 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 1 of 10

I. PURPOSE

Examiners must determine whether the Board of Directors, management, and credit union staff have complied with the requirements outlined in the USA Patriot Act, the Bank Secrecy Act, and other applicable state and federal regulations. Inherent risk within the credit union's operations and transactions must be evaluated to determine whether the credit union has instituted appropriate internal controls to mitigate or reduce the risk.


II. PRIMARY REFERENCES / RELATED REGULATIONS

1. [USA Patriot Act](#)
2. [Bank Secrecy Act](#)
3. [12 CFR 500: Foreign Assets Control Regulations](#)
4. [31 CFR 1010.310: Financial Recordkeeping and Reporting of Currency and Foreign Transactions](#)
5. [NCUA Rules and Regulations Part 748](#)
6. [NCUA Compliance Manual](#)
7. [FFIEC Bank Secrecy Act- Anti-Money Laundering Examination Manual](#)
8. [FFIEC Bank Secrecy Act- Anti-Money Laundering InfoBase](#)


III. MINIMUM PROCEDURES

The BSA review should include the following:

1. **Previous report and AIREs module:** Review the previous DIFS OCU Examination Report and the AIREs Consumer Compliance Violation (CV) module to gain knowledge of previously identified weaknesses and findings. Discuss findings with management to ensure appropriate corrective actions were taken.
2. **Risk assessment:**
 - a. Review the BSA risk assessment to gain an understanding of the level or risk in the operations of the credit union.
 - b. Determine if the risk assessment is reasonable. Ensure the risk assessment addresses all areas of operations including products, services, customers, and geographic location.
 - c. If the risk assessment is performed by an outside individual, discuss action taken as a result of the risk assessment with management.
 - d. Determine whether the risk assessment is updated periodically. Determine whether the process for periodically reviewing and updating its BSA risk assessment is adequate.

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 2 of 10

3. **BSA Policy:** Review the BSA Policy to gain an understanding of the Board-approved procedures, processes, and requirements for compliance. Refer to Sample: BSA Policy Review Checklist for guidelines for a sound BSA Policy.
4. **Compliance Program:** Review the compliance program to ensure it adequately controls the risks identified in the BSA risk assessment. The compliance program must be written, approved by the Board of Directors, and notated in the minutes.
 - a. **Compliance Officer:** The Board of Directors must appoint a qualified individual as the BSA Compliance Officer who is responsible for coordinating and monitoring day-to-day BSA compliance.
 - i. Ensure the Board of Directors has designated a BSA Compliance Officer.
 - ii. Verify that the credit union's current online profile lists the primary patriot act contact person.
 - iii. Determine whether the Compliance Officer has adequate knowledge of BSA requirements. Discuss the BSA policies and procedures with the Compliance Officer to ensure the individual understands the requirements for BSA compliance.
 - b. **Internal Controls:** The Board of Directors is responsible for ensuring an effective internal control structure which includes policies, procedures, and processes designed to limit and control risks and ensure compliance with BSA. For a detailed explanation of BSA internal controls, reference the FFIEC BSA/AML Examination Manual.
 - i. Review and determine if the internal controls are adequate for the size and sophistication of the institution to ensure ongoing compliance.
 - ii. Discuss the procedures for limiting and controlling risk with management.
 - iii. Ensure the staff has been properly trained regarding internal controls.
 - iv. *Optional Procedure:* Review the job descriptions of employees whose responsibilities relate to BSA compliance. Determine whether BSA compliance has been incorporated into the job descriptions and performance evaluations of appropriate personnel.
 - c. **Independent Testing:** Independent testing must be performed by a qualified individual or individuals who are independent from the functions being tested. For information regarding the appropriate

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 3 of 10

scope of independent testing, refer to the FFIEC BSA/AML Examination Manual.

- i. Determine whether independent testing has been performed in the last 12 to 18 months. Regulations do not specify the frequency of the independent testing; however, a sound practice is for the testing to be performed every 12 to 18 months. Verify that the credit union's current online profile states the last time a BSA audit was completed.
- ii. Review the audit report. Discuss all findings and weaknesses with management to ensure appropriate corrective actions have been taken.
- iii. If testing has been performed by internal auditors or the Audit/Supervisory Committee, determine whether the auditors are independent from the functions being tested and have sufficient knowledge to perform the testing.
- iv. *Optional Procedure:* Review the audit workpapers. Determine whether the scope of the audit is appropriate for the complexity and risk structure of the credit union.


d. Training: Ongoing training must be provided to staff, senior management, and the Board of Directors. Documentation of training should be maintained, including the training materials and a log of the dates and attendees of training.

- i. Determine whether adequate and timely training has been provided to the appropriate staff, senior management, and the Board of Directors.
- ii. Review the training log. The training log should detail the dates of training and the attendees.
- iii. Review the training materials to ensure adequate review of regulatory requirements and the credit union's policies, procedures, and processes.
- iv. Ensure new employees receive adequate BSA training at orientation.

5. Customer Identification Program (CIP):

Refer to Sample: Customer Identification Program Requirements for a list of regulatory requirements for a CIP.

- a. Review the credit union's CIP for completeness and compliance with BSA requirements.
- b. Review a sample of recently approved membership cards for compliance with BSA requirements and the credit union's CIP. Determine whether staff obtains the necessary identifying information.

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 4 of 10

- c. Determine whether the credit union maintains the identifying information for a period of five years after an account is closed.
- d. Determine whether customers are provided adequate notice of the identification requirements for opening an account.
- e. Review the procedures for determining whether a customer appears on any federal government list of known or suspected terrorists or terrorist organizations.
- f. Determine whether the credit union uses third party service providers. If so, determine whether there are sufficient procedures and controls to ensure compliance.
- g. Determine if a search is conducted on all new members and current membership on a routine basis to comply with Office of Foreign Asset Control (OFAC) requirements. The credit union's membership database should be scanned on an ongoing basis to determine potential matches to OFAC's Specially Designated Nationals (SDN) list.


6. Customer Due Diligence (CDD):

The Board of Directors and management must establish CDD policies and procedures for obtaining member information so they can predict with relative certainty the types of transactions in which a member is likely to engage. CDD policies and procedures assist in detecting and reporting unusual or suspicious transactions and avoiding exposure from persons who use or attempt to use the credit union's products and services for illicit purposes.

- a. Determine whether the CDD policies, procedures, and processes are sufficient for the institution's risk profile.
- b. Determine whether there are processes in place for obtaining information at account opening, in addition to ensuring current customer information is maintained.
- c. Determine whether management/staff provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient information or inaccurate information is obtained.
- d. Determine whether staff identifies at account opening whether a business member is or likely to operate as a Money Service Business (MSB).

7. Currency Transaction Reports (CTRs):

The credit union must file a CTR for any transaction or combination of transactions in currency in a single day over \$10,000. The form must be filed within 15 days after the transaction and retained for five years from the date of the report. Some individuals and transactions may be exempt from the

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 5 of 10


CTR requirements. For an exemption, the credit union must file a Designation of Exempt Person Form TDF 90-22.53 by March 15th of each year. The Compliance Officer must maintain a list of exemptions. Refer to the FFIEC BSA/AML Examination Manual for a detailed list of persons eligible for CTR exemption.

- a. Obtain a list of CTR exemptions, if any. Ensure Designation of Exempt Person Forms have been filed for the exemptions by March 15th.
- b. Review copies of filed CTRs or a sample of filed CTRs, depending on the quantity filed since the previous examination. Ensure all sections of the forms have been properly completed and reported within 15 days after the transaction.
- c. Review correspondence received from the IRS relating to incorrect or incomplete CTRs. Determine whether management has taken corrective action, when necessary.
- d. Review a sample of aggregate cash transactions reports. Determine whether the reports are reviewed on a daily basis. Determine whether all necessary CTRs have been filed.

8. Suspicious Activity Reports (SARs):

The credit union must file a SAR no later than 30 days from the date of the initial detection of facts that constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing is extended to 60 days. FinCEN suggests a credit union should report continuing suspicious activity by filing a report at least every 90 days. Management must notify the Board of Directors only that a SAR has been filed; no details regarding the SAR should be disclosed. Management must ensure the SARs are complete, thorough, and timely. It is critical that the narrative section of the SAR is thorough and complete; it is the only section that summarizes the details of the suspicious activity. The credit union is prohibited from notifying any person involved in the transaction that the transaction has been reported on a SAR. Refer to the FFIEC BSA / AML Examination Manual for SAR filing requirements.

- a. Through discussions with the Compliance Officer, determine whether adequate policies, procedures and processes exist for identifying suspicious activity and filing SARs. The policies and procedures should indicate the persons responsible for the identification, research, and reporting of suspicious activity.
- b. Determine whether the credit union uses a manual or automated monitoring system.
 - i. If the credit union uses an automated system, review the filtering criteria for reasonableness.

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 6 of 10

- ii. If the credit union uses a manual system:
 - 1. Determine which activity reports are reviewed.
 - 2. Determine which individual or position is responsible for reviewing the reports.
 - 3. Review a sample of the activity reports (i.e. currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, NSF reports, etc.) to verify all necessary SARs have been filed.
- c. Review a sample of filed SARs; the size of the sample should depend on the size, complexity, and risks of the credit union. Ensure all sections of the form have been properly completed, including the narrative section.
- d. Determine if the Compliance Officer and/or management is providing the Board of Directors notice of when a SAR is filed. The Board of Directors should be notified in summary, the volume and nature of SARs filed.


9. Information Sharing:

a. Section 314(a) Request:

- i. Discuss with the Compliance Officer the procedures for responding to a Section 314(a) request. Determine whether the procedures are adequate to ensure the credit union complies with the requirements within two weeks of receiving the information request.
- ii. Verify that the credit union is currently receiving section 314(a) requests from FinCEN. Review the documentation of 314(a) searches performed by the credit union.

b. Section 314(b) Voluntary Information Sharing: Determine whether the credit union voluntarily shares information under Section 314(b) with other financial institutions. If the credit union does:

- i. Verify it has filed a 314(b) Notice with FinCEN annually.
- ii. Determine whether the credit union verifies that its information sharing partners have filed a notification with FinCEN.
- iii. Review the policies and procedures in place to ensure confidentiality and compliance.
- iv. *Optional Procedure:* review a sample of positive matches or recent requests to ensure compliance with the credit union's policies and procedures, appropriate searches are

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 7 of 10

performed, and the credit union uses information only for the purposes allowed and keeps the information secure and confidential.

10. Foreign Accounts / International Transportation of Currency:

a. Currency and Monetary Instrument Report (CMIR) (FinCEN Form 105): A CMIR must be filed for each shipment of currency or other monetary instrument(s) in excess of \$10,000 out of or into the U.S., except via the postal service or common carrier. For transport into or out of the U.S., the credit union must file a CMIR at the time of entry or departure from U.S. For receipt from outside the U.S., the credit union must file a CMIR within 15 days of receipt of instruments (unless a report has already been filed).

- i. Determine whether the credit union has been involved in the transportation of currency into or outside the U.S. If so, verify the necessary CMIRs have been filed the by the appropriate deadline.
- ii. Review any copies of CMIRs for completeness and accuracy.


b. Report of Foreign Bank Financial Accounts (FBAR)(Treasury Form 90-22.1):

- i. Determine whether the credit union has a financial interest in or signature authority over, bank, securities, or other financial accounts in a foreign country, or whether the credit union is otherwise required to file a FBAR form for trust customers.
- ii. If the credit union is required to file a FBAR, review the FBAR for completeness. Ensure all necessary FBARs have been filed.


11. Record Retention:

a. Monetary Instruments Involving \$3,000 to \$10,000 in Currency:


- i. Determine whether the credit union maintains the required records for the sale of monetary instruments in amounts between \$3,000 and \$10,000. The following information is required:
 - 1. For deposit account holders:
 - a. Name
 - b. Date of purchase
 - c. Type of instrument purchased
 - d. Serial number(s) of each instrument

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 8 of 10

- e. Amount in dollars of each of the instruments purchased
 - 2. For non-deposit holders:
 - a. Name and address
 - b. Social Security number
 - c. Date of birth
 - d. Date of purchase
 - e. Type of instrument purchased
 - f. Serial number(s) of each instrument
 - g. Amount in dollars of each of the instruments purchased
 - ii. Ensure the credit union treats multiple purchases in one business day totaling \$3,000 or more as one transaction if staff has knowledge that the purchases have occurred.
 - iii. Review a sample of monetary instruments sold for currency in the amounts between \$3,000 and \$10,000 to determine whether the credit union obtains, verifies, and retains records to ensure compliance with regulatory requirements.
- b. Funds Transfer:** Review a sample of funds transfers to determine whether the credit union acquires and maintains the following required information for five years. Ensure the retained information is retrievable by reference to the name of the member and account number.
 - i. For each payment order of \$3,000 or more that a credit union accepts as an originator's credit union, the credit union must obtain and retain the following records:
 - 1. Name and address of originator
 - 2. Amount of the payment order
 - 3. Date of the payment order
 - 4. Any payment instructions
 - 5. Identity of the beneficiary's institution
 - 6. As many of the following items as are received with the payment order:
 - a. Name and address of the beneficiary
 - b. Account number of the beneficiary
 - c. Any other specific identifier of the beneficiary
 - ii. For each payment order of \$3,000 or more that the credit union accepts as the beneficiary's credit union, the credit union must retain a record of the payment order.

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 9 of 10

- c. **Historical Records:** Determine whether the credit union maintains the appropriate records for compliance with [31 CFR 103](#) (listed below) for five years.
- i. Extensions of credit greater than \$10,000, except those secured by an interest in real property
 - ii. Attempts to transfer more than \$10,000 to or from any person, account or place outside the US
 - iii. All signature cards
 - iv. Member transaction statements or ledger cards
 - v. Credit union and member share drafts or money orders over \$100
 - vi. All withdrawals, other than share drafts or money orders, over \$100 to accounts, except credit union charges or periodic charges made pursuant to an agreement
 - vii. Transfers of more than \$10,000 to any person, account or place outside the US
 - viii. Drafts over \$10,000 issued by, or drawn on, a foreign bank and paid by the credit union
 - ix. Transfers of credit, cash, drafts, other checks, investment securities or other monetary instruments over \$10,000 received directly from a foreign bank, broker or dealer in currency located outside the US
 - x. Records which allow tracing deposited share drafts over \$100
 - xi. Name, address, taxpayer ID number, date of transaction, description of instrument, and method of payment for purchases and redemptions of share certificates
 - xii. Deposit slips or credit checks for transactions, or equivalent wire transfer and direct deposit transactions, over \$100 which specify the amount of currency involved
 - xiii. SARs and supporting documentation
 - xiv. CTRs

 Office of Credit Unions Policies and Procedures	POLICY NUMBER
	10710
COMPLIANCE	EFFECTIVE DATE
	11/01/2018
SUBJECT	REVISION DATE
	11/01/2018
Bank Secrecy Act	PAGE(S)
	Page 10 of 10

12. Money Service Businesses:

Determine if the credit union provides services to Money Service Business (MSB) members. The following are procedures to assist in identifying and reviewing MSBs.

- a. Review the 5300 Call Report/Financial Performance Report (FPR) to determine if the credit union reported any MSBs.
- b. Review a sample of member business account transactions to identify potential MSB accounts.
- c. Determine if the credit union and/or compliance officer has adequate procedures and controls in place to identify MSBs. The BSA policy should include whether the credit union will provide services to MSBs. If so, procedures should be included.
- d. Determine if the compliance officer completes ongoing due diligence and monitoring of MSBs to ensure the business is in compliance. MSBs are required to register with FinCEN within 180 days of establishment (31 CFR 1022.380(b)(3) FinCEN Form 107. MSBs are required to renew their status every 24 months.
- e. FFIEC provides guidelines on what information a credit union should request from MSBs as well as the requirements of the MSB to operate. This includes but is not limited to, independent testing for BSA compliance conducted on the MSB, a compliance officer contact person and BSA/AML training.
- f. Determine if any MSBs are independent money transmitters and registered with the State of Michigan.

13. AIREs Consumer Compliance Violations module and BSA Questionnaire:

- a. Complete the AIREs BSA Questionnaire. Discuss the questionnaire with management to obtain answers, if necessary.
- b. If any violations were identified, complete the Consumer Compliance Violations module.

IV. ATTACHMENTS / FORMS

1. [10710 A1: Sample BSA Items Requested for Examination](#)
2. [10710 A2: BSA Policy Review Checklist](#)
3. [10710 A3: Customer Identification Program Requirements](#)