if only the payable-on-death (POD) beneficiary appears on the OFAC list?

A: Possibly - see previous Q&A. We have received different answers to this question over the years. So, be sure to confirm with OFAC. If this is the case, the credit union or member can apply for a specific license to allow the primary member to continue operating the account.

Q: Can the credit union accept loan payments from an OFAC target?

A: Technically speaking, a credit union is never allowed to conduct business with an OFAC target. However, OFAC staff have clarified that it is permissible to accept payment from an OFAC target and then block the account, i.e., freeze the payment. However, the credit union cannot apply the payment to the outstanding loan balance without first obtaining a license from OFAC authorizing the release of the funds.
314(a) and 314(b) Information Sharing

Information Sharing Requirements

Section 314(a) of the USA Patriot Act "encourages" the sharing of information between financial institutions and the federal government regarding individuals, entities, and organizations engaged in or suspected of engaging in terrorist acts or money laundering activities. Section 314(b) permits financial institutions to share information with one another in order to better identify and report to the federal government concerning activities that may involve money laundering or terrorist activities.

314(a) Requests: Information Sharing with Federal Law Enforcement Agencies

FinCEN receives information requests from federal law enforcement and upon review, posts subject lists through the Web-based 314(a) Secure Information Sharing System. Every two weeks (or more frequently if an emergency request is transmitted), the credit union's designated point(s) of contact will receive notification from FinCEN that there are new postings to FinCEN's secure Web site. The point of contact will be able to access the section 314(a) subject list and download the files for searching.

Credit unions are required to query their records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last 6 months. They have 2 weeks from the transmission date of the request to respond to 314(a) requests. Credit unions should report all positive matches via the Secure Information Sharing System (SISS). However, if the search does not uncover any matching of accounts or transactions, credit unions are instructed not to reply to the 314(a) request.

Unless noted otherwise in the instructions to a 314(a) request, credit unions are only required to conduct a one-time search of the following records, whether or not they are kept electronically (if not maintained in electronic form, the record need only be searched if it is required to be kept under federal law or regulation):

- Deposit account records (e.g., checking/share drafts, savings, and certificates of deposit) to determine whether a named subject is or was an accountholder;
- Funds transfer (wire) records maintained pursuant to 31 CFR 103.33 to determine whether a named subject was an originator/transmittor of a funds transfer for which you were the originator/transmittor's financial institution, or a beneficiary/recipient of a funds transfer for which you were the beneficiary/recipient's financial institution;
- Records of the sale of monetary instruments (e.g., cashier's checks, money orders, or traveler's checks) maintained pursuant to 31 CFR 103.29 to determine whether a named subject purchased a monetary instrument;
- Loan records to determine whether a named subject is or was a borrower;
- Trust department account records to determine whether a named subject matches the name in which an account is titled;
• Records of accounts to purchase, sell, lend, hold, or maintain custody of securities to
determine whether a named subject is or was an accountholder;
• Commodity futures, options, or other derivatives account records to determine whether a
named subject is or was an accountholder; and
• Safe deposit box records to determine whether a named subject maintains or maintained,
or has or had authorized access to, a safe deposit box, but only if such safe deposit box
records are searchable electronically.

Any record described above not maintained in electronic form need only be searched if it is
required to be kept under federal law or regulation.

Credit unions are not required to search the following:

• Checks processed through an account to determine whether a named subject was a
  payee of a check;
• Monetary instruments (e.g., cashier's checks, money orders, or traveler's checks) issued
  by the institution to determine whether a named subject was a payee of such an
  instrument;
• Signature cards to determine whether a named subject is a signatory to an account
  (unless such a search is the only method to confirm whether a named subject maintains
  an account, as described above); and
• Reports (e.g., CTRs and SARs) that the institution previously filed with FinCEN.

**Take No Further Action**

Unless noted otherwise in a 314(a) request, the credit union is not required by the request to
close any account or take any other action with respect to an account or a transaction by virtue
of a match with any named subject.

The credit union should also not maintain the attached list of named subjects for the purpose of
evaluating whether to open an account or to conduct a transaction, unless the 314(a) request
clearly states that the subject list should be treated as a government list for purposes of section
326 of the USA Patriot Act.

Section 314(a) lists are not official U.S. designations such as the OFAC SDN List, but are
names of persons under investigation. Therefore, FinCEN strongly encourages financial
institutions not to maintain a 314(a) list for the purposes of determining whether to open an
account or conduct a transaction, except where the instructions to a 314(a) request state
otherwise.
Requests Must Remain Confidential

Credit unions must maintain adequate procedures to protect the security and confidentiality of information contained in requests from FinCEN. If credit unions apply the same procedures used to meet the privacy requirements under the Gramm-Leach Bliley Act, they will meet the safeguarding requirements of this rule. Credit unions cannot use an information request for any purpose other than to report matching information to FinCEN, to determine whether to establish or maintain an account, or to engage in a transaction, or to help the credit union comply with any part of the Bank Secrecy Regulations (Part 103).

Credit unions are prohibited from disclosing the fact that FinCEN has requested or obtained information under the rule, except to the extent necessary to comply with the request. Credit unions may share a list of suspects included on an information request with a commercial contractor to help the credit union comply with the request. However, the credit union must take necessary steps such as including confidentiality and nondisclosure requirements in its contract to safeguard the confidentiality of the information shared.

Compliance with the Right to Financial Privacy Act

The information reported under 314(a) is “information required to be reported under Federal law or rule,” which is permitted under section 3413(d) of the Right to Financial Privacy Act.

A financial institution that submits a positive 314(a) response to FinCEN concerning a subject may receive a Grand Jury subpoena, a National Security Letter (a request from the FBI or other government authority for a matter relating to terrorism) or an Administrative Summons (similar to an administrative subpoena). The federal law enforcement agency seeking information related to a 314(a) request must provide FinCEN with a written certification that each individual, entity, or organization about which the agency is seeking information is engaged in, or reasonably suspected based on credible evidence, of engaging in, money laundering or terrorist activity.

The certification must also have enough specific identifying information, such as date of birth, address, and social security number that would let the credit union differentiate between common or similar names. The certification must further identify an individual at the requesting law enforcement agency who will act as a point of contact concerning the request.

314(b) Voluntary Information Sharing Among Financial Institutions

Section 314(b) of the USA Patriot Act allows financial institutions or associations of financial institutions to share information with each other regarding individuals, entities, organizations, and countries for purposes of detecting, identifying, or reporting activities that the financial institution or association suspects may involve possible money laundering or terrorist activities. An “association of financial institutions” means a group or organization comprised of financial institutions defined above. Associations are included because they can enhance information-sharing among their members.
In order to participate in voluntary information sharing, credit unions must do the following:

- Provide an annual notice to FinCEN before information is shared. The annual notices may be submitted to FinCEN at [https://www.fincen.gov/314b/Register](https://www.fincen.gov/314b/Register).

- Before a credit union can share information, it must also verify that the other financial institution or association with which it wants to share information has also submitted the required notice.

- Maintain adequate procedures to protect the security and confidentiality of the information that is shared. If credit unions apply the same procedures used to meet the privacy requirements under the Gramm-Leach Bliley Act, they will meet the safeguarding requirements of this rule.

- File a Suspicious Activity Report if, as a result of information sharing, the credit union knows, suspects, or has reason to suspect that the individual, entity, or organization is involved in terrorist activity or money laundering.

- If a situation involves violations that require immediate attention, the credit union must immediately notify, by telephone, the appropriate law enforcement authority and NCUA or the credit union’s state supervisory authority may voluntarily report information to law enforcement concerning suspicious transactions relating to money laundering or terrorist activity that was discovered as a result of this information-sharing.

Shared information must only be used for identifying and reporting on activities that may involve terrorist or money laundering activities, determining whether to close or maintain an account, to engage in a transaction or assist the credit union with complying with this rule. Credit unions will not be liable to any person under any law or regulation for this type of information sharing, or for any failure to provide notice of this sharing.
Frequently Asked Questions on Information Sharing

Q: What is the difference between the 314(a) process and the OFAC requirements?

A: The 314(a) process and the OFAC requirements are separate and distinct. Credit unions not required to close, block or freeze any account or terminate any relationship simply because a name appears on a 314(a) request. If, however, that name also appears on the OFAC List, the credit union must comply with the OFAC regulations with respect to that individual or entity.

Q: How quickly must a credit union respond to a 314(a) request?

A: Credit unions must begin searching their records immediately upon receiving a 314(a) request. If the request comes in during non-business hours or during the weekend, the credit union must begin the search the next business day. If the credit union finds a match with a named subject, the match must be reported to FinCEN. Unless the instructions to a request state otherwise, the credit union must complete the search on all the subjects listed in the 314(a) request and respond with any matches no later than fourteen calendar days after receiving the request.

Q: What should a credit union do if it finds a match to a named subject?

A: The credit union should stop its search on that subject; the credit union is not required to search its records further for other matches with that subject unless and until it has been contacted by the requesting federal law enforcement agency for additional information.

If the 314(a) request contains multiple subjects, the credit union must continue to search its records for an account or transaction matching any of the other named subjects. After it has completed its search on all the subjects listed in the 314(a) request, the credit union must report any match to FinCEN by completing the Subject Information Form (one form per request).

If the search does not uncover any matching account or transaction, the credit union should not reply to the 314(a) request.

Q: How should the credit union report a match?

A: The Subject Information Form containing any positive matches must be sent to FinCEN via the Secure Information Sharing System (SISS). No details should be provided to FinCEN other than the fact that the credit union has a match. A negative response is not required.

Q: How close a match must a name be to a name on the 314(a) request in order to be considered a positive response or hit?

A: If information relating to an account or a transaction matches only one portion of a name on the attached subject list, such as last name only, and none of the additional information provided on the subject corresponds to the account or transaction in question, an institution need not report this as a positive response.
Q: Is a financial institution required to file a SAR if it identifies any accounts or transactions involving a 314(a) subject?

A: No, a 314(a) match does not trigger a SAR filing.

Q: Does the credit union have any special recordkeeping requirements concerning 314(a) requests?

A: While there are no specific recordkeeping requirements concerning 314(a) requests, appropriate documentation of the request and record search should be maintained for a reasonable time period to provide for an effective audit and examination trail.

Q: Can the credit union provide the 314(a) list to a vendor to perform searches?

A: According to the FFIEC BSA-AML Exam Manual, a financial institution may provide the 314(a) subject lists to a third-party service provider or vendor to perform or facilitate record searches as long as the institution takes the necessary steps, through the use of an agreement or procedures, to ensure that the third party safeguards and maintains the confidentiality of the information.

Q: What happens if the credit union failed to perform the required searches? Can we perform them retroactively?

A: If a credit union fails to perform or complete searches on one or more information request(s) received during the previous 12 months, it must immediately obtain these prior requests from FinCEN and perform a retroactive search of its records.

The credit union is not required to perform retroactive searches for requests that were transmitted more than 12 months before the date the credit union discovered its failure to perform or complete searches on prior information requests.

Additionally, in performing retroactive searches a financial institution is not required to search records created after the date of the original information request.
Responding to Requests from Law Enforcement

The SAR instructions advise credit unions not to include any supporting documentation with the suspicious activity report. Instead, the credit union must identify and retain a copy of the SAR and all original supporting documentation for five years from the date of the SAR filing. Supporting documentation may include spreadsheets, photocopies of cancelled checks or other documents, surveillance photos, transaction records, periodic statements, wire transfers, etc. All supporting documentation must be made available to appropriate authorities upon request.

Occasionally, after a credit union has submitted a suspicious activity report, a government agency may contact the credit union requesting supporting documents or additional information concerning the member or the member’s transactions or further information regarding the suspicious activity. It is at this point that the credit union must determine whether it can simply supply the requested information or whether it must request that the Federal agency comply with the Right to Financial Privacy Act.

Responding to a Request from a United States Government Agency

Within the Scope of the SAR

If a federal agency requests additional information or documentation related to a SAR, the credit union must first determine whether the information falls within or outside of the scope of the SAR. If the information or documentation is within the scope of the SAR, then the credit union must comply with the request and turn over the information to the government agency. FinCEN guidance FIN-2007-G003.

Beyond the Scope of the SAR

If the credit union determines that the requested information or documentation is outside the scope of the SAR, the credit union must request that the government agency comply with the Right to Financial Privacy Act by submitting either a member authorization, an administrative subpoena or summons, a search warrant, a judicial subpoena, or a formal written request. Regardless of the type of request provided, it should specifically identify the financial records, documentation, or information required. In many instances, the request may be worded very broadly.

Responding to a Request from a State or Local Law Enforcement Agency

Some state and local law enforcement agencies receive copies of SARs and/or have access to FinCEN’s database. If a state or local law enforcement agency requests additional information related to a SAR filing that is beyond the scope of the SAR, the law enforcement agency should submit a subpoena or search warrant to obtain the requested information. State and local law enforcement agencies are not subject to the federal RFPA, however, they would likely be subject to any state privacy laws. Credit unions should consult their state league for information on any applicable state privacy statute.
Responding to a Law Enforcement Request to Maintain Accounts

In June 2007, FinCEN issued guidance on how credit unions should handle law enforcement requests to maintain certain accounts. FinCEN acknowledged that in some instances, law enforcement agencies may have “an interest in ensuring certain account relationships remain open, despite suspicious or potential criminal activity in connection with the account.” Maintaining such accounts could be of assistance to law enforcement agencies investigating possible money laundering and terrorist financing crimes. However, it should be noted that the decision of whether or not to maintain such accounts is entirely up to the credit union. Credit unions that receive these requests should use measured decision-making—weighing the pros, cons, and risks involved in such requests.

Credit unions that decide to comply with a law enforcement agency’s request to maintain an account should be sure to do the following: (i) get the request in writing, (ii) make sure the request is issued by a supervisory agent or an attorney representing the federal, state, or local law enforcement agency, (iii) limit the duration of the request to no more than six months, and (iv) maintain documentation of such requests for at least five years after the requests have expired.

The most important thing to note is that complying with such law enforcement requests would not relieve a credit union of its recordkeeping and reporting responsibilities under the Bank Secrecy Act. For example, a credit union that opts to maintain an account at law enforcement’s request that reflects suspicious activity would still be expected to complete and file suspicious activity reports on the account.

Responding to a Civil Subpoena that Asks for the Production of a SAR

Federal law prohibits financial institutions that are subpoenaed or otherwise requested to produce a SAR from providing the SAR in discovery (i.e., the process of gathering information in preparation for a trial). The law even prohibits providing information that would disclose whether a SAR has been prepared or filed. In addition, a credit union must notify FinCEN along with its response to such request.

In addition to contacting a competent attorney, a credit union that receives a subpoena or request to produce a SAR should get in touch with FinCEN as soon as possible. FinCEN will often assist a financial institution that is contesting the issuance of such a subpoena by filing an amicus brief with the court in support of the credit union’s position that the SAR information is confidential and cannot be disclosed.

Nevertheless, documentation or financial records supporting a SAR are subject to discovery. Business records made in the ordinary course of business, such as periodic statements, account documents such as signature cards, wire transfers, transaction records or reports, checks, deposit slips, etc. are subject to discovery because they are prepared regardless of whether a financial institution has an obligation to report suspicious activity to the federal government.
If the subpoena does not specifically ask for the production of a SAR, but appears to be worded broadly enough that the SAR would be included, the credit union’s attorney should object to the subpoena on the grounds that some of its responsive material consists of confidential supervisory information. If the subpoena specifically asks for the production of a SAR, the credit union’s attorney should send the issuer of the subpoena a written objection referring to the Treasury regulations that specifically state that all SARs are confidential and cannot be released.

Right to Financial Privacy Act Requirements

Obviously, a credit union should already have policies and procedures in place to deal with the receipt of any subpoena, summons, National Security Letter or other request for information under the Right to Financial Privacy Act. The following is a review of the requirements for release of financial records or information to government agencies pursuant to the Right to Financial Privacy Act.

The RFPA prohibits any federal agency or department from obtaining the financial records of a financial institution’s member without prior member consent, except where access is authorized by one of the express exceptions to the Act or is accomplished through one of the access mechanisms mandated by the Act, including administrative subpoenas or summons, search warrants, judicial subpoenas, formal written requests or National Security Letters.

Member Authorizations

A member may authorize the credit union to release certain financial records to a specific government agency if he or she furnishes to both the credit union and the government agency a signed statement that:

- Authorizes the disclosure of the financial records for a period of time not exceeding 90 days;
- States that the member may revoke the authorization at any time before the financial records are actually disclosed or provided to the government agency;
- Identifies the financial records to be disclosed;
- Specifies the purposes for which the records may be disclosed and indicates the specific government agency the records are to be provided to; and
- States the member’s rights under the Right to Financial Privacy Act.

A credit union must maintain a record of all instances in which the member’s financial records are disclosed to a government agency under Section 3404 of the RFPA, including the identity of the agency. The member that authorized such disclosure has the right to obtain a copy of this record.

Administrative Subpoenas and Summons

An administrative subpoena or summons (in the context of the RFPA) is defined as a demand issued by a federal agency that compels document production or witness testimony.
A government agency may obtain financial records protected by the RFPA pursuant to an administrative subpoena or summons only if:

- There is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry; and
- A copy of the subpoena or summons has been served upon the member or mailed to his or her last known address on or before the date on which the subpoena or summons was served on the credit union together with a notice stating with reasonable specificity the nature of the law enforcement inquiry.

This means that a credit union should provide only those records that are actually requested by the subpoena or summons. Providing financial records that are not requested or required by the subpoena or summons may subject the credit union to liability for violating a member’s privacy rights.

Section 3405 of the RFPA requires the federal agency to provide notice to the member and gives sample language for the notice. The member has ten days after the receipt of the notice, or fourteen days after the notice was mailed to the member, to challenge the government’s access to his or her records by filing a sworn statement and motion to quash in the appropriate U.S. District Court.

**Search Warrants**

A government agency may obtain a member’s financial records pursuant to a search warrant obtained under the Federal Rules of Criminal Procedure. When providing records pursuant to a search warrant a credit union must be certain that it provides only those records requested. Within the 90 days after the government agency serves the search warrant on the financial institution, the agency must mail to the member’s last known address a copy of the search warrant along with the following notice:

“Records or information concerning your transactions held by the financial institution named in the attached search warrant were obtained by this (agency or department) on (date) for the following purpose:_______. You may have rights under the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 et seq.].”

If requested by the government agency, a court may grant a delay in the mailing of the notice up to 180 days from the service of the search warrant and may grant additional delays of up to 90 days. Upon expiration of the period of delay, the government agency must mail the following notice to the member along with a copy of the search warrant:

“Records or information concerning your transactions held by the financial institution named in the attached search warrant were obtained by this (agency or department) on (date). Notification was delayed beyond the statutory ninety-day delay period pursuant to a determination by the court that such notice would seriously jeopardize an investigation concerning________. You may have rights under the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 et seq.].”
Judicial Subpoenas

A government agency may obtain a member’s financial records pursuant to a judicial subpoena only if:

- The subpoena is authorized by law and there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry; and
- A copy of the subpoena has been served upon the member or mailed to his last known address on or before the date on which the subpoena was served on the credit union together with a notice stating with reasonable specificity the nature of the law enforcement inquiry.

Section 3407 requires the federal agency to provide notice to the member and provides specific language to be used in the notice. The member has ten days after receipt of the notice or fourteen days after the notice was mailed, to challenge the government’s access to the records by filing a sworn statement and motion to quash in the court that issued the subpoena.

Formal Written Requests

A government agency may obtain a member’s financial records pursuant to a formal written request only if:

- No administrative summons or subpoena appears to be available to the government agency in order to request a member’s financial records;
- The request is authorized by regulations issued by the head of the agency or department;
- There is reason to believe that the financial records sought are relevant to a legitimate law enforcement inquiry; and
- A copy of the request has been served upon the member or mailed to his last known address on or before the date on which the request was made to the financial institution together with a notice stating with reasonable specificity the nature of the law enforcement inquiry.

Section 3408 requires the federal agency to provide notice to the member and provides specific language for use in the notice. The member has ten days after receipt of the notice or fourteen days after the notice was mailed, to challenge the government’s access to the records by filing a sworn statement and motion in the appropriate U.S. District Court to enjoin the government agency from obtaining the requested financial records pursuant to the formal written request.

National Security Letters

National Security Letters (NSL) are basically administrative subpoenas issued by the FBI to demand information in connection with terrorism investigations that can be used to obtain several types of records. The authority for the FBI to issue NSLs predated the USA Patriot Act and 9/11. However, the Patriot Act enhanced the government’s authority to issue NSLs including the use of the letters to obtain member information from credit unions and other financial institutions.
Section 3414(a)(5) of the RFPA, permits the FBI to issue NSLs to obtain financial records from credit unions, banks, other financial institutions and other parties. Pursuant to the Electronic Communications Privacy Act (ECPA), the FBI can issue NSLs for telephone subscriber information, for local and long distance telephone billing records and electronic communication records; and under the Fair Credit Reporting Act (FCRA), NSLs can be issued to obtain consumer identifying information and the identity of financial institutions from credit bureaus.

NSLs must be hand delivered and contain a statement warning the financial institution that no officer, employee or agent of the institution may disclose to any party that the FBI has sought or obtained access to the requested information or financial records.

The requirements under Section 3414 are significantly different from other sections of the RFPA with respect to certification and member notification. For example, except where the member has authorized the disclosure himself, the sections of the RFPA relating to administrative subpoenas or summons, judicial subpoenas, and formal written requests require the government agency to provide a copy of the appropriate order or request to the member prior to providing it to the financial institution.

The requirements for search warrants are somewhat different, although the member must still receive a copy (within 90 days after service upon the financial institution). However, NSLs contain a gag provision that prevents anyone at the credit union including any officer, employee or agent of the credit union from disclosing to any party, including the member, that the FBI has sought or obtained access to the requested information or financial records.

Ordinarily, for administrative subpoenas, judicial subpoenas, formal written requests, and search warrants under the RFPA, the credit union would only release a member’s financial records after the government agency certifies in writing that it has complied with the applicable provisions of the RFPA. However, under Section 3414, for NSLs, the FBI will generally provide two certifications in writing: (1) that the records are required for foreign counter intelligence purposes to protect against international terrorism; and (2) that the FBI has complied with all applicable provisions of the RFPA. In fact, both certifications for NSLs are included in the NSL itself. The NSL letter and certifications must be signed by an FBI employee with the rank of Special Agent in Charge of a field division or an employee with a higher rank such as Deputy Director or Assistant Director.

The FBI’s internal procedures state that NSLs must be hand delivered and the institution is required to provide the financial records personally to a representative of the FBI field division that delivered the NSL. Records obtained pursuant to an NSL should never be returned to the FBI by mail or fax.
Federal Grand Jury Subpoenas

Financial records about a member obtained from a credit union pursuant to a subpoena issued under the authority of a Federal grand jury:

- Shall be returned and presented to the grand jury unless the volume of records makes the presentment impractical in which case the grand jury shall be provided with a description of the contents of the records.
- Shall be used only for the purpose of considering whether to issue an indictment by the grand jury, or of prosecuting a crime for which the indictment is issued, or for other purposes consistent with the Federal Rules of Criminal Procedure.
- Shall be destroyed or returned to the credit union if not used for the purposes specified.
- Shall not be maintained other than in the sealed records of the grand jury, unless the records has been used in the prosecution of a crime for which the grand jury issued an indictment.

No officer, director, or employee of the credit union shall notify any person named in a grand jury subpoena about the existence or contents of the subpoena, or that information has been furnished to the grand jury in response to the subpoena.

Certifications

Upon receipt of a request for financial records from a government agency and regardless of the method for requesting such records including a member authorization, administrative subpoena or summons, search warrant, judicial subpoena, formal written request or National security Letter, the credit union shall assemble the requested records and must be prepared to deliver the records to the government agency upon receipt of the Certification of Compliance required under Section 3403 (b) of the RFPA. However, no written Certification of Compliance is required for a subpoena or court order issued regarding a grand jury proceeding. Even though the credit union has already compiled the requested records it shall not release or submit the financial records until the government agency has actually provided the written Certification of Compliance to the credit union.

Exceptions

There are a number of specific situations where a Government agency does not have to comply with the Certification and Notification requirements. These are listed below:

- When the disclosure is in accordance with procedures authorized by the Internal Revenue Code.

- When the request for disclosure is not identified with a particular member. This also includes records or information that are not identifiable as being derived from the financial records of a particular member.
• When the request for disclosure is pursuant to exercise of supervisory, regulatory, or monetary functions with respect to financial institutions.

• When the request for disclosure is sought under the Federal Rules of Civil or Criminal Procedure or comparable rules of other courts in connection with litigation to which the government authority and the member are parties.

• When the request is pursuant to lawful proceeding or investigation directed at a financial institution or legal entity.

• When a member applies for participation in a government loan, loan guaranty, or loan insurance program, the government authority administering such a program shall give the member written notice of the authority's access rights under this subsection. No further notification shall be required for subsequent access by that authority during the term of the loan, loan guaranty, or loan insurance agreement.

• When it is necessary for the government to use or transfer financial records to process, service or foreclose a loan, or to collect on an indebtedness to the government resulting from a customer's default.

• When the credit union discloses what is necessary for the proper administration of programs regarding the withholding of taxes on nonresident aliens, Federal Old-Age Survivors, Disability Insurance Benefits, and Railroad Retirement Act Benefits.

• When the request is pursuant to the authority of the Federal Reserve System, or the Federal Housing Finance Board to extend credit to the financial institutions or others.

• When the request is necessary for the administration of certain veteran benefits laws.

• When the request is pursuant to an administrative subpoena issued by an administrative law judge in an adjudicatory proceeding.

• When the request is pursuant to legitimate law enforcement inquiry and is seeking only the name, address, account number and type of account of any member.

• When the request is issued by a subpoena or court order in connection with proceedings before a grand jury.

• When records are sought by the General Accounting Office pursuant to an authorized proceeding, investigation, examination or audit directed at a government authority.

• When a credit union or supervisory agency provides any record of any officer, director, or employee to the Attorney General, a state law enforcement agency, or Secretary of the
Responding to Requests from Law Enforcement

- Treasury if there is reason to believe there were crimes against the credit union by the insider.
- When the examination by or disclosure to the Resolution Trust Corporation or its employees or agents of financial records or information in the exercise of its conservatorship, receivership, or liquidation functions with respect to a financial institution.
- When the request is pursuant to Federal statute or rule.

What a financial institution should expect after submitting a 314(a) response to FinCEN

A financial institution that submits a positive 314(a) response to FinCEN concerning a subject will likely receive a Grand Jury subpoena. In certain cases, however, the financial institution may receive a National Security Letter (a request from the FBI or other government authority for a matter relating to terrorism, see 12 U.S.C. 3414(a)(1)(C)) or an Administrative Summons (similar to an administrative subpoena, see 12 U.S.C. 3405).

In the case of an Administrative Summons, individuals must be afforded notice and an opportunity to challenge, and the institution must obtain a certification of compliance with the Right to Financial Privacy Act, 12 U.S.C. 3401 et seq., from the law enforcement agency that issued the summons, before the institution may disclose a customer's records using this procedure. See 12 U.S.C. 3403(b) and 3405.

The timing of the law enforcement response will vary on a case-by-case basis. As noted on the response form, the 314(a) response should provide specific instructions as to whom and where at the credit union any follow-up from law enforcement should be addressed. The credit union should also provide a contact name and number of the individual employee at the credit union in charge of the 314(a) research.
Money Services Businesses (MSBs)

The Bank Secrecy Act (BSA) applies not only to depository financial institutions, such as credit unions and banks, but other financial services providers referred to as “money service businesses”, or MSBs.

MSBs include five distinct types of financial services providers, as well as the U.S. Postal Service:

1. Currency dealers or exchangers;
2. Check cashers;
3. Issuers or sellers of traveler’s checks or money orders;
4. Providers of prepaid access; and
5. Money transmitters.

Threshold Requirements: To be considered an MSB, the first three categories (currency dealer or exchanger, check cashers, issuers and sellers of traveler’s checks and money orders) must engage in such transactions in an amount greater than $1,000 for any person on any day in one or more transactions. (31 CFR 103.11(uu)).

A credit union is not considered an MSB. Although a credit union may, for example, exchange currencies or sell money orders, it is still not considered an MSB for purposes of the BSA.

Some credit unions accept MSBs as business accounts, while others offer some MSB services through a CUSO – either way, such credit unions should become familiar with the BSA requirements for money services businesses.

NCUA has warned credit unions that without proper controls, MSBs may generate transaction volume that could overwhelm a credit union and cover up illegal activities. NCUA field staff have been directed to closely scrutinize credit unions’ relationship with MSBs to ensure that credit unions are in compliance with all BSA requirements.

NOTE: The BSA does not require credit unions to serve as the de facto regulator of any MSBs with which they have a relationship. While credit unions are required to manage risk associated with all accounts, including MSB accounts, credit unions will not be held responsible for the MSB’s Bank Secrecy Act/Anti-Money Laundering program.

CREDIT UNION’S MSB ACCOUNTS – DUE DILIGENCE

Like with any other account, credit unions are expected to apply their risk-based BSA standards to money services business accounts. All MSBs must, at a minimum, be prepared to provide the credit union with:

1. basic identifying information,
2. state licensing documentation, if appropriate,
(3) its FinCEN registration, and
(4) any other information the credit union requires to make an adequate risk assessment.

As with any other account, if the MSB cannot provide this necessary information and there is no reasonable explanation as to why it cannot provide the information, the credit union must file a suspicious activity report (SAR). (For more information go to SARs chapter)

**MSB Registration**

Most businesses that meet the definition of an MSB are required to register with FinCEN. A person that is an MSB solely because that person serves as an agent of another MSB is not required to register. But an MSB that engages in activities requiring registration on its own behalf must register even if it is also engaging in activities as an agent of others. Registration must be renewed every two calendar years.

MSBs not required to register include:
- The U.S. Postal Service;
- Agencies of the U.S., of any state, or of any political subdivision of a state;
- A person that is an MSB solely because that person serves as an agent of another MSB or a branch office of an MSB.

*Note: In 1999, FinCEN deferred the registration requirements for prepaid access cards but a 2011 final rule added this requirement. The Prepaid Access Final Rule was issued in the summer of 2011, and FinCEN issued guidance in the form of FAQs to assist providers and sellers of prepaid access.*

**Due Diligence Expectations**

Effective May 11, 2018, credit unions will be required to identity and verify the beneficial owners of their “legal entity” accounts, including MSB accounts.

In April 2005, the federal agencies, including NCUA, issued guidance that sets forth the minimum steps that banking organizations, such as credit unions, should take when providing financial services to MSBs. Additionally, this guidance provides assistance to credit unions in assessing and minimizing the risk of money laundering posed by individual money services business members. FinCEN and the Federal Banking Agencies expect financial institutions that open and maintain accounts for money services businesses to apply the requirements of the Bank Secrecy Act on a risk-assessed basis, as they do with all accountholders.

As with any category of accountholder, there will be MSBs that pose little risk of money laundering and those that pose a significant risk. It is essential that credit unions neither define nor treat all MSBs as posing the same level of risk. For example, a local grocer that also cashes payroll checks for customers purchasing groceries will not present the same level of risk as a money transmitter specializing in cross-border wire transfers to jurisdictions posing heightened risk for money laundering.
Minimum Expectations

Based on existing Bank Secrecy Act requirements applicable to credit unions, the minimum due diligence expectations associated with opening and maintaining accounts for money services businesses are:

- Apply the credit union’s Customer Identification Program (CIP);
- Confirm FinCEN registration, if required;
- Confirm compliance with state or local licensing requirements, if applicable;
- Confirm agent status, if applicable; and
- Conduct a basic Bank Secrecy Act/Anti-Money Laundering risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.

Basic Risk Assessment

While the extent to which credit unions should perform further due diligence beyond the minimum compliance obligations listed above will be dictated by the level of risk posed by the individual MSB member. Not all money services businesses will require further due diligence.

Accordingly, as with any business account, in determining how much, if any, further due diligence will be required for any MSB member, the credit union should consider the following basic information:

**Types of products and services offered by the money services business:** In order to properly assess risks, credit unions should know the categories of money services engaged in by the particular MSB accountholder. In addition, credit unions should determine whether the MSB is a “principal” (with a fleet of agents) or is itself an agent of another MSB. Other relevant considerations include whether or not the money services business is a new or established operation, and whether or not money services are the MSB member’s primary or ancillary business (such as a grocery store that derives a small fraction of its overall revenue from cashing checks).

**Location(s) and market(s) served by the money services business:** Money laundering risks within a money services business can vary widely depending on the locations, customer bases, and markets served by the MSB. Relevant considerations include whether markets served are domestic or international, or whether services are targeted to local residents or broad markets. For example, a convenience store that only cashes payroll checks generally presents lower money laundering risks than a check casher that cashes any type of third-party check or cashes checks for commercial enterprises (which generally involve larger amounts).

**Anticipated account activity:** Credit unions should determine the expected services that the MSB will use, such as currency deposits or withdrawals, check deposits, or funds transfers. For example, an MSB may operate out of one location and use one branch of the credit union, or
may have several agents making deposits at multiple branches throughout the credit union's network. Credit unions should also have a sense of expected transaction amounts.

**Purpose of the account:** Credit unions should understand the purpose of the account for the money services business. For example, a money transmitter might require the credit union account to remit funds to its principal U.S. clearing account or may use the account to remit funds cross-border to foreign-based agents.

**Risk Indicators**

To further assist credit unions in determining the level of risk posed by a money services business member, the federal agencies have provided examples of what may be indicative of lower and higher risk. In determining the level of risk, a credit union should not take any single indicator as determinative of the existence of lower or higher risk. An effective risk assessment should be a composite of multiple factors, and depending upon the circumstances, certain factors may be weighed more heavily than others.

Examples of potentially **lower risk** indicators:

The money services business –

- primarily markets to customers that conduct routine transactions with moderate frequency in low amounts;
- offers only a single line of money services business product (for example, only check cashing or only currency exchanges);
- is a check casher that does not accept out of state checks;
- is a check casher that does not accept third-party checks or only cashes payroll or government checks;
- is an established business with an operating history;
- only provides services such as check cashing to local residents;
- is a money transmitter that only remits funds to domestic entities; or
- only facilitates domestic bill payments.

Examples of potentially **higher risk** indicators:

The money services business –

- allows customers to conduct higher-amount transactions with moderate to high frequency;
- offers multiple types of money services products;
- is a check casher that cashes any third-party check or cashes checks for commercial businesses;
is a money transmitter that offers only, or specializes in, cross-border transactions, particularly to jurisdictions posing heightened risk for money laundering or the financing of terrorism or to countries identified as having weak anti-money laundering controls;

is a currency dealer or exchanger for currencies of jurisdictions posing heightened risk for money laundering or the financing of terrorism or countries identified as having weak anti-money laundering controls;

is a new business without an established operating history; or is located in an area designated as a High Risk Money Laundering and Related Financial Crimes Area or a High-Intensity Drug Trafficking Area.

FinCEN added the following as examples of higher-risk indicators in 2008 guidance:

- The MSB has not performed a risk assessment.
- The MSB does not have an AML program or has not implemented the AML program.
- The AML program does not define the duties of the MSB’s personnel.
- The AML program has not been modified to identify specific risks at agent level.
- The AML program in place does not address all financial services that the entity provides.
- An independent review has not been conducted, or the MSB has not implemented the recommendations from the independent review.
- The MSB does not provide continuous BSA/AML training to appropriate personnel.
- The author of the compliance program, policies, procedures and training also conducts the independent review for the MSB.
- The MSB does not have written procedures for the separation of duties.
- The same staff conducting the financial transactions prepares, reviews, and files required BSA reports
- The MSB does not document its oversight duties and decisions.
- Employees can override input fields with invalid or illogical data entries when completing customer transactions.
- Electronic data is not secure. No plans are in place for emergency data restoration.
- The MSB has special rates for different types of transactions or special customers that are not available to the general public.
- Transactional limits are not in place. For example, the use of multiple money orders/traveler’s checks to purchase product or service is typical.
- Transactional limitations do not meet customer needs, yet affected customers continue to use the MSB services.
- Transactions limitations do not meet customer needs, yet affected customers continue to use the MSB services.
• Transactions limitations enforced by 3rd party, but no provision at retail level to prevent multiple transactions that could circumvent the limitations.
• Frequent employee turnover.
• MSB relies solely on paper documents.

• MSB relies solely on automated reporting systems. Frontline employees do not initiate SARs.
• New employees can conduct transactions of any amount before they receive BSA/AML training.
• MSB receives the currency needed to provide the financial service from sources other than its bank.
• No transaction limitations, or no system lock-out when processing transactions greater than the established limit.
• No organized recordkeeping system is used.
• The MSB does not separate the financial and bookkeeping activities of the MSB from his/her other business.
• The management of the MSB is unaware of the BSA, sound business practices (such as cash flow management) and accounting controls and procedures.
• MSB does not charge check cashing fees.
• The customer base is volatile in terms of few repeat customers; transaction volume is unpredictable, and subject to large swings between time period. For example, customers are self-employed.
• The MSB provides check cashing services to businesses that require large amounts of currency.
• The value of individual transactions as well as total volume are not within expected range for customer base.
• Customers transmit funds to countries that have poor money laundering oversight and controls.
• The MSB has more than one Agent relationship.
• The Principal does not monitor the day-to-day activities of its agents, provide up-to-date BSA/AML training, or perform internal reviews of its agents.
• The MSB is located in a HIFCA and/or HIDTA area.
• The MSB derives significant business from customers outside the community.
• The MSB is located in owner’s personal residence or area that is not accessible to the public.
• Entity with multiple locations, uses an AML program and procedures that do not consider the risks of all locations.
Customers generally pay for funds transmittal and/or purchase money orders/traveler's checks with currency or with proceeds from business checks or other monetary instruments.

One or more product or service that is needed by the MSB's customer base is not offered.

Products purchased by customers are shipped overseas.

Transactions are not done face-to-face.

Due Diligence for Higher Risk Members

A credit union’s due diligence should be commensurate with the level of risk of the money services business member identified through its risk assessment. If a credit union’s risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, it will be expected to conduct further due diligence in a manner commensurate with the heightened risk. This is no different from requirements applicable to any other business account member and does not mean that a credit union cannot maintain the account.

Depending on the level of perceived risk, and the size and sophistication of the particular money services business, credit unions may pursue some or all of the following actions as part of an appropriate due diligence review. Likewise, if the credit union becomes aware of changes in the profile of the MSB member, these additional steps may be appropriate. However, it is not the expectation of FinCEN or NCUA that credit unions will uniformly require any or all of the actions identified below for all money services business members:

- review the money services business’s anti-money laundering program;
- review results of the money services business’s independent testing of its anti-money laundering program;
- conduct on-site visits;
- review list of agents, including locations, within or outside the United States, that will be receiving services directly or indirectly through the money services business account;
- review written procedures for the operation of the money services business;
- review written agent management and termination practices for the money services business; or
- review written employee screening practices for the money services business.

The extent to which a credit union should inquire about the existence and operation of the anti-money laundering program of a particular MSB will be dictated by the credit union’s assessment of the risks. Given the diversity of the MSB industry and the risks they face, credit unions should expect significant differences among anti-money laundering programs of money services.
businesses. However, FinCEN and NCUA do not expect banking organizations to act as the de facto regulators of the MSB industry.

**Suspicious Activity Reporting**

Existing regulations require credit unions to identify and report known or suspected violations of law and/or suspicious transactions relevant to possible violations of law or regulations. Risk-based monitoring of accounts maintained for all members, including money services businesses, is a key element of an effective system to identify and, where appropriate, report violations and suspicious transactions. The level and frequency of such monitoring will depend, among other things, on the risk assessment and the activity in the account.

Based on the credit union’s assessment of the risks of its particular MSB members, monitoring should include periodic confirmation that initial projections of account activity have remained reasonably consistent over time. Account activity would typically include deposits or withdrawals of currency, deposits of checks, or funds transfers. The mere existence of variances does not necessarily mean that a problem exists, but may be an indication that additional review is necessary. Furthermore, risk-based monitoring generally does not include “real-time” monitoring of all transactions flowing through the account of a MSB, such as a review of the payee or drawer of every deposited check.

**Foreign-Located Money Services Businesses**

In 2011, FinCEN amended the definition of “money services business” to include foreign-located entities that provide money services within the United States, even if none of its agents, agencies, branches, or offices are physically located in the U.S. [This rule, and its 2012 Advisory](https://www.fincen.gov/statutes-and-regulations), is a result of FinCEN’s recognition that the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the U.S. from foreign locations.
Examples of Suspicious Activity

Examples of potential suspicious activity within money services business accounts, generally involving significant unexplained variations in transaction size, nature, or frequency through the account, include:

- A check casher deposits checks from financial institutions in jurisdictions posing heightened risk for money laundering or the financing of terrorism or from countries identified as having weak anti-money laundering controls when the money services business does not overtly market to individuals related to the particular jurisdiction;

- A check casher deposits currency in small denomination bills or unusually large or frequent amounts. Given that a check casher would typically deposit checks and withdraw currency to meet its business needs, any recurring deposits of currency may be an indicator of suspicious activity;

- A check casher deposits checks with unusual symbols, stamps, or written annotations either on the face or on the back of the negotiable instruments;

- A money transmitter transfers funds to a different jurisdiction than expected, based on the due diligence information that the credit union had assessed for the particular money services business. For example, if the money transmitter represented to the credit union or in its business plan that it specializes in remittances to Latin America and starts transmitting funds on a regular basis to another part of the world, the unexplained change in business practices may be indicative of suspicious activity;

- A money transmitter or seller/issuer of money orders deposits currency significantly in excess of expected amounts, based on the due diligence information that the credit union had assessed for the particular MSB, without any justifiable explanation, such as an expansion of business activity, new locations, etc.

- A money service business has failed to register with FinCEN or failed to obtain a license under applicable state law. According to FinCEN, given the importance of the licensing and registration requirement, a credit union should file a suspicious activity report if it becomes aware that a member is operating in violation of the registration or state licensing requirement. This approach is consistent with long standing practices of FinCEN and the Federal Banking Agencies under which financial institutions file suspicious activity reports on known or suspected violations of law or regulation.

However, credit unions are not expected to terminate existing accounts of MSBs based solely on the discovery that the member is a money services business that has failed to comply with licensing and registration requirements (although continuing non-compliance by the money services business may be an indicator of heightened risk). There is no
requirement in the Bank Secrecy Act regulations that a financial institutions must close an account that is the subject of a suspicious activity report. The decision to maintain or close an account should be made by the credit union’s management under standards and guidelines approved by its board of directors. However, if an account is involved in a suspicious or potentially illegal transaction, the credit union should examine the status and history of the account thoroughly and should determine whether or not the credit union is comfortable maintaining the account. If the credit union is aware that the reported activity is under investigation, FinCEN strongly recommends that the credit union notify law enforcement before making any decision regarding the status of the account.

Voluntary Information Sharing

The USA PATRIOT Act of 2001 allows certain financial institutions, after providing notice to FinCEN, to voluntarily share information with each other for the purpose of identifying and, where appropriate, reporting possible money laundering or terrorist financing under protection of legal safe harbor.

Credit unions and MSBs can utilize this information sharing provision to work together to identify money laundering and terrorist financing. While participation in the information sharing program is voluntary, FinCEN and NCUA encourage credit unions and their money services business members to consider how voluntary information sharing could enable each institution to more effectively comply with its anti-money laundering and suspicious activity monitoring requirements.

MSB COMPLIANCE REQUIREMENTS

Most MSBs are subject to the full range of BSA regulatory requirements, including the anti-money laundering program rule, the suspicious activity and currency transaction reporting rules, and various other identification and recordkeeping rules. Certain MSBs are required to register with FinCEN and many states have established supervisory requirements, often including the requirement that an MSB be licensed with the state.

The BSA responsibilities for money services businesses are activity based, irrespective of what the business states is its main business activity. If the business performs certain specific activities in excess of certain monetary threshold, then the business is an MSB for BSA purposes.

MSBs can range from large sophisticated chains with interstate operation facilities that provide an assortment of financial services to small one-owner store front operations that provide a few financial services as an auxiliary service to its primary retail store operations. The business and management structure, as well as the overall risk profile, of an MSB can vary based on the size and complexity of the MSB. Some MSBs may engage in several different types of MSB-defined activities simultaneously. Some MSB-defined activities require more recordkeeping and reporting under the BSA than others.
Currency Dealers or Exchangers: A currency dealer or exchanger is defined as an MSB, subject to all applicable regulations. To be considered an MSB, must engage in such transactions in an amount greater than $1,000 for any person on any day in one or more transactions. (31 CFR 103.11(uu)).

Currency dealers or exchangers typically operate along international borders, in port-of-entry cities (where international flights land), or near communities of resident aliens. Some travel agencies will also operate as currency dealers or exchangers.

Check Cashers: Check cashing services may be offered by a retail business, for example, a grocery store, as an accommodation to its customers. A check casher may also be a stand-alone “brick and mortar” operation. To be considered an MSB, must engage in such transactions in an amount greater than $1,000 for any person on any day in one or more transactions. (31 CFR 103.11(uu)).

Issuance and Sale of Money Order/Travel’s Checks: An issuer of money orders or traveler’s checks is defined as an MSB, subject to all applicable regulations. To be considered an MSB, must engage in such transactions in an amount greater than $1,000 for any person on any day in one or more transactions. (31 CFR 103.11(uu)).

Money transmitter: A money transmitter is defined as:
- any person, whether or not licensed or required to be licensed,
  - that engages, as a business, in accepting currency or funds denominated in currency, and
  - transmits the currency or funds, or the value of the currency or funds, by any means through a financial agency or institutions, a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both, or
  - an electronic funds transfer network, or
- any person that is engaged as a business in the transfer of funds.

To provide customer access and convenience, large money transmitters may contract with agents, such as grocery stores, truck stops, check cashers, pharmacists, travel agents and supermarket chains. No threshold requirements apply.

Provider of Prepaid Access: A provider of prepaid access is the participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. A prepaid program is an arrangement under which one or more persons acting together provide(s) prepaid access.

The participants in each prepaid access program must determine a single participant within the prepaid program to serve as the provider of prepaid access. This person will have principal oversight and control over the program.

EXCEPTIONS:
(A) closed loop prepaid access to funds not to exceed $2,000 maximum value that can be associated with a prepaid access device or vehicle on any day;
(B) prepaid access solely to funds provided by Federal, State, local, Territory and Insular Possession, or Tribal government agency;
(C) prepaid access solely to funds from pre-tax flexible spending arrangements for health care and dependent care expenses or from Health Reimbursement Arrangements; or
(D) (1) prepaid access solely to (i) employment benefits, incentives, wages or salaries; or (ii) funds not to exceed $1,000 from which not more than $1,000 maximum value can be initially or subsequently loaded, used, or withdrawn on any day through a device or vehicle, and (2) it does not permit: (i) funds or value to be transmitted internationally; (ii) transfers between or among users of prepaid access within a prepaid program; or (iii) loading additional funds or the value of funds from non-depository sources.

MSB Anti-Money Laundering Program

MSBs are required to implement an effective anti-money laundering program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and terrorist financing. The anti-money laundering program must be written and must be commensurate with the MSB’s risk profile. Furthermore, the program must be fully implemented and reasonably designed to meet the BSA requirements. Policy statements alone are not sufficient; practices must coincide with the MSB’s written program.

The program must include:
- Policies, procedures, and internal controls designed to ensure ongoing compliance;
- Designation of individuals responsible for coordinating and monitoring day-to-day compliance;
- Training for appropriate personnel; and
- Independent review to adequately monitor the program.

Recordkeeping Requirements

All MSBs are required to keep records on extensions of credit over $10,000 and instructions regarding transfers over $10,000 into or out of the United States.

An MSB must maintain a record of the issuance or sale of a cashier’s check, money order, or traveler’s check for $3,000 or more in currency. Federal regulations do not require a specific format for these records.

An MSB must obtain and retain information relating to the transmittal of funds in the amount of $3,000 or more. For transmittals greater than $10,000 made with currency, a currency transaction report (CTR) is required as well. There is no aggregation rule for transmittals to reach the $3,000 limit requirement.

Currency dealers or exchangers are required to make and retain additional records as set forth in 431 CFR 103.37.
Record Retention

Generally, records must be retained for a period of five years from the date of the transaction.

Currency Transaction Reporting

An MSB must file a Currency Transaction Report (CTR) for each transaction in currency (deposit, withdrawal, exchange, or other payment or transfer) of more than $10,000 by, through, or to the MSB. A transaction that is a transfer of funds by means of bank check, funds transmittal, or other written order, and that does not include the physical transfer of currency, is not a transaction in currency for this purpose.
Suspicious Activity Reports

MSBs have different requirements for filing Suspicious Activity Reports (SARs), depending on the type of financial service provided to the public. For example, an MSB acting solely as a check cashing business is exempt from SAR-MSB requirements.

MSBs that provide money transmission or currency dealing or exchange – or businesses that issue, sell, or redeem money orders/traveler’s checks – must report suspicious activity involving any transaction or pattern of transactions at or above $2,000. MSBs may voluntarily file SAR-MSBs for amounts below the required reporting thresholds.

For issuers of money orders/traveler’s checks, to the extent that the identification of a suspicious transaction is derived from a review of clearance records or other similar records of money orders/traveler’s checks that have been sold or processed, the issuer is required to report a suspicious transaction or pattern of transaction that involves or aggregates funds or other assets of at least $5,000.
MONEY SERVICES BUSINESS ACCOUNTS CHECKLIST

1. Has the credit union collected, at least, all of the following information from each MSB account member?
   - Basic identifying information,
   - State licensing documentation, if appropriate
   - Its FinCEN registration, and
   - Any other information the credit union requires to make an adequate risk assessment.

2. For any MSB member that has not provided the necessary information, has the credit union filed a suspicious activity report?

3. Has the credit union completed, at a minimum, the following due diligence requirements?
   - The Customer Identification Program requirements,
   - Confirm FinCEN registration, if required;
   - Confirm compliance with state or local licensing requirements, if applicable;
   - Confirm agent status, if applicable, and
   - Conduct a basic BSA/AML risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.

4. When determining whether further due diligence is necessary, did the credit union take the following information into consideration?
   - Types of products and services offered by the MSB;
   - Location(s) and market(s) served by the MSB;
   - Anticipated account activity;
   - Purpose of the account.

5. Is the due diligence performed by the credit union commensurate with the determined level of risk?

6. Did the credit union perform enhanced due diligence for higher risk MSB accounts?

7. Has the credit union effectively monitored its MSB accounts for suspicious activity?
For credit unions servicing marijuana-related MSB accounts:

8. Has the credit union performed the additional 7 customer due diligence requirements included in FinCEN’s 2014 guidance?  

☐

9. Has the credit union met the requirements of the 8 priorities listed in FinCEN’s 2014 guidance?  

☐

10. Has the credit union filed the Marijuana Limited suspicious activity reports?  

☐

11. Has the credit union filed the Marijuana Priority and/ or Marijuana Termination reports, if required?  

☐
TEST YOUR KNOWLEDGE

Question 1:
True or False: Credit unions are considered money services businesses for purposes of the Bank Secrecy Act.

Question 2:
True or False: Credit unions must ensure that any MSB it is doing business with is in compliance with the Bank Secrecy Act and Anti-Money Laundering requirements.

Question 3:
True or False: Most MSBs must provide their FinCEN registration number to the credit union when opening an account.

Question 4:
True or False: If a credit union cashes checks for non-members it is considered an MSB for BSA purposes.

Question 5:
Which of the following are consider high-risk indicators for MSB accounts:

☐ primarily markets to customers that conduct routine transactions with moderate frequency in low amounts;

☐ is a money transmitter that offers only, or specializes in, cross-border transactions, particularly to jurisdictions posing heightened risk for money laundering or the financing of terrorism or to countries identified as having weak anti-money laundering controls;

☐ allows customers to conduct higher-amount transactions with moderate to high frequency

☐ is an established business with an operating history

☐ offers multiple types of money services products
Quiz Answers:

Answer 1:

False! This is not true. The Bank Secrecy Act specifically excludes banks from the definition of a "money services business" (31 CFR 103.11 (uu) and credit unions are specifically included in the definition of a "bank" (31 CFR 103.11 (c)(6)).

Answer 2:

False! The BSA does not require credit unions to serve as the de facto regulator of any MSBs with which they have a relationship. While credit unions are required to manage risk associated with all accounts, including MSB accounts, credit unions will not be held responsible for the MSB's Bank Secrecy Act/Anti-Money Laundering program.

Answer 3:

True! With some exceptions, MSBs must, at a minimum, be prepared to provide the credit union with:

1. basic identifying information,
2. state licensing documentation, if appropriate,
3. its FinCEN registration, and
4. any other information the credit union requires to make an adequate risk assessment.

Answer 4:

False! For the same reason noted in the Answer to Question 1. The Bank Secrecy Act specifically excludes banks from the definition of a "money services business" (31 CFR 103.11 (uu) and credit unions are specifically included in the definition of a "bank" (31 CFR 103.11 (c)(6)).

Answer 5:

✓ is a money transmitter that offers only, or specializes in, cross-border transactions, particularly to jurisdictions posing heightened risk for money laundering or the financing of terrorism or to countries identified as having weak anti-money laundering controls;

✓ allows customers to conduct higher-amount transactions with moderate to high frequency

✓ offers multiple types of money services products
BSA Recordkeeping Requirements

The BSA regulations require credit unions to maintain numerous records so that law enforcement can reconstruct transactions when necessary. The general retention period under the BSA is five years. OFAC also requires credit unions to maintain all reports of blockings or rejected items and related records for five years.

The specific BSA recordkeeping requirements include:

- Records to be made and retained by financial institutions;
- Additional records to be made and retained by banks; and
- Nature of records and retention period.

Credit unions must be able to provide access to BSA records upon an examiner or law enforcement official’s request within a reasonable period of time. At a minimum, credit unions must retain the records as original, microfilm, or other copy or reproduction, both front and back.

Credit unions must maintain the following records:

- Records filed pursuant to the BSA, i.e., SAR and CTR;
- Cash sales of monetary instruments (e.g., money orders, traveler’s checks, cashier’s checks) between $3,000 and $10,000;
- Member identification information and payment data related to the sender and the recipient of each incoming or outgoing wire transfer of $3,000 or more.
- Member identification information obtained to comply with the USA Patriot Act’s Customer Identification Program requirements for five (5) years after the account has been closed;
- A record of each loan that exceeds $10,000 (except those secured by real estate), which must contain the borrower’s name and address, the amount, purpose or nature, and date of the loan;
- A record of each advice, request, or instruction received or given regarding any transaction resulting in or intending to result in the transfer of currency and other monetary instruments, funds, checks, investment securities, or credit, of more than $10,000 to or from any person, account or place outside the United States;
- A record of any report required by the Department of Treasury’s special order concerning the transfer of United States coins or currency in a geographic area;
• Social security number or taxpayer identification number (TIN) for each share account and share certificate account;

• Either the original or a copy of each of the following:
  
  o The signature card granting signature authority over each share account, including the information used in verifying the signer’s identity, such as a driver’s license number;

  o Each statement, ledger card or other record for each share account, showing each transaction for that account;

  o Each check, clean draft, or money order drawn on the credit union, or issued and payable by the credit union unless the amount is less than $100, drawn on an account that averages at least 100 checks a month, and written for employee benefits or dividends.

  o Each item in excess of $100 comprising a debit to a member’s deposit account not otherwise exempted;

  o Each item, including checks, drafts, or transfers of credit, of more than $10,000 remitted or transferred to a person, account, or place outside the United States;

  o Each record of remittance or transfer of funds, currency, other monetary instruments, checks, investment securities, or credit, of more than $10,000 to a person, place, or account outside the United States;

  o Each check or draft in an amount in excess of $10,000 drawn on or issued by a foreign bank which the credit union has paid or presented to a non-bank drawee for payment;

  o Each item, including checks, drafts or transfers of credit, of more than $10,000 received directly and not through a domestic financial institution, by letter, wire, or any other means from a bank, broker, or dealer in foreign exchange outside the United States;

  o A record of each receipt of currency, other monetary instruments, investment securities or checks, and of each transfer of funds or credit, of more than $10,000 received on any one occasion directly from a bank, broker, or dealer in foreign exchange outside the United States;

  o Records prepared or received by the credit union in the ordinary course of business and needed to reconstruct a share draft account and to trace a check or share draft in excess of $100 deposited in such account through its processing
system or to supply a description of a deposited check or share draft in excess of $100 (this applies to demand deposits only);

- A record containing the name, address, and taxpayer identification number, if available, of any person presenting a certificate of deposit for payment, as well as a description of the instrument, and the date of the transaction; and

- Each deposit slip or credit ticket reflecting a transaction in excess of $100 or the equivalent record for direct deposit or other wire transfer deposit transactions. The slip or ticket shall record the amount of any currency involved.

There are no specific recordkeeping requirements concerning FinCEN’s 314(a) information requests. However, the credit union should maintain appropriate documentation of the request and record search for a reasonable time period to provide for an effective audit and examination trail.

Credit unions that participate in voluntary information sharing with other financial institutions should maintain a copy of their annual certification with the Treasury Department as evidence of compliance with the 314(b) requirements.

Sources:

* FFIEC BSA/AML Examination Manual, Appendix P: Record Retention Requirements

* NCUA Consumer Compliance Manual, Bank Secrecy Act Overview: Record Keeping

* NCUA Examiner’s Guide, Chapter 18 and Appendix 18A - Bank Secrecy Act: BSA Recordkeeping Requirements