Appendix 308A

Excerpts from the Federal Financial Institutions Examination Council's BSA/AML Examination Guide

The federal banking agencies are responsible for the oversight of the various banking entities operating in the United States, including foreign branch offices of U.S. banks and credit unions. The federal banking agencies are charged with chartering (National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision), insuring (Federal Deposit Insurance Corporation and National Credit Union Administration), regulating, and supervising banks, credit unions, and savings associations. 12 USC 1818(s)(2) requires the appropriate federal banking agency include a review of the BSA compliance program at each examination of an insured depository institution.

This Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA) /Anti-Money Laundering (AML) Examination Manual provides guidance to all of the banking agencies examiners for carrying out BSA/AML and Office of Foreign Assets Control (OFAC) examinations. The development of the examination manual was a collaborative effort of the federal banking agencies and the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, to ensure consistency in the application of the BSA/AML requirements. In addition, OFAC assisted in the development of the sections of the manual that relate to OFAC reviews.

While OFAC regulations are not part of the BSA, examination procedures include examining a bank or corporate credit union's policies, procedures, and processes for ensuring compliance with OFAC sanctions. Refer to Appendix 308B for more information on OFAC.

The federal banking agencies require each institution under their supervision to establish and maintain a BSA compliance program. In accordance with the Patriot Act, FinCEN's regulations require certain financial institutions to establish an AML compliance program that

guards against money laundering and terrorist financing and ensures compliance with the BSA and its implementing regulations.

As part of a strong BSA/AML compliance program, the NCUA seeks to ensure each credit union has policies, procedures, and processes to identify and report suspicious transactions to law enforcement. The examination process assesses whether credit unions have established the appropriate policies, procedures, and processes based on their BSA/AML risk to identify and report suspicious activity and they provide sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions reported.

NCUA Rules and Regulations, Part 748.2 require credit unions to develop and provide for the continued administration of a BSA compliance program reasonably designed to assure and monitor compliance with Department of Treasury regulations and related BSA implementing laws and regulations. The compliance program must be commensurate with its respective BSA/AML risk profile. Furthermore, the program must be fully implemented and reasonably designed to meet the BSA requirements. Policy statements alone are not sufficient; practices must coincide with the credit union's written policies, procedures, and processes. The compliance program must be:

- written
- approved by the board of directors, and
- be reflected in the minutes of the credit union.

Each credit union must also comply with the U.S.A. Patriot Act and its promulgating regulations and laws, which require a customer identification program to be implemented as part of the BSA compliance program.

The BSA/AML compliance program shall at a minimum:

1) provide for a system of internal controls to assure ongoing compliance;
2) provide for independent testing for compliance to be conducted by credit union personnel or outside parties;

3) designate an individual responsible for coordinating and monitoring day-to-day compliance; and
4) provide training for appropriate personnel.

Risk Assessment

An effective BSA/AML compliance program requires sound risk management. The same risk management principles the credit union uses in traditional operational areas should be applied to assessing and managing BSA/AML risk. A well-developed risk assessment will assist in identifying the credit union's BSA/AML risk profile. Understanding the risk profile enables the credit union to apply appropriate risk management processes to the BSA/AML compliance program to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in the credit union's control environment. The risk assessment should provide a comprehensive analysis of the BSA/AML risks in a concise and organized presentation. The risk assessment should be shared and communicated with all business lines across the financial institution, the board of directors, management, and appropriate staff. As such, it is a sound practice the risk assessment be reduced to writing.

Examiners should review and evaluate the reasonableness of the credit union's BSA/AML risk assessment. The development of the BSA/AML risk assessment generally involves two steps: first, identifying the specific risk categories (i.e., products, services, members, entities, and geographic locations) unique to the credit union; and second, conducting a more detailed analysis of the data identified to better assess the risk within these categories. In reviewing the risk assessment, the examiner should determine whether management has considered all products, services, members, and geographic locations, and whether management's detailed analysis within these specific risk categories was adequate. If the credit union has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the credit union has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment based on available information. Refer to the FFIEC BSA/AML Examination Manual Appendices I and J for more information on risk assessments.

System of Internal Controls

Management should structure the credit union's BSA/AML compliance program to adequately address its risk profile, as identified by the risk assessment. Management should understand the credit union's BSA/AML risk exposure and develop the appropriate policies, procedures, and processes to monitor and control BSA/AML risks. For example, the credit union's monitoring systems to identify, research, and report suspicious activity should be risk-based, with particular emphasis on high risk products, services, members, and geographic locations as identified by the credit union's BSA/AML risk assessment.

The board of directors, acting through senior management, is ultimately responsible for ensuring the credit union maintains an effective BSA/AML internal control structure, including suspicious activity monitoring and reporting. The board of directors and management should create a culture of compliance to ensure staff adherence to the credit union's BSA/AML policies, procedures, and processes.

Internal Controls

Internal controls are the credit union's policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the credit union. Large complex credit unions are more likely to implement departmental internal controls for BSA/AML compliance. Departmental 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. Internal controls should:

- Identify "banking" operations (products, services, members, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the credit union's risk profile; and provide for a BSA/AML compliance program tailored to manage risks.

- Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of Suspicious Activity Reports (SARs) filed.
- Identify a person or persons responsible for BSA/AML compliance.
- Provide for program continuity despite changes in management or employee composition or structure.
- Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance, and provide for timely updates in response to changes in regulations.
- Implement risk-based customer due diligence (CDD) policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports including SARs, Currency Transaction Reports (CTRs), and CTR exemptions. (Credit unions should consider centralizing the review and report filing functions within the organization.)
- Provide sufficient controls and systems for filing CTRs and CTR exemptions.
- Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
- Incorporate BSA compliance into the job descriptions and performance evaluations of appropriate personnel.

The above list is not all-inclusive and should be tailored to reflect the credit union's BSA/AML risk profile. Refer to the FFIEC BSA/AML Examination manual for additional policy guidance for specific risk areas.

Independent Testing

As part of the scoping and planning process, examiners should obtain and evaluate the supporting documents of the independent testing (audit) of the credit union's BSA/AML compliance program. The scope and quality of the audit may provide examiners with a sense of particular risks in the credit union, how these risks are being managed and controlled, and the status of compliance with the BSA. The

independent testing scope and work papers can assist examiners in understanding the audit coverage and the quality and quantity of transaction testing. This knowledge will assist examiners in determining the examination scope, identifying areas requiring greater (or lesser) scrutiny, and identifying when expanded examination procedures may be necessary.

Independent testing should review the credit union's risk assessment for reasonableness. Additionally, management should consider the staffing resources and the level of training necessary to promote adherence with these policies, procedures, and processes. For credit unions that assume a higher risk BSA/AML profile, management should provide a more robust program, specifically monitoring and controlling the higher risks management and the board have accepted.

Parties Conducting Independent Testing & Frequency
A credit union's internal audit department, outside auditors, consultants, or other qualified independent parties should conduct independent testing. While the frequency of audit is not specifically defined in any statute, a sound practice is for the credit union to conduct independent testing generally every 12 to 18 months, commensurate with the BSA/AML risk profile of the credit union. Credit unions that do not employ outside auditors or consultants or have internal audit departments may comply with this requirement by using qualified persons who are not involved in the function being tested. The persons conducting the BSA/AML testing should report directly to the board of directors or Supervisory Committee.

Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with the BSA, and evaluate pertinent management information systems (MIS). The audit should be risk based and evaluate the quality of risk management for all "banking" operations, departments, lines of business, and subsidiaries. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

BSA Compliance Officer

The credit union's board of directors must designate a qualified individual to serve as the BSA compliance officer. The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the credit union's adherence to the BSA and its implementing regulations; however, the board of directors is ultimately responsible for the credit union's BSA/AML compliance.

While the title of the individual responsible for overall BSA/AML compliance is not important, his or her level of authority and responsibility within the credit union is critical. The BSA compliance officer may delegate BSA/AML duties to other employees, but the officer should be responsible for overall BSA/AML compliance. The board of directors is responsible for ensuring the BSA compliance officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML compliance program based on the credit union's risk profile.

The BSA compliance officer should be fully knowledgeable of the BSA and all related regulations. The BSA compliance officer should also understand the credit union's products, services, members, and geographic locations, and the potential money laundering and terrorist financing risks associated with those activities. The 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.

The line of communication should allow the BSA compliance officer to regularly apprise the board of directors and senior management of ongoing compliance with the BSA. Pertinent BSA related information, including the reporting of SARs filed with FinCEN, should be reported to the board of directors or an appropriate board committee so these individuals can make informed decisions about overall BSA/AML compliance. The BSA compliance officer is responsible for carrying out the direction of the board and ensuring employees adhere to the credit union's BSA/AML policies, procedures, and processes.

Training

Credit unions must ensure appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the credit union's internal BSA/AML policies, procedures, and processes. At a minimum, the credit union's training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person's specific responsibilities. In addition, an overview of the BSA/AML requirements typically should be given to new staff during employee orientation. Training should encompass information related to applicable business lines, such as trust services, international, and private banking. The BSA compliance officer should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall BSA/AML risk profile of the credit union.

The board of directors and senior management should be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. While the board of directors may not require the same degree of training as operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the credit union. Without a general understanding of the BSA, the board of directors cannot adequately provide BSA/AML oversight; approve BSA/AML policies, procedures, and processes; or provide sufficient BSA/AML resources.

Training should be ongoing and incorporate current developments and changes to the 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 and senior management place on the credit union's compliance with the BSA and ensure all employees understand their role in maintaining an effective BSA/AML compliance program. Examples of money laundering activity and suspicious activity monitoring and reporting can and 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.

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.

As part of the scoping and planning procedures, examiners must review the credit union's OFAC risk assessment and independent testing to determine the extent to which a review of the credit union's OFAC program should be conducted during the examination.

Suspicious Activity Reporting

Suspicious activity reporting forms the 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. Within this system, FinCEN and the federal banking agencies recognize, as a practical matter, it is not possible for a financial institution to detect and report all potentially illicit transactions that flow through the organization. Examiners should focus on evaluating a credit union's policies, procedures, and processes to identify and research suspicious activity. However, as part of the examination process, examiners should review individual Suspicious Activity Report (SAR) filing decisions to determine the effectiveness of the suspicious activity monitoring and reporting process. Above all, examiners and credit unions should recognize the quality of SAR data is paramount to the effective implementation of the suspicious activity reporting system.

Credit unions are required by federal regulations to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount;
- Criminal violations aggregating $5,000 or more when a suspect can be identified;
- Criminal violations aggregating $25,000 or more regardless of a potential suspect; and
- 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 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; or
- Has no business or apparent lawful purpose or is not the type of transaction the particular 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.

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

Safe Harbor for Banks from Civil Liability for Suspicious Activity Reporting

Federal law (31 USC 5318(g)(3)) 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. Specifically, the law provides a credit union and its directors, officers, employees, and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.

Systems to Identify, Research, and Report Suspicious Activity

Policies, procedures, and processes should indicate the persons responsible for the identification, research, and reporting of suspicious activities. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The level of monitoring should be dictated by the credit union's assessment of risk, with particular emphasis on high risk

products, services, members, entities, and geographic locations. Monitoring systems typically include employee identification or referrals, manual systems, automated systems, or any combination. The credit union should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities considering the credit union's overall risk profile and the volume of transactions.

Upon identification of unusual activity, additional research is typically conducted. Customer due diligence (CDD) information assists in evaluating if the unusual activity is considered suspicious. After thorough research and analysis, decisions to file or not to file a SAR should be documented. If applicable, reviewing and understanding suspicious activity monitoring across the organization's affiliates, business lines, and risk types (e.g., reputation, compliance, or transaction) may enhance a credit union's ability to detect suspicious activity and thus minimize the potential for financial losses, increased expenses, and reputation risk to the organization.

Identifying Underlying Crime

Credit unions are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and certain other crimes above prescribed dollar thresholds. However, credit unions are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). **Investigation is the responsibility of law enforcement.** When evaluating suspicious activity and completing the SAR, credit unions should, to the best of their ability, identify the characteristics of the suspicious activity. Part III, Section 35, of the SAR provides 20 different characteristics of suspicious activity. Although an "Other" category is available, the use of this category should be limited to situations that cannot be broadly identified within the 20 characteristics provided.

Law Enforcement Inquiries and Requests

Credit unions should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects, identifying unusual or suspicious activity related to those subjects, and filing, as applicable, SARs related to those subjects. Law enforcement inquiries and requests can include grand jury subpoenas, National Security Letters (NSLs), and section 314(a) requests.

Mere receipt of any law enforcement inquiry, does not, by itself, require the filing of a SAR by the credit union. Nonetheless, a law enforcement inquiry may be relevant to a credit union's overall risk assessment of its members and accounts. For example, the receipt of a grand jury subpoena should cause a credit union to review account activity for the relevant member. It is incumbent upon a credit union to assess all of the information it knows about its member, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program.

The credit union should determine whether a SAR should be filed based on all member information available. Due to the confidentiality of grand jury proceedings, if a credit union files a SAR after receiving a grand jury subpoena, law enforcement discourages credit unions and banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Rather, the SAR should reference only those facts and activities that support a finding of suspicious transactions identified by the credit union.

SAR Decision-Making Process

The credit union should have policies, procedures, and processes for referring unusual activity from all 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.

The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the credit union has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the credit union has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the credit union should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.

Credit unions are encouraged to document SAR decisions. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR; however, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact each suspicious activity reporting decision will be based on unique facts and circumstances, no single, standard form of documentation is required when a credit union makes a decision not to file.

Timing of a SAR Filing

The SAR rules require a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a member to determine whether to file a SAR. The need for a review of member activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect the activity or transactions under review meet one or more of the definitions of suspicious activity.

For situations involving violations requiring immediate attention, in addition to filing a timely SAR, a credit union is required to immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the credit union's regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the Internal Revenue Service Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a credit union of its obligation to file a SAR.

Notifying Board of Directors of SAR Filings

Credit unions are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and credit unions should have flexibility in structuring their format. Therefore, credit unions may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, credit unions may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the credit union, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties.

SAR Quality

Credit unions are required to file SAR forms that are complete, thorough, and timely. Credit unions should include all known suspect information on the SAR form. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR

form, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. However, there may be legitimate reasons why certain information may not be provided in a SAR, such as when the filer does not have the information. A thorough and complete narrative may make the difference in whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Because the SAR narrative section is the only area summarizing suspicious activity, the narrative section, as stated on the SAR form, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

By their nature, SAR narratives are subjective, and examiners generally should not criticize the credit union's interpretation of the facts. Nevertheless, credit unions should ensure SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and are included within the SAR form (e.g., no attachments to the narrative section will be included within the BSA reporting database). More specific guidance is available in Appendix L ("SAR Quality Guidance") to assist credit unions in writing, and assist examiners in evaluating, SAR narratives. In addition, comprehensive guidance is available from FinCEN ("Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative") at www.fincen.gov.

Prohibition of SAR Disclosure

No credit union, director, officer, employee, or agent of a credit union that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. Thus, any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement or federal banking agency, shall decline to produce the SAR or to provide any information that would disclose a SAR has been prepared or filed, citing 31 CFR 103.18(e) and 31 USC 5318(g)(2). FinCEN and the credit union's federal banking agency should be notified of any such request and of the credit union's response. Furthermore, FinCEN and the federal banking agencies take the position that credit unions' internal controls for the filing of SARs should minimize the risks of disclosure.

SAR Record Retention and Supporting Documentation

Credit unions must retain copies of SARs and supporting documentation for five years from the date of the report. Additionally, credit unions must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency. "Supporting documentation" refers to all documents or records that assisted a credit union in making the determination that certain activity required a SAR filing. No legal process is required for disclosure of supporting documentation to FinCEN or an appropriate law enforcement or supervisory agency.

Additional Information on BSA

Examiners can find more detailed information on conducting BSA/AML examinations in the FFIEC BSA/AML Examination manual. The manual may be accessed via the FFIEC website at www.ffiec.gov.