NAFCU

2022

BSA

CERTIFICATION SCHOOL MANUAL

NCBSO | NAFCU CERTIFIED BANK SECRECY OFFICER

WELCOME TO THE NAFCU BSA SCHOOL CERTIFICATION MANUAL!

This comprehensive manual will provide you with the necessary information you'll need to certify as a NAFCU Bank Secrecy Officer. We are extremely glad you chose us for your certification needs. Should you have any questions, please do not hesitate to ask any NAFCU staff for assistance.

A special thank you goes to our sponsor whose contributions make these programs a success. Their continued support is greatly appreciated.

Always remember: we believe in you and your mission. That's why we provide the best federal advocacy, education and compliance assistance possible.

Thanks for all you do.
Sincerely,

B. Dan Berger
President & CEO

In tandem with the BSA School, NAFCU's 2022 BSA Certification School Manual is designed to help you prepare for the certification exam, consisting of 50 questions, to obtain your NAFCU Certified Bank Secrecy Officer (NCBSO) designation. You must receive a score of 76 percent (38/50) or higher on the exam to become NCBSO certified. Along with the school presentations, the manual will provide you with all the necessary information for the exam. It also includes sample questions to help in studying for the NCBSO certification exam.

The source material for the manual was synthesized from the Federal Financial Institutions Examination Council (FFIEC) *Bank Secrecy Act (BSA) /Anti-Money Laundering (AML) Examination Manual*. While the FFIEC manual provides guidance to examiners for carrying out BSA/AML and Office of Foreign Assets Control (OFAC) examinations, it also serves as an excellent resource for compliance with the BSA. NAFCU's 2022 BSA Certification School Manual also includes links to additional resources to assist you with future BSA compliance research.

Pricing. The cost of the NCBSO exam is $79 for NAFCU members and $119 for non-members. The exam may be purchased during the BSA School online registration process.

Notification of Results. You will be notified of your results once you finish the exam. New NCBSO's will receive a certificate via U.S. mail within the month following school.

Failed Exams and Retakes. If you do not pass the NCBSO exam during virtual school, you may still retake the exam as many times as needed before December 31, 2022.

Once you successfully pass the exam, you will become a NAFCU Certified Bank Secrecy Officer (NCBSO) with all rights to promote your designation. The certification marks and abbreviations related to the NCBSO are the property of NAFCU and we maintain the sole right to control the use of the brand.

NCBSOs must recertify every two years to maintain their certification. Recertification can be done by earning 19 continuing education units (CEUs) related to Bank Secrecy Act compliance content *OR* by retaking the certification exam.

As a new NCBSO, the accumulation period for recertification begins on January 1 of the year after you passed the exam. For example, if you passed your exam in February 2022, your accumulation period would be January 1, 2023, through December 31, 2024. Each time you recertify, your NCBSO designation is valid for another two-year period during which you would need to obtain 19 CEUs to maintain your NCBSO status.

NCBSOs can earn CEUs by completing one or more of the following:

- Attending NAFCU's Regulatory Compliance Seminar with BSA Track (24 CEUs);
- Attending NAFCU's BSA Compliance School (19 CEUs);
- Viewing NAFCU's BSA compliance webinars (1.0 CEUs for 1.0-hour webinars);
- Attending NCBSO-accredited BSA compliance sessions at other NAFCU conferences; and
- Attending other compliance-related training. Note: non-NAFCU Program CEUs may be accepted at a fee of $10 per 0.5 CEU earned. BSA-related trainings from CAMS, Verafin, CUNA and the Leagues are almost always accepted. A request for credit for Non-NAFCU Program CEUs can be submitted here.

To obtain CAMS credit, attendees will receive an attendance certificate containing the number of CAMS credits (19) via email the week after school. Attendees must provide the certificate to ACAMS, it will then add the credits to their profiles.

Additional information is available at NAFCU's NCBSO webpage. If you have a specific question that is not addressed here, please send an email to bsa@nafcu.org for assistance.

***

TABLE OF CONTENTS

THE ABC'S OF THE BANK SECRECY ACT

The Bank Secrecy Act (BSA) was originally passed by Congress in 1970. Under this law, U.S. financial institutions are required to keep records to assist law enforcement and regulatory agencies in the detection and prevention of money laundering. These records assist with investigations of criminal, tax and regulatory violations, and in some instances provide useful evidence in prosecuting money laundering and other financial crimes. The BSA is sometimes referred to as an anti-money laundering law (AML) or jointly as BSA/AML.

Enacted shortly after the September 11, 2001, terrorist attacks, Congress passed the USA PATRIOT Act of 2001. Among other things, the USA PATRIOT Act expanded the scope of the existing BSA framework to focus on terrorist financing in addition to money laundering.

Government Agencies and the BSA

BSA regulations and examination guidance are developed and implemented by the U.S. Department of the Treasury (Treasury), the Financial Crimes Enforcement Network (FinCEN) and the federal banking agencies including but not limited to the Board of Governors of the Federal Reserve System (Federal Reserve) and the National Credit Union Administration (NCUA). There are also various international government bodies that support the fight against money laundering and terrorist financing.

Treasury

Treasury has oversight of the BSA and has issued a number of implementing regulations, located under 31 CFR Chapter X. Under these regulations credit unions and other financial depository institutions are required to establish AML programs, file certain reports such as currency transaction reports (CTRs) and suspicious activity reports (SARs) and keep certain records of transactions. In recent years, some BSA provisions have been extended to cover not only traditional depository institutions, but also nonbank financial institutions, such as money services businesses, casinos, brokers/dealers in securities, futures commission merchants, mutual funds, insurance companies and operators of credit card systems.

FinCEN

A bureau of Treasury, FinCEN is the delegated administrator of the BSA. FinCEN issues regulations and interpretive guidance, provides outreach to regulated industries, supports the examination functions performed by federal banking agencies and pursues civil enforcement actions.

NCUA

As the credit union primary government regulator, NCUA is required by the BSA to examine credit unions for BSA compliance. The agency also has its own set of BSA regulations, which are located in Part 748 of the Code of Federal Regulations. NCUA has its own BSA resources page located here.

Money Laundering and Terrorist Financing

Money Laundering

Money laundering occurs when a criminal takes funds or "dirty" money, earned through illegal activities and attempts to "clean" them into what appear to be legitimate funds. Although it is often a complex process, generally there are three stages to "wash" the illegal funds:

- **Placement.** In the first stage, "dirty" money is put into the financial system or the retail economy. During this stage, the money is at its most vulnerable to detection and seizure. This can be accomplished in a variety of ways. Some common methods include: loan repayment with illegal proceeds; buying gambling chips or placing bets on sporting events; moving illegal currency or monetary instruments over the border; purchasing foreign money with illegal funds through foreign currency exchanges; and using a legitimate cash focused business to blend or co-mingle dirty funds with legitimate sales receipts.
- **Layering.** In the second stage, funds are moved through a series of transactions to confuse and complicate any paper trail, making it difficult to trace it back to its original source. An example of layering is moving funds through wire transfers from one country to another, which are then divided into different types of investments; these funds are constantly moved to avoid detection. With the high daily volume of wire transfers, it is difficult to trace these transactions.
- **Integration.** The final stage includes additional transactions to make it appear as though the funds are legal. Examples include the purchase of automobiles, businesses, real estate and other investments to give the funds an air of legitimacy.

Terrorist Financing

Funds used for terrorist financing can be raised from unlawful or legitimate sources such as a person's employment income and or by donations from people unaware of where or how the money is eventually used. Terrorist organizations may be disguised as charitable or non-profit organizations and may also receive funds from sympathetic government sponsors.

Although terrorist financing is motivated by ideology rather than making profits, money laundering methods used to fund terrorist operations can be the same as or very similar to methods used by other criminals laundering funds.

Penalties for Violations

News headlines have highlighted the large institutional fines imposed by FinCEN and other regulators for BSA violations. Under various statutes, credit unions and individual employees are also subject to criminal and civil liability for violations of AML and terrorist financing laws, and for structuring transactions to avoid filing BSA reports. These penalties can be severe. A recent trend in BSA enforcement is the increased risk of individual liability.

Criminal penalties can be assessed for willful BSA regulation violations. Any individual, including a credit union employee, found guilty of this is subject to criminal fines of up to $250,000 or five years in prison, or both. If the individual commits a willful BSA violation while breaking another law or committing other criminal activity, he or she is subject to a fine of up to $500,000, or ten years in prison, or both. Violations of certain BSA provisions or special measures can make a credit union subject to a criminal money penalty up to the greater of $1 million or twice the value of the transaction.

The federal banking agencies and FinCEN have the authority to bring civil money penalty actions for BSA violations. In addition to criminal and civil money penalty actions, individuals can be removed from working within the financial industry for violation of AML laws "as long as the violation was not inadvertent or unintentional." This type of BSA violation may also incur reputational risk.

BSA'S FIVE PILLARS

A credit union's BSA/AML compliance program must at a minimum meet these requirements and include:

- A system of internal controls to ensure ongoing compliance.
- Independent testing of BSA/AML compliance.
- A designated individual or individuals responsible for managing BSA compliance (BSA compliance officer).
- Training for appropriate personnel.
- Risk-based procedures for ongoing member/customer due diligence.

These are what are referred to in the industry as the "five pillars" of BSA/AML compliance. Customer due diligence (CDD) was added by a FinCEN final rule in 2016.

Internal Controls

Internal controls are policies, procedures and processes designed to limit and control risks and to achieve compliance with the BSA. A credit union's internal controls should be commensurate with its size, structure, risks and complexity. Internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive BSA/AML compliance program throughout the credit union.

In addition to ensuring ongoing compliance with BSA regulatory requirements, internal controls are meant to:

- Incorporate the credit union's BSA/AML risk assessment and the identification of illicit financial activity risks, along with any changes in those risks.
- Provide for program continuity despite changes in operations, management, employee composition or structure.
- Facilitate oversight of information technology sources, systems and processes that support BSA/AML compliance.
- Provide for timely updates in response to changes in regulations.
- Incorporate dual controls and the segregation of duties to the extent possible.
- Include mechanisms to identify and inform the board of directors and senior management of BSA compliance initiatives, identified compliance deficiencies and corrective action taken, and notify the board of directors of SARs filed.
- Identify and establish specific BSA compliance responsibilities for staff and provide appropriate oversight for the execution of those responsibilities.

The *BSA/AML Examination Manual* notes this is not an exhaustive list and a credit union would want to tailor internal controls to its risk profile.

Independent Testing

Independent testing should be conducted by the internal audit department, outside auditors, consultants or other qualified independent parties. If conducted by an internal audit department, testing should be conducted by someone qualified and not involved in

the function being tested. Testing should be done generally every 12 to 18 months, commensurate with a credit union's BSA/AML risk profile and to areas identified as being of greatest risk and concern.

Risk-based independent testing programs vary depending on a credit union's size or complexity, organizational structure, scope of activities, risk profile, quality of control functions, geographic diversity and use of technology. Testing should include evaluating pertinent internal controls and information technology sources, systems and processes used to support the BSA/AML compliance program. Consideration should also be given to the expansion into new product lines, services, customer types and geographic locations through organic growth or merger activity.

The independent testing is expected to evaluate the overall adequacy of the credit union's BSA/AML compliance program. Such an evaluation helps make the board of directors and senior management aware of weakness, or areas in need of enhancements or stronger controls. It typically will also include an explicit statement in the report(s) about the credit union's overall compliance with BSA regulatory requirements. At a minimum, the independent testing should contain sufficient information for the reviewer (e.g., board of directors, senior management, BSA compliance officer, review auditor, or an examiner) to surmise the overall adequacy of the credit union's BSA/AML compliance program.

It is expected for auditors to document the independent testing scope, procedures performed, transaction testing completed and any findings. All independent testing documentation and supporting workpapers should be available for examiner review. Violations; exceptions to policies, procedures or processes; or other deficiencies noted during the independent testing should be documented and reported to the board of directors or a designated board committee in a timely manner. The board of directors, or a designated board committee, and appropriate staff should track deficiencies and document progress of corrective actions.

BSA Compliance Officer

The credit union's BSA compliance officer is designated by its board. The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance and managing all aspects of the BSA/AML compliance program. This person should be fully knowledgeable of the BSA, all related regulations and the credit union's internal procedures.

In addition to ongoing BSA training, BSA compliance should be included in the job descriptions of credit union personnel. The line of communication within the credit union

should allow the BSA compliance officer to regularly inform the board of directors and senior management of ongoing BSA compliance. The BSA compliance officer is responsible for carrying out the direction of the board and ensuring that employees follow and maintain the credit union's BSA/AML compliance program.

The *BSA/AML Examination Manual* indicates it is critical that the individual responsible for overall BSA compliance have the appropriate authority, independence and access to resources within the credit union. Examples of this might include having input into BSA risks with any new products, services or operational changes and no undue influence from the business lines. Having the independent authority to identify and report any issues to the board of directors and senior management. Having adequate staffing with the skills and expertise and the systems necessary to support the timely identification, measurement, monitoring, reporting and management of the credit union's illicit financial activity risks.

Training

BSA/AML training must be given to the appropriate personnel and tailored to the employee's specific responsibilities. It should cover regulatory requirements and the credit union's internal policies, procedures and processes. Training should be ongoing and incorporate any development and changes to the BSA and related regulations.

While a credit union's board of directors may not require the same degree of training as its operations personnel, the board needs to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance and risks posed to the credit union. Without this general understanding, the board of directors cannot adequately provide oversight; approve policies, procedures, and processes; or provide sufficient resources.

Training should include changes to the credit union's internal policies, procedures and processes, and its products, services, customers, and geographic locations. Changes to information technology sources, systems, and processes used in BSA compliance may also be covered if appropriate. Examples of money laundering and suspicious activity monitoring and reporting tailored to each operational area should also be included. The training program may be used to reinforce the importance that the board of directors and senior management place on the credit union's compliance with the BSA and that all employees understand their role in maintaining an adequate BSA/AML compliance program.

Customer Due Diligence

The CDD rule requires a credit union to develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence. There are four key components to CDD or member due diligence. The first component is to identify and verify a member's identity. This is the Member/Customer Identification Program (CIP) requirement, which has been included within BSA's fifth CDD pillar. The second CDD component, is to identify and verify the identity of beneficial owners of legal entities, therefore extending CIP requirements to both individual members and beneficial owners of legal entities. Although understanding the nature and purpose of member relationships and ongoing monitoring, the third and fourth components, were already supervisory expectations, they are now regulatory requirements of the BSA/AML compliance program.

BSA/AML COMPLIANCE PROGRAM/RISK ASSESSMENT

NCUA examiners expect a credit union to apply the same risk management principals used in its traditional operations in assessing and managing its BSA/AML risk. Identifying and understanding its risk profile allows a credit union to apply appropriate risk management processes to the BSA/AML compliance program. This process enables management to better identify and mitigate gaps in the credit union's controls. A risk assessment should provide a comprehensive, concise and organized analysis of the BSA/AML risks and should be shared and communicated with all business lines across the credit union, board of directors, management and appropriate staff. It is also considered a sound practice to have a written risk assessment. As part of any risk assessment, a credit union should perform due diligence and evaluate its field-of-membership before introducing any new product or service.

Identification of Specific Risk Categories

An initial step of the risk assessment process is to identify the specific products, services, customers, entities and geographic locations unique to the credit union.

Products and Services

Certain products and services offered by credit unions may pose a higher risk of money laundering or terrorist financing. Depending on the nature of the specific product or service offered, they may provide a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents.

Members/Customers and Entities

Although any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation or anticipated transaction activity, certain members and entities may pose specific risks. In assessing member risk, credit unions should consider other variables, such as services sought and geographic locations, e.g., whether the credit union is located in a high-risk money laundering and related financial crimes area or high intensity drug trafficking area.

Geographic Locations

Credit unions are expected to understand and evaluate the specific risks associated with doing business in, opening accounts for members from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a member's or transaction's risk level and higher-risk geographic locations, e.g., high intensity drug trafficking areas, can be either international or domestic.

Analysis of Specific Risk Categories

The second step of the risk assessment process involves a more detailed analysis of information obtained during the identification stage. This involves evaluating data pertaining to the credit union's activities in relation to the Member/CIP and CDD information. The analysis of the data pertaining to the credit union's activities would likely consider, as appropriate, the following factors:

- Purpose of the account.
- Actual or anticipated activity in the account.
- Nature of the member's business/occupation.
- The member's location.
- Types of products and services used by the member.

Developing the BSA/AML Compliance Program Based Upon the Risk Assessment

Examiners expect a credit union's management to structure its BSA/AML compliance program to adequately address the credit union's risk profile, as identified by the risk assessment. Management should understand the BSA/AML risk exposure and develop the appropriate policies, procedures and processes to monitor and control these risks.

Updating the Risk Assessment

An effective risk assessment is an ongoing process and updated to identify any changes to the credit union's risk profile. Even in the absence of such changes, it is considered sound practice to periodically reassess BSA/AML risks at least every 12 to 18 months as new products and/or services are added by the credit union.

MEMBER/CUSTOMER IDENTIFICATION PROGRAM

Section 326 of the USA PATRIOT Act requires a credit union to implement a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements. It must include account opening procedures that specify what identifying information is collected as well as reasonable and practical risk-based procedures for verifying the identity of each member.

The CIP rule defines an "account" as a formal banking relationship such as a deposit account, a transaction or asset account, a credit account, or another extension of credit. It also includes a relationship established to provide a safe deposit box or other safekeeping services or to provide cash management, custodian or trust services. Under the CIP rule, an account would not include providing products or services such as check cashing, funds transfer, or the sale of a check or money order as this generally does not involve a formal banking relationship.

The CIP rule applies to a "customer" (or for credit unions, member, however customer is used in the rule and is the industry-wide term), which is defined as a "person" (an individual, a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a **new** account, an individual who opens a new account for another individual who lacks legal capacity, or an individual who opens a new account for an entity that is not a legal person (e.g., a civic club). A person who does not receive banking services, such as a person whose loan application is denied is not a customer. Under this definition, it also does not include an existing customer as long as the credit union has a reasonable belief that it knows the customer's true identity. Once a customer's identity is established, the credit union does not need to form a reasonable belief again for every other account they may open. Also excluded from this definition of customer are federally regulated banks, banks regulated by a state bank regulator, governmental entities, and publicly traded companies.

Required Information to be Collected at Account Opening

At a minimum, the *BSA/AML Examination Manual* indicates the credit union must collect this identifying information from each customer before opening the account:

- Name.
- Date of birth for individuals.
- Address (although not specified in the regulation, guidance has indicated this should be a physical address, not a mailing address).
- Identification number such as a taxpayer identification number (TIN).

Based on its risk assessment, a credit union may require additional identifying information for certain customers or product lines.

Verifying a Member's Identity

A credit union's procedures will include what documentary and nondocumentary methods it will use to verify the member's identity.

Using Documentary Methods

If using documents to verify a member's identity, the credit union would need procedures for what is acceptable documentation. The CIP rule reflects the federal banking agencies' expectations that such documentation may include an unexpired government-issued form of identification that provides evidence of a member's nationality or residence and bear a photograph or similar safeguard, such as a driver's license or passport.

For a "person" other than an individual (such as a corporation, partnership or trust), the credit union should collect documents showing the legal existence of the entity, such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement or a trust instrument.

Verification Through Nondocumentary Methods

If using nondocumentary methods to verify a member's identity, the credit union's CIP procedures would need to describe how it does so. Nondocumentary methods may include contacting a customer; independently verifying the customer's identity by comparing information they have provided with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement.

Nondocumentary procedures must also address when an individual is unable to present an unexpired government-issued identification document with a photograph or similar safeguard; unfamiliar documents are presented; the account is opened without collecting documents; the account is opened without the member appearing in person at the credit union; or under any circumstances that increase the risk the credit union will be unable to verify the true identity of a member through documents.

Additional Verification for Certain Members

The *BSA/AML Examination Manual* states that the CIP must address situations where a new account is opened by a member that is not an individual and the credit union cannot verify

the member's identity through either documentary or nondocumentary methods. In this case, the credit union will collect information about individuals with authority or control over new accounts, including signatories, to verify the member's identity.

Lack of Verification

The CIP should include procedures for when the credit union cannot form a reasonable belief that it knows the identity of the member.

Recordkeeping and Retention Requirements

As outlined in the FFIEC BSA/AML Examination Manual, the CIP must include recordkeeping procedures. The identifying information (name, address, date of birth for an individual, TIN, and any other information required by the CIP) collected at account opening must be kept for a period of five years after the account is closed. For credit cards, the retention period is five years after the account closes or becomes dormant. A description of the following documents must be kept for five years after the record was made:

- Documents used to verify identity, noting the type of document, identification number, where it was issued, and, if any, the date it was issued and expiration.
- The method used to verify identity and the results.
- Any discrepancy discovered when verifying identity.

Adequate Member Notice

A credit union's CIP will include procedures to give the member adequate notice that it is requesting information to verify their identities. The notice should outline the credit union's identification requirements and be provided in a way that allows the member to view or to receive the notice prior to opening an account. Examples include posting the notice in the lobby, on a website or within loan application documents. The regulation gives sample language:

> *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.*

Internal Controls of CIP

During an examination, a credit union's CIP internal controls (policies, procedures, and processes) will be assessed to determine whether these controls are designed to mitigate and manage illicit financial activity risks. Internal controls should be designed to assure ongoing compliance with CIP requirements and be commensurate with a credit union's size or complexity and organizational structure.

MEMBER/CUSTOMER DUE DILIGENCE

A credit union's policies, procedures and processes enable it to understand the nature and purpose of its members' relationships and potential transactions.

Establishment of Risk-Based Policies, Procedures and Processes in Relation to a Credit Union's BSA/AML Risk Profile

CDD policies, procedures, and processes are critical to:

- Detecting and reporting unusual or suspicious activity that potentially exposes the credit union to financial loss, increased expenses or other risks.
- Avoiding criminal exposure from persons who use or attempt to use the credit union's products and services for illicit purposes.
- Adhering to safe and sound banking practices.

Understanding the Nature and Purpose of the Member Relationship in Order to Develop a Risk Profile

CDD allows a credit union to understand the nature and purpose of member relationships and potential transactions in order to develop a risk profile. The member risk profile or risk rating helps a credit union to understand the money laundering and terrorist financing risks of its members. In developing the risk profile, the credit union should take into consideration products and services; members and entities; and geographic locations.

Use of Risk-Based Procedures to Maintain and Update Member Information

The requirement for ongoing monitoring of the member relationship reflects existing practices established to identify and report suspicious transactions and, on a risk basis, to maintain and update member information. As outlined in the *BSA/AML Examination Manual* credit union's CDD procedures must outline its ability to:

- Establish and verify a member's identity.
- Establish and verify beneficial owners who ultimately own or control any legal entity members.
- Understand the nature and purpose of member relationships.
- Perform ongoing monitoring to report suspicious transactions and update member information on a risk basis.

Note that while member information collected under CDD requirements includes beneficial ownership information for legal entity customers, this is governed by the requirements outlined in the beneficial ownership rule.

Conduct Ongoing Monitoring

The credit union must have the appropriate risk-based procedures in place to conduct ongoing due diligence. The requirement to update member information is event driven. The credit union's procedures should establish the criteria for when and by whom member relationships will be reviewed, including the updating of information and reassessment of the member's risk profile.

Higher Risk Profile Members and Enhanced Due Diligence

Members that pose higher money laundering or terrorist financing risks present increased risk exposure. A credit union's due diligence policies, procedures and processes should define both when and what additional information will be collected about members that pose heightened risk. This is referred to as enhanced due diligence (EDD). Even within categories of members with a higher risk profile, there can be a spectrum of risks and the extent to which additional ongoing due diligence measures are necessary may vary on a case-by-case basis. Based on the risk profile, a credit union may consider obtaining, at account opening (and throughout the relationship), more information to understand the nature and purpose of the relationship, such as:

- Source of funds and wealth.
- Occupation or type of business (of the member or others with ownership or control over the account).
- Financial statements for business members.
- Location where the business member is organized and principal place of business.
- Proximity of the member's residence, place of employment or place of business to the credit union.

- Description of the business member's primary trade area, whether transactions are expected to be domestic or international, and the expected volumes of such transactions.
- Description of the business operations, such as total sales, the volume of currency transactions, and information about major customers and suppliers.

Performing an appropriate level of ongoing due diligence that is commensurate with the member's risk profile is especially critical in understanding the member's transactions.

BENEFICIAL OWNERSHIP REQUIREMENTS FOR LEGAL ENTITY MEMBER/CUSTOMERS

A credit union is required to have written procedures that are reasonably designed to identify and verify any natural person that has control or is the beneficial owner(s) a of legal entity.

What is a Legal Entity?

A legal entity is defined as a corporation, limited liability company or other entity that is created by the filing of a public document with a Secretary of State or other similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account. The rule excludes a number of entities from this definition under 31 CFR 1010.230(e)(2).

What is a Beneficial Owner?

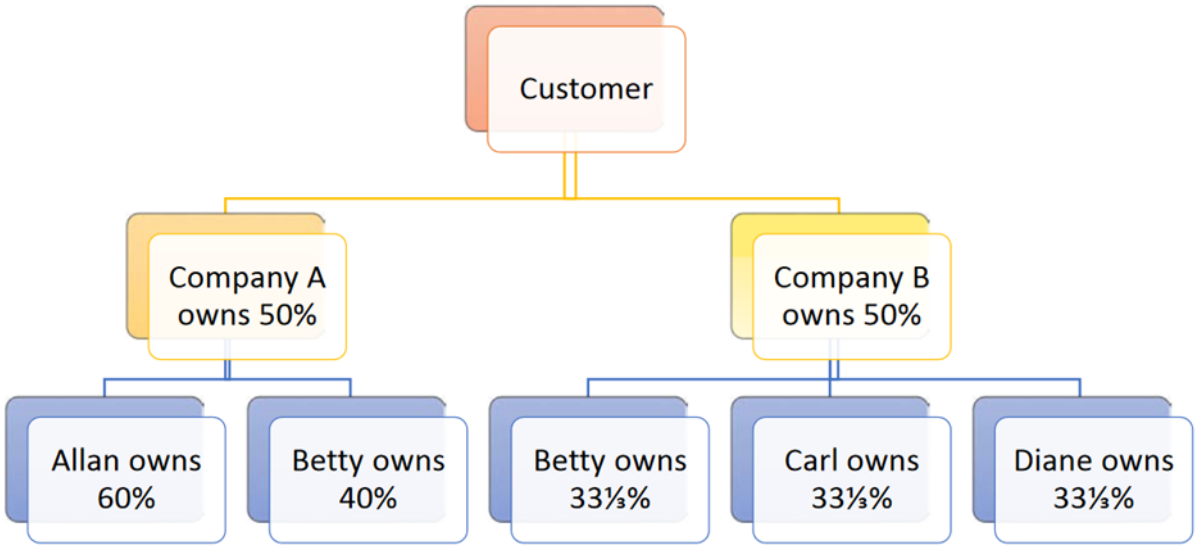
Beneficial ownership interests are determined by the amount of control and ownership an individual has over the legal entity. The rule refers to these as "prongs." All legal entity members will have a total of between one and five beneficial owner(s) with at least one individual under the control prong and zero to four individuals under the ownership prong.

Control – Where a single person has a significant responsibility to control, manage or direct a legal entity such as an executive officer or senior manager. This would include chief executive officer, chief financial officer, chief operating officer or president. One beneficial owner must be identified as having control of each legal entity.

Ownership – When a person(s) either directly or indirectly owns 25 percent or more of the equity interests of a legal entity member through any contract, arrangement, understanding, relationship or other means. If a trust owns, directly or indirectly, 25 percent or more of the equity interests of a legal entity, the beneficial owner is the trustee.

FinCEN has provided an example and chart illustrating direct and indirect beneficial ownership:

"…. Allan is a beneficial owner of Customer because he owns indirectly 30 percent of its equity interests through his direct ownership of Company A. Betty is also a beneficial owner of Customer because she owns indirectly 20 percent of its equity interests through her direct ownership of Company A plus 16⅔ percent through Company B for a total of indirect ownership interest of 36⅔ percent. Neither Carl nor Diane is a beneficial owner because each owns indirectly only 16⅔ percent of Customer's equity interests through their direct ownership of Company B."



FinCEN

Identification and Verification of Beneficial Owners

A credit union must obtain identifying information for each of the one to five beneficial owners of a legal entity. At a minimum, this would include:

- Name.
- Date of birth.
- Address (although not specified in the regulation, guidance has indicated this should be a physical address, not a mailing address).
- Identification number such as a TIN.

A sample certification form for the identifying information is available under Appendix A of section 1010.230 of the rule. Other methods to obtain the required information can be used as long as the individual certifies to the best of his or her knowledge that the information is accurate.

Credit unions are required under section 1010.230(b) to identify beneficial owners every time a new account is opened. However, a credit union may rely on existing beneficial ownership records so long as it confirms either in writing or verbally that the information is still accurate at account opening. In some situations, account renewals and rollovers can also be considered a new account.

Verifying the identity of each beneficial owner of a legal entity must be done within a reasonable period after the account is opened and prior to account activity. A credit union must verify enough information to form a reasonable belief that it knows the true identity of the beneficial owner(s) of the legal entity member.

FinCEN's FIN-2018-G001 provides additional guidance concerning the collection of beneficial ownership information for existing accounts and conducting ongoing CDD. For existing accounts, credit unions are required to collect or update beneficial ownership information on accounts opened prior to May 11, 2018. For members with accounts opened before May 11, 2018, the obligation to collect or update beneficial ownership information is triggered when the credit union becomes aware of information about the member during the course of normal monitoring necessitating an assessment or reassessment of risk and an indication of a possible change of beneficial ownership.

The guidance further notes credit unions are not required to ask for or to update beneficial ownership information during regular or periodic reviews if there are no specific risk-based concerns. A credit union is required to develop and implement risk-based procedures for conducting ongoing CDD. Periodic reviews are not necessarily a trigger to obtain or update beneficial ownership information. If there is not a risk-related trigger or event for an existing account, the collection or updating of beneficial ownership information is at the discretion of the credit union and implemented as deemed appropriate.

Recordkeeping and Retention Requirements

Beneficial ownership identifying information (including the certification, if obtained) must be kept for five years after the account is closed. If non-documentary methods are used to get the identifying information, document descriptions, how the information was obtained and how any discrepancies were resolved should be kept for five years after any record is made.

Reliance on Another Financial Institution

The credit union can rely on another financial institution's fulfillment of the beneficial ownership requirements for a legal entity for an account opening under certain provisions. These include the following:

- That such reliance is reasonable.
- The financial institution is subject to a rule implementing 31 USC 5318(h) and is regulated by a federal functional regulator.
- The other financial institution contracts with the credit union for an annual certification of its AML program and procedures to comply with the beneficial ownership requirements.

SUSPICIOUS ACTIVITY REPORTS (SARS)

Suspicious activity reporting is considered a cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering and other financial crimes.

What is a SAR?

A SAR is a report that credit unions must file with FinCEN following a suspected incident of money laundering or fraud. These reports are required by the BSA.

Regulatory Requirements to File a SAR

Part 748 of NCUA's rules and regulations requires credit unions to file a SAR for:

- 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 credit union (or an affiliate) and aggregating $5,000 or more, if the credit union 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 member would normally be expected to engage in, and the credit union knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Transactions include deposits; withdrawals; transfers between accounts; currency exchanges; extensions of credit; purchases or sales of any stock, bond, certificate of deposit or other monetary instrument or investment security; or any other payments, transfers or deliveries by, through or to the credit union.

Safe Harbor From Civil Liability

Federal law 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. This safe harbor applies to both SARs filed within the required reporting thresholds and those filed voluntarily on any activity below the threshold.

Systems to Identify, Research and Report Suspicious Activity

Suspicious activity monitoring and reporting are critical internal controls. Appropriate policies, procedures and processes should be in place to monitor and identify unusual activity. The sophistication of monitoring systems depends on the credit union's risk profile, with emphasis on the composition of its higher-risk products, services, members, entities and geographies. There should be adequate staff assigned to the identification, research and reporting of suspicious activities. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems or any combination of these.

Generally, effective suspicious activity monitoring and reporting systems include five key components that are interdependent:

1. Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output).
2. Managing alerts.
3. SAR decision making.
4. SAR completion and filing.

5. Monitoring and SAR filing on continuing activity.

Identifying Unusual or Suspicious Activity

Credit unions use a variety of methods to identify potentially suspicious activity. Some of these include problematic activity identified by employees during day-to-day operations, law enforcement inquiries or requests, such as those typically seen in section 314(a) and section 314(b) requests, advisories issued by regulatory or law enforcement agencies, transaction and surveillance monitoring system output or any combination of these.

Managing Alerts

Alert management focuses on processes used to investigate and evaluate identified unusual activity. A suspicious activity monitoring program should include processes to evaluate any unusual activity identified, regardless of the method of identification. There should be policies, procedures and processes for referring unusual activity from all areas of the credit union or business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation. After thorough research and analysis, investigators should document conclusions including any recommendation regarding whether to file a SAR.

SAR Decision Making

A credit union is expected to establish policies and procedures for a clear and defined process from the point of the initial detection of activity to the results of any investigation. The decision to file a SAR is an inherently subjective judgment. Any decisions should be documented, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including any decisions not to file. However, there is no single form of documentation required when a decision is made not to file.

Filing on Continuing Activity

FinCEN's guidance indicates a credit union can file a SAR on continuing activity after a 90-day review, with a filing deadline of 120 calendar days after the date of the previously related SAR filing. Continuing activity SARs can also be filed prior to this 120-day deadline if the credit union believes the activity warrants earlier review by law enforcement.

Completion and Filing

Credit unions are required to file complete and accurate SARs in a timely manner. The SAR narrative should give a sufficient description of the activity reported as well as the basis for filing. SARs are filed electronically using the BSA Suspicious Activity Report (BSAR) through FinCEN's BSA E-Filing System.

Timing of a SAR Filing

A SAR is required to be filed no later than 30 calendar days from the date of the initial detection of facts that might make the case for filing. If no suspect is identified, the time period for filing a SAR is extended to 60 days. Transactions or account activity may need to be reviewed but this does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the credit union knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity. "Initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. 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 regulation.

SAR Quality

A thorough and complete narrative may make the difference in determining whether the described conduct and its possible criminal nature are clearly understood by law enforcement. As the narrative section is the only area summarizing suspicious activity, this section is "critical." The narrative should give a sufficient description of the activity reported as well as the basis for filing and include five essential elements of information – who? what? when? where? and why? – about the suspicious activity being reported, *SAR Activity Review — Trends, Tips & Issues* (Issue 22), A checklist to preparing the narrative is included on pp. 167-168 of FinCEN's Suspicious Activity Report (SAR) XML Filing Requirements accessible on the BSA E-Filing System. FinCEN issues advisories and guidance containing examples of "red flags" for suspicious activity. Credit unions are requested to check the appropriate box(es) in the Suspicious Activity Information section and include certain key terms in the narrative section of the SAR.

Notifying Board of Directors of SAR Filings

Part 748 of NCUA's regulations require credit unions to notify the board of directors or an appropriate board committee that SARs have been filed. Although there is no requirement

for a specific notification format, management should give enough information, while being mindful of the confidential nature of the SAR.

Record Retention and Supporting Documentation

Copies of SARs and the supporting documentation, either in a paper or electronic format, must be kept for five years from the date of filing. All documentation supporting the filing of a SAR must be provided upon request by FinCEN or an appropriate law enforcement or federal banking agency. "Supporting documentation" includes all documents or records that assisted in making the decision to file a SAR.

Prohibition of SAR Disclosure

No director, officer, employee or agent of a credit union may notify any person involved in the transaction that the transaction has been reported. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities.

CURRENCY TRANSACTION REPORTS (CTRS)

Reporting Large Currency Transactions

CTRs, filed electronically, are required for each currency transaction (deposit, withdrawal, exchange, or other payment or transfer) of more than $10,000 by, through, or to the credit union. Certain types of currency transactions do not need to be reported, such as those involving "exempt persons," a group meeting specific criterion as defined later in this guide.

Identity Verification Required

A credit union is required to verify and record the name and address of a person making the transaction, as well as record the identity, account number, and Social Security or taxpayer identification number, if any, of the individual or entity on whose behalf such a transaction is conducted. A passport, alien identification card or other official document that provides proof of nationality or residence may be used for alien or non-U.S. residents.

A signature card can only be relied on if issued after identification documents verifying identity were examined and noted specifically on the signature card. The specific identity verification information must be recorded on the report. A credit union may not just notate on the CTR “known member/customer” or “signature card on file.”

Aggregation of Currency Transactions

Multiple currency transactions totaling more than $10,000 during any one business day are treated as a single transaction if the credit union has knowledge that they are by or on behalf of the same person. Transactions throughout the credit union should be aggregated when determining multiple transactions.

Types of currency transactions subject to reporting include, but are not limited to, denomination exchanges, individual retirement accounts (IRA), loan payments, automated teller machine (ATM) transactions, purchases of certificates of deposit, deposits and withdrawals, funds transfers paid for in currency, monetary instrument purchases, and certain transactions involving armored car services.

For purposes of aggregation, the credit union will aggregate deposits with deposits and withdrawals with withdrawals (cash "in" transactions are aggregated with other cash "in" transactions and cash "out" transactions are aggregated with other cash "out" transactions).

Structured Transactions – CTR Requirements

Structuring occurs when a person takes a larger transaction of currency and breaks it down into smaller amounts to avoid CTR reporting. The person then makes, or tries to make, transactions at one or more financial institutions, on one or more days.
Under the BSA, no one is to:

- Cause or attempt to cause a credit union to fail to file a CTR.
- Cause or attempt to cause a credit union to file a CTR that contains a material omission or misstatement of fact.
- Structure, assist in structuring, or attempt to structure any transaction with one or more domestic financial institutions.

If a credit union suspects that a person is structuring transactions to evade CTR filing, the *BSA/AML Examination Manual* states a SAR is to be filed. More information can be found in the manual's Appendix G: Structuring.

Filing and Record Retention

FinCEN requires the filing of the electronic Bank Secrecy Act Currency Transaction Report (BCTR) via its BSA E-Filing System within 15 calendar days after the date of the transaction. Copies of CTRs must be kept for five years from the date of the report and can be kept in an electronic format.

Back Filing

Should a credit union find it has failed to file CTRs on reportable transactions, it should begin filing from that point forward. The credit union should also contact FinCEN's Regulatory Helpline to request a determination on whether the back filing of unreported transactions is necessary.

CURRENCY TRANSACTION REPORTING EXEMPTIONS

Certain types of members can be exempted from currency transaction reporting under a two-phase exemption process. Under Phase I exemptions, transactions in currency by banks and credit unions, governmental departments or agencies, and listed public companies and their subsidiaries are exempt from reporting. Under Phase II exemptions, transactions in currency by smaller businesses that meet specific criteria laid out in FinCEN's regulations may be exempted from reporting.

Phase I CTR Exemptions

FinCEN's regulations outline five categories of Phase I exempt persons:

- A bank, to the extent of its domestic operations.
- A federal, state, or local government agency or department.
- Any entity exercising governmental authority within the United States.
- Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (with some exceptions).
- Any subsidiary (other than a bank) of any "listed entity" that is organized under U.S. law and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity.

FinCEN requires the filing of a one-time Designation of Exempt Person report (DOEP) to exempt each eligible listed public company or eligible subsidiary from currency transaction reporting. The report must be filed electronically through the BSA E-Filing System within 30 days after the first currency transaction to be exempted. Information supporting the Phase I exemption should be reviewed and verified annually.

Phase II CTR Exemptions

A business that does not fall into any of the Phase I categories may still be exempted under the Phase II exemptions if it qualifies as either a "non-listed business" or as a "payroll customer" as defined and outlined under the regulations. However, certain businesses are ineligible as an exempt non-listed business. These include:

- Serving as a financial institution or as agents for a financial institution of any type.
- A purchaser or seller of motor vehicles of any kind, vessels, aircraft, farm equipment or mobile homes.
- Law firms, accounting firms or medical practices.
- Auction houses.
- Ship, bus or aircraft charter operations.
- Pawn brokers.
- Engaging in gaming of any kind (other than licensed pari-mutuel betting at racetracks).
- Engaging in investment advisory services or investment banking services.
- Real estate brokers.
- Operating in title insurance activities and real estate closings.
- Engaging in trade union activities.
- Engaging in any other activity that may, from time to time, be specified by FinCEN, such as marijuana-related businesses.

A business that engages in multiple business activities may qualify for an exemption as a non-listed business as long as no more than 50 percent of its gross revenues per year are derived from one or more of the ineligible business activities listed in the rule.

FinCEN requires the filing of a DOEP report through the BSA E-Filing System within 30 days after the first currency transaction for Phase II customer exemptions. Information supporting the Phase II exemption should be reviewed, verified and documented annually. As part of the review, it should be noted Phase II accounts are monitored for suspicious transactions.

Annual Review

The *BSA/AML Examination Manual* states a credit union must, at least once a year, review whether a listed public company, a listed public company subsidiary, a non-listed business or a payroll customer if exempt, is still eligible for that exemption. Such a review can be accomplished by using various resources such as stock quotes from newspapers or the

annual reports filed by a public company. The annual review should also include the application of the suspicious activity monitoring system to each existing account of a Phase II exempt customer. This annual review is not necessary for all exempt persons.

Operating Rules

Subject to compliance with the requirements under §1020.315, a credit union is required to document the basis for its conclusions that a person is an exempt person.

For aggregated accounts, when determining if a customer qualifies as a non-listed business or a payroll customer, a credit union may treat all the customer's exemptible accounts as a single account. If the credit union does this, it must continue to treat such accounts consistently as a single account for purposes of determining the qualification of the customer as a non-listed business or payroll customer.

Safe Harbor for Failure to File CTRs

The rules provide a safe harbor that a credit union is not liable for the failure to file a CTR for a transaction in currency by an exempt person, unless it knowingly provides false or incomplete information or has reason to believe the member does not qualify as an exempt customer. In the absence of any specific knowledge or information indicating that a member no longer meets the exemption requirements, the credit union is entitled to a safe harbor from civil penalties to the extent it continues to treat the member as exempt until the date of the annual review.

Effect on Other Regulatory Requirements

The procedures for exempt persons do not have any effect on the requirement to file SARs or on other recordkeeping requirements.

INFORMATION SHARING

Section 314 of the USA PATRIOT Act

Section 314 of the USA PATRIOT Act establishes procedures for information sharing to deter money laundering and terrorist activity.

Information Sharing Between Law Enforcement and Financial Institutions – Section 314(a)

By way of FinCEN, a federal, state, local or foreign law enforcement agency can request certain information from a credit union or group of financial institutions. A written certification must be given to FinCEN indicating there is credible evidence of terrorist or money laundering activity for the information requested for each individual, entity or organization. FinCEN may then require a credit union to search its records to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity or organization.

Upon receipt of an information request, a credit union must conduct a one-time search of its records to identify accounts or transactions of a named suspect. Unless otherwise instructed, the credit union must search its records for current accounts, accounts maintained during the preceding 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months. The credit union must search its records and report any positive matches to FinCEN within 14 days, unless otherwise specified in the information request.

The *BSA/AML Examination Manual* states a credit union should develop and implement comprehensive policies, procedures and processes for responding to section 314(a) requests. The regulation also restricts the use of the information provided in a section 314(a) request and

Voluntary Information Sharing – Section 314(b)

Section 314(b) encourages a credit union to share information in order to identify and report activities that may involve terrorist activity or money laundering. If a credit union receives information from another financial institution, it must limit its use and maintain its security and confidentiality as indicated in 31 CFR 1010.540(b)(4). This information may be used only to identify and report on money laundering and terrorist activities; determine whether to establish or maintain an account; engage in a transaction; or assist in BSA compliance. Section 314(b) provides specific protection from civil liability. In order to take advantage of the safe harbor, the credit union has to notify FinCEN of its intent to participate in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information. Failure to comply with the requirements will result in the loss of the safe harbor protection and could result in a violation of privacy laws or other laws and regulations.

If a credit union chooses to voluntarily participate in section 314(b), the FFIEC BSA/AML Examination Manual states that policies, procedures and processes should be developed and implemented for sharing and receiving of information. A notice to share information is

effective for one year and a point of contact should be designated for receiving and providing information. A process for sending and receiving information sharing requests should be established and the credit union must take reasonable steps to verify that the other financial institution or association of financial institutions with which it intends to share information has also submitted the required notice to FinCEN. Participating financial institutions are provided with access to a list of other participating financial institutions along with related contact information by FinCEN.

SAR Supporting Information

Section 314(b) does not authorize a credit union to share or disclose the existence or nonexistence of a SAR. If a credit union shares information under section 314(b) about the subject of a prepared or filed SAR, the information shared should be limited to underlying transaction and member information. A credit union can use information obtained under section 314(b) to determine whether to file a SAR, but the intention to prepare or file a SAR cannot be shared with another financial institution.

OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

An office of the U.S. Treasury, OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as transnational organized crime.

OFAC acts under presidential wartime and national emergency powers, as well as various authorities granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. It also develops and administers U.S. sanctions programs.

All U.S. persons, including credit unions, must comply with OFAC's regulations. NCUA evaluates credit union OFAC compliance programs to ensure compliance with the sanctions. OFAC encourages credit unions to take a risk-based approach to designing and implementing an OFAC compliance program. In general, the regulations require a credit union to:

- Block accounts and other property of specified countries, entities and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities and individuals.

Blocked and Prohibited Transactions

Assets and accounts of an OFAC-specified country, entity or individual must be blocked when the property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. Assets and property include anything of direct, indirect, present, future or contingent value (including all types of banking transactions). Credit unions must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or go through a blocked entity; or
- Are in connection with a transaction in which a blocked individual or entity has an interest.

In some cases, an underlying transaction may be prohibited, but there is not a blockable interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected or not processed.

Specially Designated Nationals and Blocked Persons List

The credit union should clearly define its criteria for comparing names provided on the OFAC maintained Specially Designated Nationals and Blocked Person (SDN) List with the names in its files or on transactions and for identifying transactions or accounts involving sanctioned countries. SDNs are individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries (such as Iran and North Korea), as well as individuals, groups and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. The credit union's policies, procedures and processes should also address how it will determine whether an initial OFAC match to the SDN list (sometimes referred to as a "hit") is a valid match or a false hit.

OFAC Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. It can issue a license when it determines that the transaction does not undermine the U.S. policy objectives of the particular sanctions program or is otherwise justified by U.S. national security or foreign policy objectives.

Reporting

A credit union must report all blocks to OFAC within 10 business days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30). Once assets or funds are blocked, they should be placed in a separate blocked account. Prohibited transactions that are rejected must also be reported to OFAC within 10 business days of the occurrence. A full and accurate record of each rejected transaction must be kept for at least five years after the date of the transaction.

Compliance Program

A credit union should establish and maintain an effective, written OFAC compliance program that is commensurate with its risk profile (based on products, services, members and geographic locations). The program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate an employee(s) responsible for OFAC compliance and create training programs for appropriate personnel in all relevant areas of the credit union.

An assessment of its specific product lines, customer base and nature of transactions, and the identification of higher-risk areas for potential OFAC sanctions risk is considered a fundamental element of a credit union's compliance program. All types of transactions, products and services should be considered when conducting the risk assessment and establishing appropriate policies, procedures and processes.

A Framework for OFAC Compliance Commitments

In 2019, OFAC published *A Framework for OFAC Compliance Commitments* on the essential components of a sanctions compliance program. It outlines how the components might be used by OFAC to evaluate apparent violations and resolve any investigations resulting in settlements.

Internal Controls

An effective OFAC compliance program should include internal controls for identifying suspect accounts and transactions, as well as reporting blocked and rejected transactions. As outlined in the *BSA/AML Examination Manual*, internal controls should include certain elements.

- **Identifying and reviewing suspect transactions.** Policies, procedures and processes to address how a credit union determines whether an initial OFAC hit is a valid match or a false hit. A high volume of false hits might indicate a

review of the interdiction program is warranted. Screening criteria used to identify name variations and misspellings would be based on the level of OFAC risk associated with the particular product or type of transaction.

- **Updating OFAC lists.** Policies, procedures, and processes for the timely updating of the lists of sanctioned and blocked countries, entities and individuals.
- **Screening**. For domestic Automated Clearing House (ACH) transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying the originator is not a blocked party and not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying the receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC regulations.

As stated in the *BSA/AML Examination Manual*, if an ODFI receives domestic ACH transactions that its customer has already batched, the ODFI is not responsible for unbatching those transactions to ensure that none violate OFAC's regulations. If an ODFI unbatches a file originally received from the originator in order to process "on-us" transactions, the ODFI is responsible for the OFAC compliance for the on-us transactions because it is acting as both the ODFI and the RDFI and should already know its customers. For the remaining unbatched transactions in the file that are not "on-us," as well as in situations concerning unbatched ACH records other than to strip out the on-us transactions, the credit union should determine the level of its OFAC risk and develop appropriate policies, procedures and processes to address them. Relationships with third-party service providers and their related ACH transactions should be also be assessed to determine the level of OFAC risk.

There are somewhat more stringent OFAC obligations for International ACH transactions (IAT). For inbound IATs, regardless of whether the OFAC flag in the IAT is set, an RDFI is responsible for compliance with OFAC sanctions programs. The ODFI cannot rely on OFAC screening by an RDFI outside of the United States for outbound IATs. In these situations, the ODFI must perform increased diligence to ensure that illegal transactions are not processed. Due diligence for an inbound or outbound IAT may include screening the parties to a transaction and reviewing the details of the payment field information for an indication of a sanctions violation, investigating the resulting hits, if any, and perhaps ultimately blocking or rejecting the transaction. If acting as an ODFI/Gateway Operator (GO) for inbound IAT debits, OFAC guidance authorizes the rejection of transactions that appear to involve blockable property or property interests.

- **Reporting.** Policies, procedures and processes for handling validly blocked or rejected items. If there is a question about the validity of an interdiction,

the credit union can contact OFAC for guidance. Most other items should be reported through usual channels within ten days of the occurrence. Management of blocked accounts should also be addressed as credit unions are responsible for tracking the amount of blocked funds as well as the ownership of and interest paid on those funds. Total amounts blocked, including interest, must be reported to OFAC by September 30.

- **Maintaining license information.** Keeping copies of customers' OFAC licenses on file to verify the legality of transactions and license expiration dates.

New accounts should be compared with OFAC lists prior to opening or shortly thereafter. If performing an OFAC check after an account opening, procedures should be in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Any prohibited transactions occurring before the completion of an OFAC check could be subject to a potential enforcement action.

Independent Testing

A credit union should conduct an independent test of its OFAC compliance program that is performed by the internal audit department, outside auditors, consultants or other qualified independent parties. Testing frequency should be consistent with the OFAC risk profile or the known or perceived risk of business areas.

Designated Responsible Individual

It is an expectation that a qualified individual(s) be responsible for the day-to-day compliance of the OFAC compliance program, including changes or updates to the various sanctions programs, and the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. He or she should have an appropriate level of knowledge about OFAC regulations commensurate with the credit union's risk profile.

Training

Adequate training should be provided for all appropriate employees on a credit union's OFAC compliance program, procedures and processes. The scope and frequency of the training should be consistent with the credit union's risk profile and appropriate to employee responsibilities.

RECORDKEEPING

BSA Record Retention Requirements

The BSA establishes recordkeeping requirements related to various types of records including member accounts, BSA filing requirements and records that document a credit union's BSA compliance. In general, a credit union is required to maintain most records for at least five years. These records can be maintained in many forms including original, microfilm, electronic, copy or a reproduction. The credit union is not required to keep a separate system of records for each of the BSA requirements; however, it must maintain them, so they are retrievable and accessible within a reasonable period of time.

Purchase and Sale of Monetary Instruments Recordkeeping

Credit unions sell many types of monetary instruments such as bank checks or drafts, cashier's checks, money orders and traveler's checks in exchange for cash. It has been found that the purchases of these monetary instruments in amounts below $10,000 is a common money laundering method used to avoid large currency transaction reporting requirements. To counteract this, credit unions are required to verify the identity of persons purchasing monetary instruments for currency in amounts between $3,000 and $10,000 and to maintain records of all such sales.

The regulation requires the record be maintained for five years as of the date of the transaction and contain the following information:

- If the purchaser has a deposit account with the credit union:
- Name of the purchaser.
- Date of purchase.
- Type(s) of instruments purchased.
- Serial numbers of each of the instruments purchased.
- Specific dollar amounts of each of the instruments purchased in currency.
- Identifying information (if not already on file).
- If the purchaser does not have a deposit 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).

Funds Transfers Recordkeeping

Funds transfer systems enable the instantaneous transfer of funds, including both domestic and cross-border transfers. Unfortunately, these systems also present an attractive method to disguise the source of funds derived from illegal activity. As a result, BSA regulations require a credit union involved in funds transfers to collect and retain certain information in connection with funds transfers of $3,000 or more. The regulation defines a funds transfer as "the series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order." This definition does not cover a funds transfer as defined by Regulation E, transfers made through ACH, an ATM or a POS system.

The information required to be collected and retained depends on the credit union's role in the funds transfer (originator, intermediary or beneficiary institution). The requirements may also vary depending on whether an originator or beneficiary is an established member of the credit union and whether a payment order is made in person or otherwise.

The terms "originator" and "originator credit union" are defined in the *BSA/AML Examination Manual* as:

- **Originator -** §1010.100(ii) The sender of the first payment order in a funds transfer. Can be an organization or person that initiates an ACH transaction to an account either as a debit or credit.
- **Originator's [credit union]** - §1010.100(jj) The receiving [credit union] to which the payment order of the originator is issued if the originator is not a [credit union] or foreign bank, or the originator if the originator is a [credit union] or foreign bank.

Originator Institution Responsibilities

For a payment order of $3,000 or more where a credit union acts as the member's originator credit union, it must obtain and retain the following records:

- Name and mailing 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:
    - Name and mailing address of the beneficiary.
    - Account number of the beneficiary.
    - Any other specific identifier of the beneficiary.

In addition, Treasury issued a regulation commonly referred to as the "Travel Rule" that requires all financial institutions to include certain information in transmittal orders for funds transfers of $3,000 or more. In a transmittal of funds, a transmittor is the sender of the first transmittal order. The term includes an originator, except where the transmittor's financial institution is a financial institution or foreign financial agency other than a credit union or foreign bank.

Travel Rule Requirement

For funds transmittals of $3,000 or more, the transmittor's financial institution must include the following information in the transmittal order at the time 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.
- Mailing 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:
    - Name and mailing address of the recipient.
    - Account number of the recipient.
    - Any other specific identifier of the recipient.
- Either the name and address or the numerical identifier of the transmittor's financial institution.

Note that although an intermediary financial institution must pass on all of the information received from a transmittor's financial institution or the preceding financial institution, it has no duty to obtain information not provided by the transmittor's financial institution or the preceding financial institution.

Beneficiary Financial Institution Responsibilities

For each payment order of $3,000 or more that a credit union accepts as a beneficiary's institution, it must retain a record of the payment order.

RESEARCH RESOURCES

Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA) /Anti-Money Laundering (AML) Examination Manual

- Risks Associated with Money Laundering and Terrorist Financing
- Appendix 1: Beneficial Ownership - Exclusions From the Definition of Legal Entity Customer
- Appendix F: Money Laundering and Terrorist Financing "Red Flags"
- Appendix G: Structuring
- Appendix I: Risk Assessment Link to the BSA/AML Compliance Program
- Appendix J: Quantity of Risk Matrix
- Appendix K: Customer Risk Versus Due Diligence and Suspicious Activity Monitoring
- Appendix L: SAR Quality Guidance
- Appendix M: Quantity of Risk Matrix—OFAC Procedures
- Appendix P: BSA Record Retention Requirements
- Appendix Q: Abbreviations
- Appendix R: Enforcement Guidance
- Appendix S: Key Suspicious Activity Monitoring Components

Financial Crimes Enforcement Network (FinCEN)

- Regulations
- Advisories/Bulletins/Fact Sheets
- Guidance
- Answers to Frequently Asked Bank Secrecy Act (BSA) Questions
- FinCEN SAR FAQs
- FinCEN CTR FAQs
- BSA E-Filing System

- FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Requirements
- FinCEN Currency Transaction Report (CTR) Electronic Filing Requirements

National Credit Union Administration (NCUA)

- Bank Secrecy Act Resources
- Letters to Credit Unions and Other Guidance
- Examiner's Guide

Office of Foreign Assets Control - Sanctions Programs and Information

- OFAC's Frequently Asked Questions (FAQs) Index
- When should I call the OFAC Hotline?

NAFCU

- Quarterly BSA Enewsletter w/ staff quizzes, BSA Blast (member only)
- NAFCU Compliance Blog – BSA topics

EXAM PREPARATION STUDY QUESTIONS

THE ABC'S OF THE BANK SECRECY ACT

What are the stages of money laundering?

Type your answer here...

What kinds of penalty assessments can be incurred for BSA violations?

Type your answer here...

BSA'S FIVE PILLARS

What must an BSA/AML program include?

Type your answer here...

What are BSA training requirements?

Type your answer here...

BSA/AML COMPLIANCE PROGRAM/RISK ASSESSMENT

What should be considered when developing a credit union's risk assessment?

Type your answer here...

MEMBER/CUSTOMER IDENTIFICATION PROGRAM

What types of identification can be used for CIP?

Type your answer here...

MEMBER/CUSTOMER DUE DILIGENCE

What should a credit union have for ongoing CDD monitoring?

Type your answer here...

Should CDD only be performed for certain accounts?

Type your answer here...

BENEFICIAL OWNERSHIP REQUIREMENTS FOR LEGAL ENTITY MEMBER/CUSTOMERS

When did it become a requirement to obtain beneficial ownership information?

Type your answer here...

What would be a trigger to obtain beneficial ownership information for existing accounts?

Type your answer here...

SUSPICIOUS ACTIVITY REPORTS (SARS)

What information makes for a good SAR narrative?

Type your answer here...

WHEN MUST A SAR BE FILED?

Is there a dollar amount to file a SAR on insider abuse?

Type your answer here...

What are some examples of suspicious activity triggers?

Type your answer here...

CURRENCY TRANSACTION REPORTS (CTRS)

What types of transactions trigger the need for a CTR to be filed?

Type your answer here...

When is a transaction aggregated?

Type your answer here...

How are CTRs filed?

Type your answer here...

CURRENCY TRANSACTION REPORTING EXEMPTIONS

What types of businesses can be CTR exempt?

Type your answer here...

INFORMATION SHARING

What is the difference between 314(a) and 314(b)?

Type your answer here...

OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

How long are blocked transaction records retained?

Type your answer here...

Do all transactions get OFAC screening?

Type your answer here...

Does OFAC apply when collecting beneficial ownership information?

Type your answer here...

RECORDKEEPING

How long must BSA records be retained?

Type your answer here...

To help focus your studying, here is a breakdown of the exam questions per topic

NCBSO EXAM – 50 QUESTIONS

BSA School Session	Number of Questions
Tuesday, February 8	
The ABC's of the Bank Secrecy Act (BSA)	3-5 Questions
BSA's Five Pillars	4-6 Questions
BSA/AML Compliance Program/Risk Assessment	1-3 Questions
Member/Customer Identification Program (CIP)	3-5 Questions
Member/Customer Due Diligence (CDD)	3-5 Questions
Wednesday, February 9	
Beneficial Ownership Requirements for Legal Entity Member/Customers	6-8 Questions
Suspicious Activity Reports (SARs)	5-7 Questions
Currency Transaction Reports (CTRs) - Part I	6-8 Questions
Currency Transaction Reports - Part II Reporting Exemptions	1-3 Questions
Thursday, February 10	
Information Sharing	3-5 Questions
Office of Foreign Assets Control (OFAC)	3-5 Questions
Recordkeeping	3-5 Questions