

NCUA LETTER TO CREDIT UNIONS

**NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314**

DATE: October 2005 **LETTER NO.:** 05-CU-16
TO: Federally Insured Credit Unions
SUBJ: Bank Secrecy Act Compliance
ENCL: AIREs Bank Secrecy Act Questionnaire

Dear Board of Directors:

Compliance with the Bank Secrecy Act (BSA) remains a mandatory area of review during examinations and a condition for continued federal deposit insurance through the National Credit Union Share Insurance Fund.

Recent Developments

In June 2005, the National Credit Union Administration (NCUA), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) jointly issued examination procedures for evaluating compliance with BSA. These examination procedures are contained in the Federal Financial Institutions Examination Council Bank Secrecy Act /Anti-Money Laundering Examination Manual (FFIEC BSA/AML Manual).

The enclosed AIREs BSA questionnaire has been updated to reflect the agreed-upon procedures contained in the FFIEC BSA/AML Manual. This questionnaire will be completed during all NCUA examinations started after September 30, 2005. The AIREs BSA questionnaire establishes a minimum standard for NCUA review of BSA compliance.

Credit unions will notice three significant changes from the prior version of the AIREs BSA questionnaire. The updated questionnaire includes questions about credit union risk assessment, independent testing of internal controls over BSA processes, and monitoring for suspicious activity. NCUA examiners will be looking closely at these areas of focus during their review of BSA compliance.

Areas of Focus: Risk Assessment, Independent Testing, and Monitoring

During the BSA examination process, examiners will evaluate the rationale underlying a decision to accept avoidable risk, the frequency and quality of independent testing, and the process of monitoring accounts and transactions for suspicious activity.

Risk Assessment

While there is no statutory requirement for a credit union to prepare a written risk assessment, it is the initial step in the development and approval of anti-money laundering policies and procedures. Before a board of directors can approve a BSA policy or set standards for the identification of members, decisions about risk are required.

By documenting these decisions in a written risk assessment, officials and credit union management will better understand areas of risk exposure, internal controls adopted to offset risk exposure, and decisions made to accept risk. The complexity and documentation associated with a credit union's risk assessment should correspond to the extent of products and services offered.

Independent Testing

Credit unions must perform periodic independent tests to validate internal controls over compliance with the Bank Secrecy Act. Independent testing is required by Section 748.2(c)(2) of the NCUA Rules and Regulations. Unless a credit union can demonstrate strong controls and limited risk exposure, NCUA expects independent testing to be conducted annually. Additional guidance concerning independent testing is provided in Letter to Credit Unions, 05-CU-09, *Bank Secrecy Act Compliance*, published in June 2005. A copy is available on NCUA's web site at: <http://www.ncua.gov/letters/letters.html>

Monitoring for Suspicious Activity

Credit unions must establish systems to identify suspicious transactions and to monitor accounts for suspicious activity, including structuring. In July 2005, the Financial Crimes Enforcement Network (FinCEN) published FinCEN Ruling 2005-06, *Suspicious Activity Reporting (Structuring)*. This ruling clarifies that credit unions must have systems in place to identify transactions and accounts that appear suspicious. A copy of the ruling is available on FinCEN's web site at: <http://www.fincen.gov/fincenruling2005-6.pdf>

NCUA will expect to see identification and monitoring systems commensurate with credit union resources, product breadth, and services offered.

Communication

To support credit unions in better understanding their BSA responsibilities, NCUA has made a special effort to communicate about the importance of the BSA and agency expectations for compliance.

NCUA has:

- Participated in development of the FFIEC BSA/AML Manual. An electronic copy of the manual is available at: <http://www.ncua.gov/RegulationsOpinionsLaws/BankSecrecy/BankSerecy.htm>
- Engaged in outreach to credit unions through free Credit Union Conferences hosted by the NCUA Office of Small Credit Union Initiatives. A list of upcoming conferences is available at: <http://www.ncua.gov/CreditUnionDevelopment/Events/>
- Coordinated with credit union leagues, chapters, and trade groups
- Published written guidance addressing BSA compliance, including Regulatory Alerts and Letters to Credit Unions. This guidance is available on the NCUA web site, <http://www.ncua.gov/>
- Updated the AIREs questionnaire used by NCUA to assist in evaluating compliance with BSA. The enclosed BSA questionnaire incorporates material from the FFIEC BSA/AML Manual. An electronic copy of the questionnaire is available on the NCUA website at: <http://www.ncua.gov/CreditUnionResources/aires/aires.html>

If you have questions regarding the enclosed questionnaire or compliance with BSA, please contact your district examiner, regional office, or state supervisory authority.

Sincerely,

/s/

JoAnn Johnson
Chairman

Enclosure

	A	B	D	E
1	Type "X" when complete			Return to Checklist
2				
3	BSA - Bank Secrecy Act			
4	INTRODUCTION AND PURPOSE			
5	REPORTS			
6	PENALTIES			
7	RECORD RETENTION REQUIREMENTS			
8	Regulatory References		Yes/No	Comments
9	Risk Assessment / Scoping			
10	1.0.0	Does review of the AIREs Compliance Violations module indicate that all prior violations are resolved?		
11	2.0.0	Has the credit union received correspondence from law enforcement or outside regulatory agencies relating to BSA compliance since the last examination?		
12	3.0.0	Does the credit union maintain a list of high risk accounts?		
13	4.0.0	Has the credit union completed an appropriate assessment of BSA AML risk?		
14	4.0.a	a. If response to Question 4.0.0 is no, assess BSA risk using examiner judgment and note exam BSA risk assessment in Comments box.		
15	Basic Requirements - Policy			
16	5.0.0	Has the board of directors established an appropriate written program to assure the CU meets BSA reporting and recordkeeping requirements?		
17	5.0.a	a. Internal Controls (748.2(c)(1))		
18	5.0.b	b. Independent Testing (748.2(c)(2))		
19	5.0.c	c. Responsible Individual (748.2(c)(3))		
20	5.0.d	d. Training (748.2(c)(4))		
21	5.0.e	e. Customer Identification (748.2(b))		
22	Basic Requirements - Practice			
23	6.0.0	Has the credit union established an adequate Customer (member) Identification Program (CIP)? (103.121)		
24	6.0.a	a. Does the CIP require the minimum information (name, date of birth, address, identification number) prior to opening an account? (103.121(b)(2))		
25	6.0.b	b. Does the CIP require verification of the information obtained? (103.121(b)(2))		
26	6.0.c	c. Does the CU have a process for handling exceptions to the standard CIP policy?		
27	6.0.d	d. Does the CU keep CIP data for five years after account is closed and CIP documents for, at least, five years after account is opened? (103.121(b)(3)(ii))		
28	7.0.0	Is the credit union's independent testing adequate for the size and complexity of the institution? (748.2(c)(2))		
29	8.0.0	Does the BSA officer have appropriate knowledge, resources, and authority - commensurate with the complexity of the credit union's operations? (748.2(c)(3))		
30	9.0.0	Is the credit union's training adequate for the size and complexity of the institution? (748.2(c)(4))		

	A	B	D	E
31	Reporting - Data Quality Violations			
32	10.0.0	Does the credit union have an adequate process for identifying transactions that require completion of a Currency Transaction Report (CTR)? (103.122)		
33	10.0.a	a. Since the prior exam, have one or more transactions occurred that require report through a Currency Transaction Report (CTR)?		
34	10.0.b	b. Does the CU file CTR, Form 104, with the IRS for all transactions (103.22b), and multiple transactions in currency occurring in one day (103.22c), unless it is an exempt transaction, greater than \$10,000 in currency?		
35	10.0.c	c. Is the CTR filed within 15 days after the transaction occurs? (103.27(a)(1))		
36	10.0.d	d. Does the CU properly exempt permitted persons from CTR filing by filing a "Designation of Exempt Person" form? (103.22(d)(2)) and (103.22(d)(3))		
37	10.0.e	e. For exempt persons, does the CU perform an annual review of the account (103.22d4) and renew, biennially (103.22(d)(5)), a statement certifying that the exempt person's account was monitored and the exemption remains appropriate?		
38	11.0.0	Does the CU have an adequate Customer Due Diligence (CDD) process for identifying suspicious transactions and monitoring accounts for suspicious activity? (103.18(a)(2)(iii))		
39	11.0.a	a. Is a Suspicious Activity Report (SAR) filed within 30 days after discovery of a suspicious activity? (103.18(b)(3))		
40	11.0.b	b. Is supporting documentation for a SAR retained for 5 years? (103.18(d))		
41	11.0.c	c. Does CU document decision process on whether to file a non-mandatory SAR?		
42	Recordkeeping			
43	12.0.0	Does the CU maintain the necessary information for the purchase or issuance, by currency, of credit union checks, cashier's checks, traveler's checks, and money orders for amounts between \$3,000 and \$10,000? (103.29(a)) and (103.29(b))		
44	13.0.0	Does the CU maintain adequate historical records on certain transactions for 5 years? If YES, continue to question 14, otherwise answer each sub-question		
45	13.0.a	a. Extensions of credit greater than \$10,000, except those secured by an interest in real property? (103.33(a))		
46	13.0.b	b. Attempts to transfer more than \$10,000 to or from any person, account or place outside the U.S.? (103.33(b))		
47	13.0.c	c. All signature cards? (103.34(b)(1))		
48	13.0.d	d. Member transaction statements or ledger cards? (103.34(b)(2))		
49	13.0.e	e. CU and member share drafts or money orders over \$100? (103.34(b)(3))		

	A	B	D	E
50	13.0.f	f. All withdrawals, other than share drafts or money orders, over \$100 to accounts, except CU charges or periodic charges made pursuant to an agreement? (103.34(b)(4))		
51	13.0.g	g. Transfers of more than \$10,000 to any person, account, or place outside the US? (103.34(b)(5,6))		
52	13.0.h	h. Drafts over \$10,000 issued by, or drawn on, a foreign bank and paid by the CU? (103.34(b)(7))		
53	13.0.i	i. 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? (103.34(b)(8,9))		
54	13.0.j	j. Records which allow tracing of deposited share drafts over \$100? (103.34(b)(10))		
55	13.0.k	k. Name, address, taxpayer ID#, date of transaction, description of instrument, and method of payment for purchases and redemptions of share certificates? (103.34(b)(11,12))		
56	13.0.l	l. Deposit slips or credit checks for transactions, or equivalent wire transfer and direct deposit transactions, over \$100 which specify the amount of currency involved? (103.34(b)(13))		
57	Specific Products & Services			
58	14.0.0	Since the prior exam, has the CU originated or received any wire transfers? If answer is NO, skip to question 15		
59	14.0.a	a. With regard to wire transfers, does the CU retain, for 5 years, the required information for each payment order that it accepts of \$3,000 or more? (103.33(e))		
60	14.0.b	b. Is the required wire transfer information, identified in the above question, retrievable by reference to the originator's name and account number? (103.33(e)(4))		
61	15.0.0	Since the prior exam, has the CU been involved with the transportation of currency outside the US or maintenance of an account in a foreign country? If answer is NO, skip to question 16		
62	15.0.a	a. Does the CU file FinCEN Form 105 for the physical transportation of currency in excess of \$10,000 into or outside the USA? (103.23)		
63	15.0.b	b. Is a Report of Foreign Bank and Financial Accounts indicating a financial interest in an account in a foreign county filed annual on or before June 30? (103.24)		
64	Information Sharing			
65	16.0.0	Has the CU designated an accurate point of contact on the most recent 5300 to receive 314a information requests from FinCEN regarding investigations of terrorist activity or money laundering? (103.100(b)(2)(iii))		
66	16.0.a	a. Is the CU accessing the electronic list on FinCEN's secure website or receiving fax transmissions? (103.100(b)) <i>Please document access method (web or fax) in comment box.</i>		

	A	B	D	E
67	16.0.b	b. Does the CU begin its search, required by the 314a information request, promptly and complete it within 2 weeks, reporting any matches to FinCEN upon detection? (103.100(b)(2))		
68	17.0.0	Does the CU voluntarily share 314b information with other financial institutions for purposes of identifying and reporting suspected terrorist activity or money laundering? (103.110) If answer is NO, continue to question 18		
69	17.0.a	Has the CU submitted a Section 314(b) notice to FinCEN for the current year? (103.110(b)(2))		
70	17.0.b	Has the CU verified that its information sharing partner completed the 314(b) notice? (103.110(b)(3))		
71	Third Party Service Providers			
72	18.0.0	Is the CU using a third party service provider?		
73	18.0.a	Does the CU have an adequate due diligence process for reviewing actions taken by the third party to comply with BSA requirements on behalf of the CU?		
74	Testing Internal Controls			
75	19.0.0	Test the CU's internal control function by reviewing a minimum of 10 account level transactions for BSA compliance	<i>When responding "Yes" for testing, briefly describe tests in comment section.</i>	
76	19.0.a	a. Were transactions reviewed for compliance with Reporting Requirements (Q10-11)		
77	19.0.b	b. Were transactions reviewed for compliance with Recordkeeping Requirements (Q12-13)		
78	19.0.c	c. Were transactions reviewed for compliance with Specific Product and Service requirements? (Q14-15)		
79	19.0.d	d. Were transactions reviewed for compliance with Information Sharing Requirements (Q16-17)		
80	19.0.e	e. Enter the total number of transactions tested		
81	Conclusion			
82	20.0.0	Did the examination identify required CTR or SAR forms that were not filed? If NO, continue to question 21.0.0		
83	20.0.a	a. For the required CTR forms that were not filed, will the credit union seek a CTR backfiling determination?		
84	21.0.0	Based on the results of exam testing, are the CU's internal controls effective?		
85	21.0.a	a. Are internal controls appropriate for the complexity of the institution?		
86	21.0.b	b. Do results of testing indicate credit union's risk assessment is appropriate?		
87				

Cell: A4

Comment: The Bank Secrecy Act (BSA) requires financial institutions to file certain currency and monetary instrument reports. These reports provide a paper trail of money laundering activities relating to drug traffickers and white collar criminals and assist law enforcement with investigations and prosecutions.

Cell: A5

Comment: Copies of required reports may be found on FinCEN's website at: <http://www.fincen.gov>.

Cell: A6

Comment: Violations of this regulation may result in significant civil penalties and criminal penalties for any domestic financial institution, and upon any director, officer or employee.

Cell: A7

Comment: Generally, all records required by the BSA must be retained for 5 years. An exception is the Customer Identification Program (CIP): CIP records must be maintained for EITHER 5 years from account closure OR from the date the information is received.

Subpart C of Part 103 of Title 31 of the C.F.R. details the records required to be maintained (See §103.31 through §103.38). For CIP recordkeeping requirements, see 31 C.F.R. §103.121.

Cell: A8

Comment: Bank Secrecy Act is set forth in Title 12 and Title 31 of the Code of Federal Regulations (CFR). Title 31 contains the text of the Bank Secrecy Act. Title 12 contains implementing regulations passed by NCUA and other federal regulators.

Unless otherwise indicated, regulatory citations beginning with 103 and references to CFR refer to Title 31 throughout this questionnaire. Regulatory citations beginning with 748 refer the NCUA Rules and Regulations, which are published in Title 12 of the CFR, throughout this questionnaire.

Some state regulatory authorities and the Internal Revenue Service have published additional anti-money laundering regulations, which may apply to federally insured state chartered credit unions.

NCUA Rules and Regulations (published in Title 12 of the CFR) can be viewed on the NCUA web site at: http://www.ncua.gov/RegulationsOpinionsLaws/rules_and_regs/rules_and_regs.html

Title 31 of the CFR, which includes the USA Patriot Act, can be viewed on FinCEN's web site at: http://www.fincen.gov/reg_statutes.html

The complete CFR can be viewed at: <http://www.gpoaccess.gov/cfr/index.html>

Cell: B10

Comment: Violations noted at a prior contact and not successfully resolved must be reported as repeat violations. Violations resolved since a prior contact should be marked as resolved within the AIRES CV (Compliance Violation) module

Cell: B11

Comment: If correspondence from law enforcement and outside parties (such as FinCEN or the IRS Detroit Computing Center) was received, it should be carefully reviewed and considered while establishing the scope of BSA review.

Examiners should not request or review National Security Letters (NSLs) since NSLs are highly confidential documents. Instead, examiners should evaluate the credit union's established processes to respond to NSLs.

Cell: B12

Comment: Credit unions should periodically perform a review of accounts to determine which member or non-member accounts may be high risk.

High risk accounts are accounts that a credit union has determined pose specific money laundering risks due to the nature of a business, occupation, or anticipated transaction activity. Credit unions should look at services sought, source of funds, geographic location, and other factors when determining whether an account is high risk.

In general, accounts operated for senior foreign political persons and their family members and close associates (collectively known as politically exposed persons), nonresident aliens, cash-intensive businesses, non-bank financial institutions, or professional service providers may have a higher inherent risk of money laundering or terrorist financing activity.

However, within any category of business, there will be members that pose varying levels of risk. Each individual account must be reviewed to determine whether it should be classified as high risk.

When an account is identified as high risk, it should be tracked through coding within the credit union's data processing system or other processes, such as maintenance of a list. Some credit unions may use multiple risk classifications; other credit unions may determine no high risk accounts are served.

Cell: B13

Comment: Each credit union must have a BSA/AML compliance program tailored to the particular risks of that credit union. To set up an effective program, the credit union should assess BSA/AML risk exposure. Appendix J, Quantity of Risk Matrix, of the FFIEC BSA/AML Manual provides an example of factors that would likely be considered during a risk assessment, such as members, products, services, and geographic locations.

The risk assessment process should determine the credit union's inherent risk (quantity of risk), how internal controls mitigate (reduce) risk exposure, and whether the remaining level of risk exposure is appropriate for the credit union. While fully offsetting all BSA/AML risk would be prohibitively expensive for most financial institutions, there should be a reasonable relationship between the level of unmitigated risk and resources devoted to BSA/AML.

The credit union's risk assessment may consider the following factors during the risk identification process: customers, geographic locations, products, and services. Depending on the complexity of credit union operations, the risk assessment may be a separate written document or a discussion noted in the minutes of the board of directors.

Cell: B14

Comment: If a credit union has not developed a BSA/AML risk assessment, the examiner must complete a risk assessment and note his/her assessment of BSA/AML risk exposure at the credit union in the comment box.

See Appendix J, Quantity of Risk Matrix, for an example of factors to consider during a risk assessment.

While there is no statutory requirement for a written BSA/AML risk assessment, the appropriate and thorough assessment of risk is the foundation of a sound BSA/AML compliance program and an industry best practice.

Cell: B16

Comment: Each credit union is required to have a compliance program that includes: (1) a system of internal controls to ensure ongoing compliance; (2) testing for compliance by the credit union or outside party; (3) a compliance officer responsible for monitoring day-to-day compliance; and (4) training for appropriate employees.

Cell: B17

Comment: Internal controls are the credit union's policies, procedures, and processes designed to limit and control risks and to achieve compliance with BSA. The sophistication of internal controls should be commensurate with the size, structure, risks, and complexity of the credit union. Large, complex credit unions may implement departmental internal controls that address risks and compliance requirements unique to a particular line of business; departmental internal controls are part of a comprehensive BSA/AML compliance program.

Internal controls should: identify operations more vulnerable to abuse by money launderers, provide for periodic updates to the credit union's risk profile, provide for program continuity despite changes in staff, meet regulatory requirements, identify reportable transactions, provide for dual controls and segregation of duties, provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity, provide for adequate supervision of employees that engage in any activity covered by BSA, incorporate BSA compliance into job descriptions and performance evaluations of appropriate personnel, and otherwise mitigate BSA/AML risk exposure.

Cell: B18

Comment: Independent testing should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. Persons conducting BSA/AML testing should report directly to the board of directors or to a designated committee of the board, such as the supervisory committee.

There is no regulatory requirement to conduct annual independent testing. However, annual testing is a sound practice and strongly recommended for credit unions with limited internal controls.

When a credit union chooses to test less frequently (i.e. 18 months), the credit union should be able to demonstrate a strong history of compliance, board approval of the longer testing plan, and reasonable belief that existing internal controls function appropriately.

Cell: B19

Comment: The credit union must designate a qualified individual to serve as the BSA compliance officer. This person coordinates and monitors day to day compliance with BSA.

While the title of the person responsible for overall BSA/AML compliance is not important, the level of authority and responsibility is critical. The compliance officer must have sufficient authority (access to board and/or supervisory committee) and resources (monetary, physical, and personnel) to administer and effective BSA/AML compliance program based on the credit union's risk profile.

Appointment of a BSA compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, resources, or time to satisfactorily complete the job.

Cell: B20

Comment: Appropriate personnel must be trained in applicable aspects of BSA. Training should include regulatory requirements and the credit union's internal BSA/AML policies, procedures, and processes. At minimum, the training program must provide training for all personnel whose duties require knowledge of BSA. Board members and senior management must also be familiar with the importance of BSA/AML regulatory requirements, ramifications of noncompliance, and the risks posed to the credit union.

Credit unions should document their training programs. Training and testing materials, the dates of training sessions, and attendance records should be maintained by the credit union and be available for examiner review.

Cell: B21

Comment: As of October 1, 2003, all financial institutions must have a written customer identification program (CIP) that is incorporated into the BSA/AML compliance program. The CIP is intended to enable the credit union to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer.

Cell: B23

Comment: When establishing a CIP, a credit union should conduct a risk assessment of its customer base and product offerings. In determining risks, consider the types of accounts offered (member, business, etc), methods of opening accounts (in person, online, indirect relationships, etc), types of identifying information available (documentary, non-documentary, etc), and the credit union's size, location, and field of membership.

CIP applies to "customers". A customer is a person (individual, corporation, partnership, trust, estate, or any other entity recognized as a legal person) who opens a new account for: itself, another individual lacking legal capacity, or an entity that is not a legal person (e.g. civic club).

Excluded from the definition of customer are federally regulated banks (all financial institutions regulated by NCUA, FDIC, FRB, OCC, or OTS), banks regulated by a state bank regulator, governmental entities, and publicly traded companies as described in 13 CFR 103.22(d)(2)(ii) through 103.22(d)(2)(iv).

Cell: B24

Comment: For a U.S. person, the identification number is the taxpayer identification number; for a non-US. person, it can be a taxpayer identification number, passport number and country of issuance; alien identification card number, or number and country of issuance of any other government-issued document bearing a photo or similar safeguard.

Cell: B25

Comment: Credit union must have a reasonable belief that identity of an individual is known.

For a U.S. person, the identification number is the taxpayer identification number; for a non-US. person, it can be a taxpayer identification number, passport number and country of issuance; alien identification card number, or number and country of issuance of any other government-issued document bearing a photo or similar safeguard.

Cell: B26

Comment: Best Practice Issue – This question is not related to a regulatory requirement. Credit unions should have a process for handling requests for membership when the person cannot provide the identifying documents required in the CIP policy. For example, disabled individuals may not have driver's licenses or minors may not have state issued identification. The CIP should provide for a second level of acceptable documents or a contingency plan, such as referring the person's application to the BSA compliance officer for further investigation and consideration.

Cell: B27

Comment: At minimum, the credit union must retain the identifying information (name, address, date of birth, TIN, and any other information required by CIP) for five years after the account is closed. For credit cards, the retention period is five years after the account closes or becomes dormant.

The credit union must also keep a description of the following for five years after the record was made:

- Any document relied on to verify identity – noting the type of document, the identification number, the place of issuance, and (if any) the date of issuance and expiration date.
- The method and the results of any measures taken to verify identity.
- The results of any substantive discrepancy discovered when verifying identity.

Cell: B28

Comment: Independent testing refers to testing by a party not involved in or supervised by a person involved with BSA compliance.

Extent and type of testing should be comprehensive, timely, and adequate. It should address:

- the credit union's assessment of BSA risk,
- effectiveness of overall compliance program,
- BSA reporting (CTRs and SARs) and recordkeeping requirements,
- transaction testing in all areas (share and loan products, e-commerce, and electronic payment services),
- adequacy of training provided to staff and officials, and
- timeliness of program review and enhancement by board of directors.

Cell: B29

Comment: While the title of the person responsible for overall BSA/AML compliance is not important, the level of authority and responsibility is critical. The compliance officer must have sufficient authority (access to board and/or supervisory committee) and resources (monetary, physical, and personnel) to administer and effective BSA/AML compliance program based on the credit union's risk profile.

Appointment of a BSA compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or time to satisfactorily complete the job.

Cell: B30

Comment: Training should be ongoing and incorporate current developments and changes to BSA and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems should also be covered during training. The program should reinforce the importance the board places on compliance with BSA and ensure all employees understand their role.

Training should be tailored to a person's specific responsibilities. In addition, an overview of BSA/AML requirements should be given to new staff. Examples of money laundering activity and suspicious activity monitoring and reporting should be tailored to each individual audience. For example, training for tellers should focus on examples involving large currency transactions or other suspicious activities; training for the loan department should provide examples involving money laundering through lending arrangements.

Cell: B32

Comment: Credit union should have a process for aggregating same day transactions conducted on multiple accounts owned by the same member, multiple currency transactions, same day transactions conducted at multiple branches, and transactions conducted through third party systems, such as shared branching or ATM networks, and not posted to member share records on the day of conduct.

Multiple currency transactions shall be treated as a single transaction if the financial institution has knowledge that they are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 during any one business day (or in the case of the Postal Service, any one day). Deposits made at night or over a weekend or holiday shall be treated as if received on the next business day following the deposit.

Cell: B33

Comment: Scoping question – there is no requirement to file a minimum number of CTRs.

NCUA examiners may access Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) filed with FinCEN through request to the regional office.

Credit unions and examiners may obtain information concerning whether a CTR was filed by calling 1.800.800.CTRs. Note – credit unions cannot obtain information from FinCEN about SARs filed. FinCEN's SAR information is accessible only to supervisory agencies and law enforcement officials.

Cell: B34

Comment: Form 104 must be the exact form prescribed by the IRS, not minimized or on thermal paper. The number for the IRS National Forms Distribution Center is 1-800-829-3676.

Credit unions may also file CTRs and/or SARs using a secure internet connection through FinCEN's BSA Direct program. Information about enrollment and access to BSA Direct is available on FinCEN's web site.

Cell: B35

Comment: CTRs shall be filed by the credit union within 15 days following the day on which the reportable transaction occurred.

Cell: B36

Comment: Transactions with the Federal Reserve Banks, Federal Home Loan Bank, US Banks, savings associations, and credit unions are always exempt from CTR reporting.

Credit unions may exempt certain members from CTR reporting if they fall into one of the following categories: Retail Businesses, Specifically Enumerated Businesses, Government Agencies, and Payroll Withdrawals. See 13 CFR 103.22d for a discussion of the types of persons that may be exempted.

A credit union designates each exempt person within 30 days after the reportable transaction in currency at which a person asks to be exempted under 103.22d. Except for situations covered by 103.22d3ii, credit unions designate an exempt person by filing Treasury Form TD F 90-22.53.

Cell: B37

Comment: Each exemption will have dollar limits. The limit should reflect ordinary and expected transactions conducted by the customer, based on the credit union's analysis of the account. CTRs should be filed for transactions in excess of the dollar limits established in the exemption.

Cell: B38

Comment: Credit unions must have processes to identify and to monitor transactions to determine whether these transactions have apparent lawful purposes and are the sort that a particular customer would normally be expected to engage in. The FFIEC BSA/AML Examination Manual refers to this as a Customer Due Diligence (CDD) program.

For unusual transactions, credit unions should file a suspicious activity report (SAR) if, after examining the background and possible purpose of the transaction, the credit union knows of no reasonable explanation for the transaction after examining available facts.

Cell: B39

Comment: A SAR must be filed within 30 days after discovery for suspicious transactions of any amount or when there is reasonable suspicion that a crime against the credit union has occurred and the amount of the loss is greater than \$5,000 if a non-insider. If an insider, then any amount. Mandatory SAR filing criteria are provided in the comments for question 11.0.c.

Supporting documentation is not to be sent with the SAR, but retained in a readily retrievable form by the credit union. The narrative section of the SAR should summarize the events, participants, and suspicious actions. It should also describe supporting documentation that can be provided by the credit union.

The fact that a SAR has been filed is confidential. The person involved in the transaction must not be notified that a SAR was filed. If the credit union is subpoenaed or requested to disclose a SAR or information therein, the credit union must decline and notify NCUA's Office of General Counsel except when the request is made by FinCEN, appropriate law enforcement, or credit union supervisory agency.

Cell: B40

Comment: A credit union shall maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. Supporting documentation shall be identified, and maintained by the credit union as such, and shall be deemed to have been filed with the SAR. A credit union shall make all supporting documentation available to FinCEN and any appropriate law enforcement agencies or credit union supervisory agencies upon request.

Cell: B41

Comment: This is a best practice issue – there is no regulatory requirement to document the decision process for non-mandatory SARs. (If a potential suspicious activity does not trigger mandatory SAR filing, a credit union may investigate the activity and determine whether to file a SAR based on a lack of apparent business or lawful purpose.)

Mandatory SARs include:

- transactions involving insider abuse for any amount,
- violations aggregating \$5,000 or more when a suspect can be identified,
- violations aggregating \$25,000 or more regardless of whether a suspect can be identified,
- transactions that involve \$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act
- computer intrusion – efforts to remove, steal, procure, or otherwise affect funds or critical information or to damage, disable, or otherwise affect critical systems of the credit union.

Refusal to file a mandatory SAR is a violation of the Bank Secrecy Act.

Non-mandatory SARs include other transactions identified as suspicious by the credit union due to no apparent business or lawful purpose.

Cell: B43

Comment: The following information must be maintained by the credit union for the purchase of credit union checks, cashier's checks, traveler's checks and money orders: (a) name of purchaser; (b) address if purchaser does not have an account at the credit union; (c) purchaser's account number, or social security number; (d) date of birth of the purchaser if they do not have an account at the credit union; (e) date of purchase; (f) type of instrument purchased; (g) serial number of each purchased instrument; (h) dollar amount of each purchase by currency; (i) method used to verify identity of purchaser; and, (j) indication if transaction is part of a multiple sale during one business day.

This information may be maintained in the form of a log or produced, on demand, from a credit union's data processing system. If information is maintained in the data processing system, credit union should be able to produce report or reports showing all required information upon request.

Cell: B44

Comment: Credit unions must maintain records of certain transactions for five years or longer. These transactions are listed in questions 13.0.a-13.0.l, below.

If all applicable record retention requirements are met, an examiner may choose to answer question 13.0.0 and continue to question 14.0.0. If any of the record retention requirements are not met, questions 13.0.0 through 13.0.l must be answered.

Cell: B58

Comment: Scoping question – has the credit union originated or received wire transfers on behalf of members or non-members since the prior examination?

If credit union originates or receives wire transfer, credit union must comply with BSA recordkeeping requirements, including requirements added through the USA Patriot Act. Wire transfer records are subject to review during 314(a) searches.

Cell: B59

Comment: All records that are required to be retained by this part shall be retained for a period of five years. All such records shall be filed or stored in such a way as to be accessible within a reasonable period of time, taking into consideration the nature of the record, and the amount of time expired since the record was made.

Cell: B60

Comment: The following information may be retained as original, microfilm, other copy, or electronic record: (a) Name and address of the originator (sender of payment order); (b) amount of payment order; (c) date of payment order; (d) payment instructions from originator; (e) name of the financial institution where the payment order is to be credited; (f) name, address, and account number of the recipient of the payment order.

Cell: B61

Comment: Scoping question – has the credit union transported currency or maintained accounts in foreign countries since the prior examination?

Credit unions maintaining accounts in foreign countries may be using the accounts to facilitate currency exchange. Currency exchange can be an indicator of members with non-US residences or accounts with strong ties to foreign interests. This should be factored into the credit union's risk assessment.

Credit unions transporting currency outside the United States may have branches on US soil in foreign countries. Branches on US soil must comply with the Bank Secrecy Act.

If a foreign branch is not located on US soil (i.e. shared branching partner), transactions conducted at that branch must comply with the anti-money laundering (AML) rules governing that country. A credit union with this type of foreign branch must perform a risk assessment of transactions conducted at foreign operations and, as necessary, implement appropriate processes to identify and to monitor foreign branch transactions for suspicious activity.

Alternatively, the credit union may be acting as a third party intermediary for another party when transporting funds; if so, credit union should take reasonable steps to ensure funds are being transported for lawful purposes. For example, credit union may request information concerning source and use of funds, information about the recipient and originator of the transported currency, and other pertinent information.

Cell: B62

Comment: Credit union must file Form 105 if it transports more than \$10,000 in currency to or from the USA.

A credit union is not required to file Form 105 for actions taken by individual members, although the credit union may wish to advise members of the filing requirement. However, if member activity appears suspicious, a SAR may be appropriate.

Cell: B63

Comment: This form does not need to be completed for currency transported through the postal service or by common carrier. Report of Foreign Bank and Financial Accounts is often referred to as "FBAR"; it is Form TD F 90-22.1.

Cell: B65

Comment: Accurate point of contact information must be provided on the quarterly call report, Form 5300, submitted to NCUA or state regulator. This information is reported to FinCEN as a control over access to 314(a) request lists and the 314(a) secure web site.

If information is not correct and current, examiners should file a corrected call report, with correct point of contact information. Please note: NCUA transmits updated point of contact information to FinCEN every two weeks. There may be up to a two week delay between examiner upload of corrected information and FinCEN's receipt of

updated 314(a) point of contacts.

Cell: B66

Comment: The credit union must obtain the 314a request list, which is usually published every two weeks on Monday or Tuesday. Credit unions signed up for fax transmission will receive a fax from FinCEN. Credit unions reporting email points of contact must register with FinCEN and then log into the 314a secure web site to view or download the current 314a request list.

Credit unions may use a third party servicer provider to compare the 314a request list to member accounts. If a third party is used, the credit union remains responsible for accessing FinCEN's web site and providing the third party with the most recent 314a list. FinCEN does not grant independent web site access to third party vendors.

Cell: B67

Comment: Credit union must search records "expeditiously"; FinCEN may establish a shorter deadline than two weeks for some requests.

Credit union must search its records for:

- (A) Any current account maintained for a named suspect;
- (B) Any account maintained for a named suspect during the preceding twelve months; and
- (C) Any transaction, as defined by Sec. 103.90(d), conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmitter or the recipient, during the preceding six months that is required under law or regulation to be recorded by the financial institution or is recorded and maintained electronically by the institution.

Member activity (any activity linked to an account) must be searched for the prior 12 months, an example of records required to be searched (as above) follows:

- Deposit account records (share drafts, savings, certificates, etc.) to determine whether subject is or was an accountholder.
- Funds transfer records maintained under CFR 103.33 to determine whether subject was originator/transmitter of funds transfer or a beneficiary/recipient.
- Records of sales of monetary instruments (cashier's checks, money orders, or traveler's checks) maintained under CFR 103.29
- Loan records to determine if subject is borrower.
- Safe deposit box records to determine whether subject maintains, maintained, or had access to a safe deposit box, but only if safe deposit box records are maintained electronically.

Non-member activity (any activity not linked to an account) must be searched for the prior 6 months.

Additional information concerning search parameters and requirements is contained in the FinCEN's Frequently Asked Questions (FAQs) concerning the 314(a) Process, published in February 2003.

Cell: B68

Comment: This is a scoping question – information sharing with other financial institutions is voluntary. If credit union does not share information under 314(b) of the USA Patriot Act, continue to question 18.0.0.

Cell: B69

Comment: A credit union that intends to share information must file a notice with FinCEN each year. Upon filing the form, the credit union can share information for one year from the date of filing. The form is located on FinCEN's web site at https://www.fincen.gov/fi_infoappb.html and may be filed electronically.

Cell: B70

Comment: Before sharing information, a credit union must take reasonable steps to verify that the other financial institution

with which it intends to share information has submitted the required notice to FinCEN. A credit union may confirm the other institution appears on the list that FinCEN periodically makes available or by directly confirming the notice was filed with the other institution.

Cell: B72

Comment: Credit unions may use third parties to assist with BSA/AML compliance or to provide services and products. However, credit unions cannot transfer BSA/AML liability to a third party. The credit union remains responsible for compliance.

Areas of operation that might involve third parties in BSA/AML activities include: new members, indirect lending, account monitoring, shared branching, ATMs, brokers, CUSOs, 314a searches, customer identification, and others.

Cell: B73

Comment: Credit unions cannot assume that third parties are effectively meeting BSA/AML compliance responsibilities on their behalf. Credit unions must exercise due diligence over third party activity.

Like other areas of credit union operations, appropriate internal controls must be implemented to review actions taken by third parties and third party performance should be reviewed during independent testing. Credit unions cannot transfer BSA/AML liability to third parties.

Cell: B75

Comment: Test the credit union's internal control function by reviewing a sample of account level transactions. An account level transaction is a transaction that can be traced from the member statement (or other records of the credit union) back to source documents. See appendix O of the FFIEC BSA/AML manual for discussion of transaction testing.

At least 10 tests of transaction must be performed, examiner judgment determines which areas to test. Indicate whether tests are performed in each area (a-d). When tests are performed, briefly describe the test(s) that you chose to conduct in the appropriate comment section of the questionnaire.

Cell: B76

Comment: Transaction test example – Request a list of all cash transactions over \$7000 for a 3 week period sorted by account number. Review accounts with multiple transactions to determine if CTR or SAR should have been filed. Compare your assessment to CTRs and SARs completed by credit union.

Other tests could be conducted in this area. See FFIEC BSA/AML manual core procedures – CTR, CTR Exemptions, SAR – for additional suggestions.

Cell: B77

Comment: Transaction test example – Request a list of all purchases of monetary instruments for more than \$3000 over a 3 week period sorted by purchase date. Review sales receipts for traveler's checks, cashiers checks, and/or other monetary instrument to determine whether purchases in excess of \$3,000 were made. Compare your assessment to the list provided by credit union.

Other tests could be conducted in this area. See FFIEC BSA/AML manual core procedures – Purchase and Sale of Monetary Instruments – for additional suggestions.

Cell: B78

Comment: Transaction test example – Request a list of wire transfers for a 3 week period sorted by originator's name and account number. Compare list of transfers to credit union records and verify the maintenance of all required information.

Other tests could be conducted in this area. See FFIEC BSA/AML manual core procedures – Funds Transfers – for additional suggestions.

Cell: B79

Comment: Transaction test example – Run a sample of names from the most recent 314a list through the credit union's search process. Determine whether all required accounts and transactions are included in the search. Regional offices have access to the current 314a lists.

Other tests could be conducted in this area. See FFIEC BSA/AML manual core procedures – Information Sharing – for additional suggestions.

Cell: B80

Comment: Include all tests performed in 19.0.a-19.0.d, how many individual transactions were reviewed? Number of transactions must be 10 or more.

Level of transaction testing should correspond to exam scope, which is based on risk assessment and demonstrated ability of credit union to mitigate risk.

Cell: B82

Comment: Credit unions must complete and file all mandatory Suspicious Activity Reports. There is no waiver for the requirement to file mandatory SARs. Refusal to file a mandatory SAR could be interpreted as willful blindness.

Credit unions must either complete and file required CTRs or receive a ruling from the Internal Revenue Service Detroit Computing Center granting permission to not file the required CTRs. This type of ruling is referred to as a backfiling determination.

Cell: B83

Comment: For delinquent Currency Transaction Reports (CTRs), credit unions may either complete and file required CTRs or request a ruling from the Internal Revenue Service Detroit Computing Center (IRS DCC), which processes SARs for FinCEN. This type of ruling is referred to as a backfiling determination.

The contact telephone number for the IRS DCC Help Desk is 800.800.2877. To request a backfiling determination, the credit union need to estimate the number of CTRs that should have been filed and the timeframe for filing the CTRs.

Cell: B84

Comment: If internal controls failed, credit union may not have engaged in sufficient risk mitigation or the credit union may have under-estimated BSA/AML risk. As appropriate, credit union should be encouraged to strengthen controls, review risk assessment, and/or expand independent testing.

Cell: B85

Comment: Internal controls should be consistent with the BSA risk exposure and resources of the credit union.

Cell: B86

Comment: For credit unions where internal controls worked as intended, are the controls sufficient to provide a reasonable belief that all BSA transactions are identified and reported, as required by statute?